show mpls oam echo statistics through switching tlv

- show mpls oam echo statistics, page 4
- show mpls platform, page 6
- show mpls prefix-map, page 9
- show mpls static binding, page 11
- show mpls static crossconnect, page 14
- show mpls tp link-management admission-control failures, page 16
- show mpls traffic tunnel backup, page 18
- show mpls traffic-eng autoroute, page 20
- show mpls traffic-eng auto-tunnel backup, page 22
- show mpls traffic-eng auto-tunnel mesh, page 24
- show mpls traffic-eng auto-tunnel primary, page 26
- show mpls traffic-eng destination list, page 28
- show mpls traffic-eng exp, page 30
- show mpls traffic-eng fast-reroute database, page 32
- show mpls traffic-eng fast-reroute log reroutes, page 38
- show mpls traffic-eng forwarding-adjacency, page 40
- show mpls traffic-eng forwarding path-set, page 42
- show mpls traffic-eng forwarding statistics, page 45
- show mpls traffic-eng link-management admission-control, page 47
- show mpls traffic-eng link-management advertisements, page 49
- show mpls traffic-eng link-management bandwidth-allocation, page 52
- show mpls traffic-eng link-management igp-neighbors, page 56
- show mpls traffic-eng link-management interfaces, page 58

- show mpls traffic-eng link-management summary, page 61
- show mpls traffic-eng lsp attributes, page 65
- show mpls traffic-eng nsr, page 67
- show mpls traffic-eng process-restart iprouting, page 75
- show mpls traffic-eng topology, page 77
- show mpls traffic-eng topology path, page 81
- show mpls traffic-eng tunnels, page 83
- show mpls traffic-eng tunnels statistics, page 95
- show mpls traffic-eng tunnels summary, page 99
- show mpls ttfib, page 103
- show platform software ethernet f0 efp, page 104
- show platform software ethernet f1 efp, page 106
- show platform software mpls, page 108
- show platform software vpn, page 110
- show policy-map interface, page 111
- show pw-udp vc, page 160
- show running interface auto-template, page 162
- show running-config vrf, page 164
- show spanning-tree mst, page 168
- show ssm group, page 174
- show tech-support mpls, page 176
- show vfi, page 179
- show vrf, page 184
- show xconnect, page 188
- show xtagatm cos-bandwidth-allocation, page 202
- show xtagatm cross-connect, page 204
- show xtagatm vc, page 209
- shutdown (mpls), page 211
- signaling protocol, page 213
- snmp mib mpls vpn, page 215
- snmp-server community, page 217
- snmp-server enable traps (MPLS), page 221
- snmp-server enable traps mpls ldp, page 229

- snmp-server enable traps mpls p2mp-traffic-eng, page 232
- snmp-server enable traps mpls rfc ldp, page 234
- snmp-server enable traps mpls rfc vpn, page 237
- snmp-server enable traps mpls traffic-eng, page 240
- snmp-server enable traps mpls vpn, page 242
- snmp-server group, page 245
- snmp-server host, page 250
- source template type pseudowire, page 264
- spanning-tree mode, page 265
- spanning-tree mst configuration, page 267
- status (pseudowire class), page 269
- status control-plane route-watch, page 271
- status protocol notification static, page 273
- status redundancy, page 275
- switching-point, page 277
- switching tlv, page 279

show mpls oam echo statistics

To display statistics about Multiprotocol Label Switching (MPLS) Operation, Administration, and Maintenance (OAM) echo request packets, use the **show mpls oam echo statistics** command in privileged EXEC mode.

show mpls oam echo statistics [summary]

Syntax Description

summary	(Optional) Displays summary information about the echo request packets (that is, the type, length, values (TLVs) version and the return codes of echo packets are not displayed).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

You can use the**show mpls oam echo statistics** command to display the following:

- Currently configured TLV version for MPLS OAM operations.
- Return code distribution among the received MPLS echo reply packets.
- Statistics of sent and received MPLS echo packets, and counts of incomplete packet dispatches and timed out MPLS echo requests.

If you enter the **summary** keyword, the Echo Reply count shows all the echo reply packets, regardless of whether they are valid responses to a sent request packet. Therefore, the number of return codes will not match the number of echo reply packets received.

Examples

The following example displays sample detailed output when the **summary** keyword is not specified:

```
Router# show mpls oam echo statistics
Cisco TLV version: RFC 4379 Compliant
```

```
Return code distribution:
 !--Success (3) - 5
 B--Unlabeled output interface (9) - 0
 D--DS map mismatch (5) - 0
 f--Forward Error Correction (FEC) mismatch (10) - 0
 F--No FEC mapping (4) - 0
 I--Unknown upstream interface index (6) - 0
 L--Labeled output interface (8) - 0
 m--Unsupported TLVs (2) - 0
 M--Malformed echo request (1) - 0
 N--No label entry (11) - 0
 p--Premature termination of link-state packet (LSP) (13) - 0
 P--No receive interface label protocol (12) - 0
 U--Reserved (7) - 0
 x--No return code (0) - 0
 X--Undefined return code - 0
Echo Requests: sent (5)/received (0)/timedout (0)/unsent (0)
Echo Replies: sent (0)/received (5)/unsent (0)
```

The following example displays sample output when the **summary** keyword is specified:

```
Router# show mpls oam echo statistics summary
Cisco TLV version: RFC 4379 Compliant
Echo Requests: sent (5)/received (0)/timedout (0)/unsent (0)
Echo Replies: sent (0)/received (5)/unsent (0)
```

The table below describes the significant fields shown in the displays.

Table 1: show mpls oam echo statistics Field Descriptions

Field	Description
Return Code Distribution	In each line of the return code distribution, the following information is displayed: • Single-character code corresponding to the return code in the received packet (for example ! or B). • Description of the return code (for example, Success). • Value of the return code (for example, (3)). • Number of packets received with the return code (for example, 5).
sent	Number of MPLS echo request packets that the router sent.
timedout	Number of MPLS echo request packets that timed out.
received	Number of MPLS echo request packets that the router received from the network.
unsent	Number of MPLS echo requests that were not forwarded due to errors.

show mpls platform

To display platform-specific information, use the **show mpls platform** command in EXEC mode.

show mpls platform {**common**| **eompls**| **gbte-tunnels**| **reserved-vlans vlan** *vlan-id*| **statistics [reset]**| **vpn-vlan-mapping**}

Syntax Description

common	Displays the counters for shared code between the LAN and WAN interfaces.
eompls	Displays information about the Ethernet over Multiprotocol Label Switching (EoMPLS)-enabled interface.
gbte-tunnels	Displays information about the Multicast Multilayer Switching (MMLS) Guaranteed Bandwidth Traffic Engineering (GBTE) tunnels.
reserved-vlans vlan *vlan-id*	Displays Route Processor (RP)-reserved VLAN **show** commands; valid values are from 0 to 4095.
statistics	Displays information about the RP-control plane statistics.
reset	(Optional) Resets the statistics counters.
vpn-vlan-mapping	Displays information about the Virtual Private Network (VPN)-to-VLAN mapping table.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was introduced in the Catalyst 6500.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the counters for shared code between the LAN and WAN interfaces:

```
Router# show mpls platform common
Common MPLS counters for LAN and WAN
-------------------------------------
 No. of MPLS configured LAN interfaces           = 12
 No. of cross-connect configured VLAN interfaces = 0
Router#
```

This example shows how to display the EoMPLS-enabled interface information:

```
Router# show mpls platform eompls
Interface        VLAN
GigabitEthernet  101
FastEthernet6/1  2022
Router#
```

This example shows how to display the GBTE-tunnels information:

```
Router# show mpls platform gbte-tunnels
To            From          InLbl   I/I/F kbps     Kbits    H/W Info
Router#
```

This example shows how to display the RP-reserved VLAN **show** commands:

```
Router# show mpls platform reserved-vlans vlan 1005
```

Note This example shows the output if there are no configured reserved VLANs.

This example shows how to display the information about the RP-control plane statistics:

```
Router# show mpls platform statistics
              RP MPLS Control Plane Statistics:
      ================================================
Reserved VLAN creates                     0000000001
Reserved VLAN frees                       0000000000
Reserved VLAN creation failures           0000000000
Aggregate Label adds                      0000000001
Aggregate Label frees                     0000000000
Aggregate Labels in Superman              0000000001
Feature Rsvd VLAN Reqs                    0000000000
Feature Gen Rsvd VLAN Reqs                0000000000
Feature Rsvd VLAN Free Reqs               0000000000
EoMPLS VPN# Msgs                          0000000009
EoMPLS VPN# Msg Failures                  0000000000
EoMPLS VPN# Msg Rsp Failures              0000000000
EoMPLS VPN# Set Reqs                      0000000010
EoMPLS VPN# Reset Reqs                    0000000008
FIDB mallocs                              0000000000
FIDB malloc failures                      0000000000
FIDB frees                                0000000000
EoMPLS Req mallocs                        0000000018
EoMPLS Req malloc failures                0000000000
EoMPLS Req frees                          0000000018
EoMPLS VPN# allocs                        0000000010
EoMPLS VPN# frees                         0000000008
EoMPLS VPN# alloc failures                0000000000
GB TE tunnel additions                    0000000000
GB TE tunnel label resolves               0000000000
GB TE tunnel deletions                    0000000000
GB TE tunnel changes                      0000000000
```

```
GB TE tunnel heads skips                0000000000
gb_flow allocs                          0000000000
gb_flow frees                           0000000000
rsvp req creats                         0000000000
rsvp req frees                          0000000000
rsvp req malloc failures                0000000000
gb_flow malloc failures                 0000000000
psb search failures                     0000000000
GB TE tunnel deleton w/o gb_flow        0000000000
errors finding slot number              0000000000
Router#
```

This example shows how to reset the RP-control plane statistics counters:

```
Router# show mpls platform statistics reset
Resetting Const RP MPLS control plane software statistics ...
GB TE tunnel additions                  0000000000
GB TE tunnel label resolves             0000000000
GB TE tunnel deletions                  0000000000
GB TE tunnel changes                    0000000000
GB TE tunnel heads skips                0000000000
gb_flow allocs                          0000000000
gb_flow frees                           0000000000
rsvp req creats                         0000000000
rsvp req frees                          0000000000
rsvp req malloc failures                0000000000
gb_flow malloc failures                 0000000000
psb search failures                     0000000000
GB TE tunnel deleton w/o gb_flow        0000000000
errors finding slot number              0000000000
Router#
```

This example shows how to display information about the VPN-to-VLAN mapping table:

```
Router# show mpls platform vpn-vlan-mapping
VPN#  Rsvd Vlan  IDB Created  Feature  Has agg label  In superman    EoM data
0     1025       Yes          No       No             No             No
1     0          No           No       Yes            Yes            No
Router#
```

show mpls prefix-map

Note Effective with Cisco IOS Release 12.4(20)T, the **show mpls prefix-map** command is not available in Cisco IOS software.

To display the prefix map used to assign a quality of service (QoS) map to network prefixes that match a standard IP access list, use the **show mpls prefix-map** command in privileged EXEC mode.

show mpls prefix-map [*prefix-map*]

Syntax Description

prefix-map	(Optional) Number specifying the prefix map to be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) syntax and terminology.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was removed.

Usage Guidelines

Not entering a specific *prefix-map* argument number causes all prefix maps to be displayed.

Examples

The following is sample output from the **show mpls prefix-map** command:

```
Router# show mpls prefix-map 2
prefix-map 2 access-list 2 cos-map 2
```

The table below describes the fields shown in the display.

Table 2: show mpls prefix-map Field Descriptions

Field	Description
prefix-map	Unique number of a prefix map.
access-list	Unique number of an access list.
cos-map	Unique number of a QoS map.

Related Commands

Command	Description
mpls prefix-map	Configures a router to use a specified QoS map when a label destination prefix matches the specified access-list.

show mpls static binding

To display Multiprotocol Label Switching (MPLS) static label bindings, use the **show mpls static binding** command in privileged EXEC mode.

show mpls static binding[**ipv4**[**vrf** *vrf-name*]][*prefix*{*mask-length*| *mask*}][**local**| **remote**][**nexthop** *address*]

Syntax Description

ipv4	(Optional) Displays IPv4 static label bindings.
vrf *vrf-name*	(Optional) The static label bindings for a specified VPN routing and forwarding instance.
prefix {*mask-length* | *mask*}	(Optional) Labels for a specific prefix.
local	(Optional) Displays the incoming (local) static label bindings.
remote	(Optional) Displays the outgoing (remote) static label bindings.
nexthop *address*	(Optional) Displays the label bindings for prefixes with outgoing labels for which the specified next hop is to be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.0(26)S	This command was modified. The **vrf** *vrf-name* keyword argument pair was added.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.5S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

If you do not specify any optional arguments, the show mpls static binding command displays information about all static label bindings. Or the information can be limited to any of the following:

- Bindings for a specific prefix or mask
- Local (incoming) labels
- Remote (outgoing) labels
- Outgoing labels for a specific next hop router

Examples

In the following output, the **show mpls static binding ipv4** command with no optional arguments displays all static label bindings:

```
Router# show mpls static binding ipv4
10.0.0.0/8: Incoming label: none;
  Outgoing labels:
     10.13.0.8           explicit-null
10.0.0.0/8: Incoming label: 55 (in LIB)
  Outgoing labels:
     10.0.0.66              2607
10.66.0.0/16: Incoming label: 17 (in LIB)
  Outgoing labels:  None
```

In the following output, the **show mpls static binding ipv4** command displays remote (outgoing) statically assigned labels only:

```
Router# show mpls static binding ipv4 remote
10.0.0.0/8:
  Outgoing labels:
     10.13.0.8           explicit-null
10.0.0.0/8:
  Outgoing labels:
     10.0.0.66              2607
```

In the following output, the **show mpls static binding ipv4** command displays local (incoming) statically assigned labels only:

```
Router# show mpls static binding ipv4 local
10.0.0.0/8: Incoming label: 55 (in LIB)
10.66.0.0/16: Incoming label: 17 (in LIB)
```

In the following output, the**show mpls static binding ipv4** command displays statically assigned labels for prefix 10.0.0.0 / 8 only:

```
Router# show mpls static binding ipv4 10.0.0.0/8
10.0.0.0/8: Incoming label: 55 (in LIB)
  Outgoing labels:
     10.0.0.66              2607
```

In the following output, the **show mpls static binding ipv4** command displays prefixes with statically assigned outgoing labels for next hop 10.0.0.66:

```
Router# show mpls static binding ipv4 10.0.0.0 8 nexthop 10.0.0.66
10.0.0.0/8: Incoming label: 55 (in LIB)
  Outgoing labels:
     10.0.0.66              2607
```

The following output, the **show mpls static binding ipv4 vrf** command displays static label bindings for a VPN routing and forwarding instance vpn100:

```
Router# show mpls static binding ipv4 vrf vpn100
192.168.2.2/32: (vrf: vpn100) Incoming label: 100020
Outgoing labels: None
192.168.0.29/32: Incoming label: 100003 (in LIB)
Outgoing labels: None
```

Related Commands

Command	Description
mpls static binding ipv4	Binds an IPv4 prefix or mask to a local or remote label.

show mpls static crossconnect

To display statically configured Label Forwarding Information Database (LFIB) entries, use the **show mpls static crossconnect** command in privileged EXEC mode.

show mpls static crossconnect [*low label* [*high label*]]

Syntax Description

low label high label	(Optional) The statically configured LFIB entries.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If you do not specify any label arguments, then all the configured static cross-connects are displayed.

Examples

The following sample output from the **show mpls static crossconnect** command shows the local and remote labels:

```
Router# show mpls static crossconnect
Local  Outgoing    Outgoing   Next Hop
label  label       interface
45     46          pos5/0     point2point
```

The table below describes the significant fields shown in the display.

Table 3: show mpls static crossconnect Field Descriptions

Field	Description
Local label	Label assigned by this router.
Outgoing label	Label assigned by the next hop.
Outgoing interface	Interface through which packets with this label are sent.

Field	Description
Next Hop	IP address of the next hop router's interface that is connected to this router's outgoing interface.

Related Commands

Command	Description
mpls static crossconnect	Configures an LFIB entry for the specified incoming label and outgoing interface.

show mpls tp link-management admission-control failures

To determine the end-to-end state of MPLS Transport Profile (TP) tunnels, use the **show mpls tp link-management admission-control failures** command in user EXEC or privileged EXEC mode.

show mpls tp link-management admission-control failures

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)S	This command was introduced.

Usage Guidelines

The **show mpls tp link-management admission-control failures** command is typically used to display information about MPLS Transport Profile (TP) endpoint and midpoint label switched path (LSP) admission failures. For example, this command can determine which MPLS-TP tunnels were not admitted due to insufficient bandwidth available on the physical interfaces.

Examples

```
        R1#show mpls tp link-management admission-control failures
MPLS-TP Endpoint LSP admission failures:
Tun   Dest                                          Out      Req BW
Num   Global-id::Node-id          LSP               Intf     kbps
----- --------------------------  ----------------  -------- ------

MPLS-TP Midpoint LSP admission failures:
Src   Src                  Dest  Dest                LSP   Out      Req BW
Tun   Global-id::Node-id   Tun   Global-id::Node-id  Num   Intf     kbps
----- -------------------- ----- ------------------- ----- -------- ------
```

The table below describes the significant fields shown in the display.

Table 4: show mpls tp link-management admission-control failures Field Descriptions

Field	Description
Tun Num	Tunnel number.

Field	Description
Dest Global-id::Node-id	Destination global ID or the destination node ID. The global ID is usually the default global ID used for all endpoints and midpoint. The global ID is an autonomous system number, which is a controlled number space by which providers can identify each other.
LSP	LSP number.
Out Intf	Outbound (egress) interface.
Req BW kbps	Requisite bandwidth in kilobytes per second.
Src Tun	Source tunnel number.
Src Global-id::Node-id	Source global ID or source node ID number.
Dest Tun	Destination tunnel number.
LSP Num	LSP number.

Related Commands

Command	Description
show mpls tp tunnel-tplsps	Determines that both LSPs are up and working from a tunnel endpoint.

show mpls traffic tunnel backup

To display information about the backup tunnels that are currently configured, use the **show mpls traffic tunnel backup** command in user EXEC or privileged EXEC mode.

show mpls traffic tunnel backup tunnel *tunnel-id*

Syntax Description

tunnel*tunnel-id*	Tunnel ID of the backup tunnel for which you want to display information.

Command Default

Information about currently configured backup tunnels is not displayed.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T

Examples

The following is sample output from the **show mpls traffic tunnel backup tunnel** *tunnel-id* command:

```
Router# show mpls traffic tunnel backup tunnel 1000
Tunnel1000          Dest: 10.0.0.9        State: Up
any-pool cfg 100 inuse 0 num_lsps 0
     protects: ATM0.1
```

The table below describes the significant fields shown in the display.

Table 5: show mpls traffic tunnel backup Field Descriptions

Field	Description
Tunnel	Tunnel ID of the backup tunnel for which this information is being displayed.
Dest	IP address of the destination of the backup tunnel.

Field	Description
State	State of the backup tunnel. Valid values are Up, Down, or Admin-down.
any-pool	Pool from which bandwidth is acquired. Valid values are any-pool, global-pool, and sub-pool.
cfg	Amount of bandwidth configured for that pool.
inuse	Amount of bandwidth currently being used.
num_lsps	Number of label-switched paths (LSPs) being protected.
protects	The protected interfaces that are using this backup tunnel.

Related Commands

Command	Description
tunnel mpls traffic-eng backup-bw	Specifies what types of LSPs can use a backup tunnel, whether the backup tunnel should provide bandwidth protection, and if so, how much.

show mpls traffic-eng autoroute

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

show mpls traffic-eng autoroute

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

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

Examples

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

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

```
Router# show mpls traffic-eng autoroute

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

The table below describes the significant fields shown in the display.

Table 6: show mpls traffic-eng autoroute Field Descriptions

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

Related Commands

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

show mpls traffic-eng auto-tunnel backup

To display information about dynamically created Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels, use the **show mpls traffic-eng auto-tunnel backup** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng auto-tunnel backup

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.

Examples

The following is sample output from the **show mpls traffic-eng auto-tunnel backup** command.

```
Router# show mpls traffic-eng auto-tunnel backup

State: Enabled
  Auto backup tunnels: 4 (up:2, down:2)
  Tunnel ID Range: 65436-65535
  Create Nhop only: Yes
  Check for deletion of unused tunnels every: 600 sec
  SRLG Exclude: Preferred
  Config:
    Unnumbered-interface: Looback0
    Affinity/Mask: 0x2/0xFFFF
```

The table below describes the significant fields shown in the display.

Table 7: show mpls traffic-eng auto-tunnel backup Field Descriptions

Field	Description
State	State of the dynamically created tunnel. Valid values are enabled or disabled.
Auto backup tunnels	Number of dynamically created backup tunnels created.
Tunnel ID Range	Tunnel ID range used when creating dynamically created backup tunnels.

Field	Description
Create Nhop only	Whether the feature was configured to enable the dynamic creation of NHOP backup tunnels (and not NNHOP). Valid values are yes or no.
Check for deletion of unused tunnels every	Number of seconds before an unused dynamically created tunnel is torn down.
SRLG Exclude	Type of Shared Risk Link Group. Valid values are forced, preferred, or not configured.
Unnumbered-interface	The interface configured with the **mpls traffic-eng autotunnel backup config unnumbered-interface** command.
Affinity/mask	The affinity and mask configured with the **mpls traffic-eng autotunnel backup config affinity** command.

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup config affinity	Enables you to specify link attributes on dynamically created MPLS TE backup tunnels.
mpls traffic-eng auto-tunnel backup config unnumbered-interface	Enables you to specify the interface to use as the unnumbered interface.
mpls traffic-eng auto-tunnel backup nhop	Specifies dynamically created NHOP backup tunnels only.
mpls traffic-eng auto-tunnel backup srlg	Specifies the use of Shared Risk Link Groups (SRLGs) as part of the dynamic backup tunnel calculation.
mpls traffic-eng auto-tunnel backup timers	Specifies the use of timers with dynamically created backup tunnels.
mpls traffic-eng auto-tunnel backup tunnel-num	Specifies tunnel interface numbers for dynamically created backup tunnels.

show mpls traffic-eng auto-tunnel mesh

To display the cloned mesh tunnel interfaces of each autotemplate interface and the current range of mesh tunnel interface numbers, use the **show mpls traffic-eng auto-tunnel mesh** command in user EXEC mode or privileged EXEC mode.

show mpls traffic-eng auto-tunnel mesh

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.

Examples

The following is output from the **show mpls traffic-eng auto-tunnel mesh** command that shows the cloned mesh tunnel interfaces for autotemplate1 and shows the range of mesh tunnel interface numbers. Information for only one autotemplate is displayed because only one autotemplate was configured.

```
Router# show mpls traffic-eng auto-tunnel mesh

Auto-Template1:
 Using access-list 1 to clone the following tunnel interfaces:
  Destination  Interface
  -----------  ---------
  10.2.2.2     Tunnel64336
  10.3.3.3     Tunnel64337
Mesh tunnel interface numbers: min 64336 max 65337
```

The table below describes the significant fields shown in the display.

Table 8: show mpls traffic-eng auto-tunnel mesh Field Descriptions

Field	Description
Auto-Template1	Name of the autotemplate.

Field	Description
Destination	Destination addresses for the mesh tunnel interface cloned from access list 1.
Interface	Mesh tunnel interfaces cloned from access list 1.
min 64336 max 65337	Range of mesh tunnel interface numbers for this Auto-Template1--minimum (64336) and maximum (65337).

Related Commands

Command	Description
interface auto-template	Creates the template interface.
mpls traffic-eng auto-tunnel mesh tunnel-num	Configures the range of mesh tunnel interface numbers.

show mpls traffic-eng auto-tunnel primary

To display information about dynamically created Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels, use the **show mpls traffic-eng auto-tunnel primary** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng auto-tunnel primary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.

Examples

The following is sample output from the **show mpls traffic-eng auto-tunnel primary** command.

```
Router# show mpls traffic-eng auto-tunnel primary

State: Enabled
  Auto primary tunnels: 2 (up: 2, down: 0)
  Tunnel ID Range: 1000-1100
  Check for deletion of FRR Active onehop tunnels every: 0 Sec

  Config:
   unnumbered I/f: Looback0
   mpls ip: TRUE
```

The table below describes the significant fields shown in the display.

Table 9: show mpls traffic-eng auto-tunnel primary Field Descriptions

State	State of the dynamically created tunnel. Valid values are enabled or disabled.
Auto primary tunnels	Number of dynamically created primary tunnels.
Tunnel ID Range	Tunnel ID range used when creating dynamically created primary tunnels.
Check for deletion of FRR Active onehop tunnels every	Amount of time, in seconds, after which a failed primary tunnel is removed.

unnumbered I/f	The interface configured with the **mpls traffic-eng auto-tunnel primary config unnumbered-interface** command.
mpls ip	Whether the Label Distribution Protocol (LDP) is enabled on primary tunnels. Valid values are true or false.

Related Commands

Command	Description
mpls traffic-eng auto-tunnel primary config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel primary config mpls ip	Enables LDP on primary autotunnels.
mpls traffic-eng auto-tunnel primary onehop	Automatically creates primary tunnels to all next hops.
mpls traffic-eng auto-tunnel primary timers	Configures how many seconds after a failure that primary autotunnels are removed.
mpls traffic-eng auto-tunnel primary tunnel-num	Configures the range of tunnel interface numbers for primary autotunnels.

show mpls traffic-eng destination list

To display a Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) destination list, use the **show mpls traffic-eng destination list** command in user EXEC or privileged EXEC configuration mode.

show mpls traffic-eng destination list [**name** *destination-list-name*| **identifier** *destination-list-identifier*]

Syntax Description

name *destination-list-name*	(Optional) Specifies the name of a destination list.
identifier *destination-list-identifier*	(Optional) Specifies the number of a destination list.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

This command displays the information about any destination lists configured for an MPLS TE P2MP configuration.

Examples

The following example displays information about a destination list:

```
Router# show mpls traffic-eng destination-list
Destination list: name p2mp-list1
    ip 10.3.3.3 path-option 1 dynamic
    ip 10.4.4.4 path-option 15 explicit identifier 4
    ip 10.5.5.5 path-option 2 explicit name r1-r2-r4-r5
```

The table below describes the significant fields shown in the display.

Table 10: show mpls traffic-eng destination-list Field Descriptions

Field	Description
Destination list	The name of the destination list.
ip	The IP address of the path's destination.
path-option	Information about the dynamic or explicit path.

Related Commands

Command	Description
mpls traffic-eng destination-list	Creates a destination list for MPLS Point-to-Multipoint Traffic Engineering.

show mpls traffic-eng exp

To display the configured and the actual experimental (EXP) bit mapping on a member tunnel that is part of the Class-based Tunnel Selection (CBTS) bundle, use the **show mpls traffic-eng exp** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng exp *ip-address*

Syntax Description

ip-address	(Optional) Destination address of the master tunnel.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.

Usage Guidelines

This command shows the member tunnels associated with each master tunnel, whether the tunnel is up or down, whether the member tunnel is active or inactive, the configured EXP values, and the actual EXP values.

Examples

```
Router# show mpls traffic-eng exp

Destination: 11.11.11.11
   Master: Tunnel100            Status: up
   Members         Status               Conf Exp        Actual Exp
   Tunnel1         up   (Active)        0                    0
   Tunnel2         up   (Active)        3 4                3 4
   Tunnel3         up   (Active)        Default          1 2 5 6 7
(D) : Destination is different
(NE): Exp values not configured on tunnel
```

Related Commands

Command	Description
tunnel mpls traffic-eng exp	Specifies the EXP bits that will be forwarded over a member tunnel that is part of the CBTS bundle.

Command	Description
tunnel mpls traffic-eng exp-bundle master	Configures a master tunnel.
tunnel mpls traffic-eng exp-bundle member	Identifies which tunnel is a member (bundled tunnel) of a master tunnel.

show mpls traffic-eng fast-reroute database

To display the contents of the Multiprotocol Label Switching (MPLS) traffic engineering (TE) Fast Reroute (FRR) database, use the **show mpls traffic-eng fast-reroute database** command in user EXEC or privileged EXEC mode.

Cisco IOS Release 15.0(1)M and Later

show mpls traffic-eng fast-reroute database [**interface** *type number*| **labels** *low-label* [*high-label*]] [**backup-interface** {**tunnel** *tunnel-number*| **unresolved**}] [**role** {**head**| **middle**}] [**state** {**active**| **ready**| **requested**}] **[detail]** [**vrf** *name*]

Cisco IOS Releases 12.0S and 12.2S

show mpls traffic-eng fast-reroute database [*destination-prefix* **slot** *slot-number*| **interface** *type number*| **labels** *low-label* [*high-label*]] [**backup-interface** {**tunnel** *tunnel-number*| **unresolved**}][**role** {**head**| **middle**}] [**state** {**active**| **ready**| **requested**}] **[detail]** [**vrf** *name*]

Syntax Description

destination-prefix	(Optional) IP address of the destination.
slot	Specifies the MPLS Forwarding Infrastructure (MFI) slot.
slot-number	Slot number of the destination.
labels	(Optional) Shows only database entries that possess in-labels (local labels) assigned by this router. You specify either a starting value or a range of values.
low-label	(Optional) Starting label value or lowest value in the range.
- *high-label*	(Optional) Highest label value in the range.
interface *type number*	(Optional) Specifies the interface type and number to display the database entries related to the primary outgoing interface.
backup-interface	(Optional) Shows only database entries related to the backup outgoing interface.
tunnel *tunnel-number*	(Optional) Specifies the tunnel interface name and number.
unresolved	(Optional) Specifies the unresolved backup interface.
role	(Optional) Shows entries associated either with the tunnel head or tunnel midpoint.

head	Entry associated with tunnel head.
middle	Entry associated with tunnel midpoint.
state	(Optional) Displays entries that match one of four possible states: active, ready, partial, or complete.
active	Specifies the label switched paths (LSP) with an active FRR state.
ready	Specifies the LSPs with a ready FRR state.
requested	Specifies the LSPs with a requested FRR state.
detail	(Optional) Shows long-form information: Label Forwarding Information Base (LFIB)-FRR total number of clusters, groups, and items in addition to the short-form information of prefix, label and state.
vrf *name*	(Optional) Shows entries for a Virtual Private Network (VPN) routing/forwarding instance.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was modified. It was implemented on the Catalyst 6000 series with the SUP720 processor.
12.2(28)SB	This command was modified. It was implemented on the Cisco 10000(PRE-2) router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was modified. The output was updated to display MPLS TE point-to-multipoint (P2MP) information.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Examples

Examples

The following is sample output from the **show mpls traffic-eng fast-reroute database** command at a tunnel head link:

```
Router# show mpls traffic-eng fast-reroute database 10.0.0.0
Tunnel head fast reroute information:
Prefix        Tunnel  In-label  Out intf/label  FRR intf/label  Status
10.0.0.0/16   Tu111   Tun hd    PO0/0:Untagged  Tu4000:16       ready
10.0.0.0/16   Tu449   Tun hd    PO0/0:Untagged  Tu4000:736      ready
10.0.0.0/16   Tu314   Tun hd    PO0/0:Untagged  Tu4000:757      ready
10.0.0.0/16   Tu313   Tun hd    PO0/0:Untagged  Tu4000:756      ready
```

The table below describes the fields shown in the display.

Table 11: show mpls traffic-eng fast-reroute database Field Descriptions

Field	Description
Prefix	Address to which packets with this label are going.
Tunnel	Tunnel's identifying number.
In-label	Label advertised to other routers to signify a particular prefix. The value "Tun hd" occurs when no such label has been advertised.
Out intf/label	Out interface--short name of the physical interface through which traffic goes to the protected link. Out label: • At a tunnel head, this is the label advertised by the tunnel destination device. The value "Untagged" occurs when no such label has been advertised. • At tunnel midpoints, this is the label selected by the next hop device. The "Pop Tag" value occurs when the next hop is the tunnel's final hop.
FRR intf/label	Fast Reroute interface--the backup tunnel interface. Fast Reroute label: • At a tunnel head, this is the label selected by the tunnel tail to indicate the destination network. The value "Untagged" occurs when no such label has been advertised. • At tunnel midpoints, this has the same value as the Out Label.

Field	Description
Status	State of the rewrite: partial, ready, complete, or active. (These terms are defined above in the "Syntax Description" section).

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

```
Router# show mpls traffic-eng fast-reroute database 10.0.0.0. detail
LFIB FRR Database Summary:
  Total Clusters:      2
  Total Groups:        2
  Total Items:         789
Link 10:PO5/0 (Down, 1 group)
  Group 51:PO5/0->Tu4000 (Up, 779 members)
    Prefix 10.0.0.0/16, Tu313, active
      Input label Tun hd, Output label PO0/0:773, FRR label Tu4000:773
    Prefix 10.0.0.0/16, Tu392, active
      Input label Tun hd, Output label PO0/0:775, FRR label Tu4000:775
    Prefix 10.0.0.0/16, Tu111, active
      Input label Tun hd, Output label PO0/0:16, FRR label Tu4000:16
    Prefix 10.0.0.0/16, Tu394, active
      Input label Tun hd, Output label PO0/0:774, FRR label Tu4000:774
```

The table below describes the significant fields when the **detail** keyword is used.

Table 12: show mpls traffic-eng fast-reroute database with detail Keyword Field Descriptions

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

Field	Description
Link 10:PO5/0 (Down, 1 group)	This field describes a cluster (physical interface): • 10 is the interface's unique IOS-assigned ID number. • The colon (:) is followed by the interface's short name. • Parentheses contain the operating state of the interface (Up or Down) and the number of groups associated with it.
Group 51:PO5/0->Tu4000 (Up, 779 members)	This field describes a group: • 51 is the ID number of the backup interface. • The colon (:) is followed by the group's physical interface short name. • The hyphen and angle bracket (->) is followed by the backup tunnel interface short name. • Parentheses contain the operating state of the tunnel interface (Up or Down) and the number of items--also called "members"-- associated with it.

The following is sample output from the **show mpls traffic-eng fast-reroute database** command with the **labels** keyword specified at a midpoint link:

```
Router# show mpls traffic-eng fast-reroute database labels 250-255
Tunnel head fast reroute information:
Prefix   Tunnel   In-label   Outintf/label   FRR intf/label   Status
LSP midpoint frr information:
LSP identifier          In-label   Out intf/label  FRR intf/label  Status
10.110.0.10 229 [7334]  255        PO0/0:694       Tu4000:694      active
10.110.0.10 228 [7332]  254        PO0/0:693       Tu4000:693      active
10.110.0.10 227 [7331]  253        PO0/0:692       Tu4000:692      active
10.110.0.10 226 [7334]  252        PO0/0:691       Tu4000:691      active
10.110.0.10 225 [7333]  251        PO0/0:690       Tu4000:690      active
10.110.0.10 224 [7329]  250        PO0/0:689       Tu4000:689      active
```

Examples

The following example shows MPLS TE P2MP information as part of the command output.

```
Router> show mpls traffic-eng fast-reroute database

P2P Headend FRR information:
Protected tunnel               In-label Out intf/label   FRR intf/label   Status
---------------------------    -------- --------------   --------------   ------
Tunnel1                        Tun hd   Et0/1:20         Tu777:20         ready
P2P LSP midpoint frr information:
LSP identifier                 In-label Out intf/label   FRR intf/label   Status
---------------------------    -------- --------------   --------------   ------
P2MP Sub-LSP FRR information:
Sub-LSP identifier
```

```
src_lspid[subid]->dst_tunid    In-label Out intf/label   FRR intf/label   Status
---------------------------    -------- --------------   --------------   ------
10.1.1..201_1[1]->10.1.1..203_22   Tun hd   Et0/0:20         Tu666:20         ready
10.1.1..201_1[2]->10.1.1..206_22   Tun hd   Et0/0:20         Tu666:20         ready
10.1.1..201_1[3]->10.1.1..213_22   Tun hd   Et0/0:20         Tu666:20         ready
```

The table below describes the significant field shown in the display.

Table 13: show mpls traffic-eng fast-reroute database Point-to-Multipoint Field Descriptions

Field	Description
Sub-LSP identifier src_lspid[subid]->dst_tunid	The source and destination address of the sub-LSP being protected. The P2MP ID is appended to the source address. The tunnel ID is appended to the destination address.

The **detail** keyword provides more information about the P2MP LSPs:

```
Router# show mpls traffic-eng fast-reroute database detail

FRR Database Summary:
     Number of protected interfaces: 1
     Number of protected tunnels: 2
     Number of backup tunnels: 1
     Number of active interfaces: 0
P2MP Sub-LSPs:
   Tun ID: 1, LSP ID: 9, Source: 10.2.0.1
   Destination: 10.2.5.3, Subgroup ID: 19
   State        : Ready
   InLabel      : Tunnel Head
   OutLabel     : Se6/0:16
   FRR OutLabel : Tu100:16
```

Related Commands

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

show mpls traffic-eng fast-reroute log reroutes

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

show mpls traffic-eng fast-reroute log reroutes

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User EXEC

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was implemented on the Catalyst 6000 series with the SUP720 processor.
12.2(28)SB	This command was implemented on the Cisco 10000(PRE-2) router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

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

```
Router# show mpls traffic-eng fast-reroute log reroutes
When      Interface  Event   Rewrites  Duration  CPU msecs  Suspends  Errors
00:27:39  PO0/0      Down    1079      30 msecs  30         0         0
00:27:35  PO0/0      Up      1079      40 msecs  40         0         0
```

The table below describes significant fields shown in the display.

Table 14: show mpls traffic-eng fast-reroute log reroutes Field Descriptions

Field	Description
When	Indicates how long ago the logged event occurred (before this line was displayed on your screen). Displayed as hours, minutes, seconds.
Interface	The physical or tunnel interface where the logged event occurred.

Field	Description
Event	The change to Up or Down by the affected interface.
Rewrites	Total number of reroutes accomplished because of this event.
Duration	Time elapsed during the rerouting process, in milliseconds.
CPU msecs	CPU time spent processing those reroutes, in milliseconds. (This is less than or equal to the Duration value).
Suspends	Number of times that reroute processing for this event was interrupted to let the CPU handle other tasks.
Errors	Number of unsuccessful reroute attempts.

show mpls traffic-eng forwarding-adjacency

To display traffic engineering (TE) tunnels that are advertised as links in an Interior Gateway Protocol (IGP) network, use the **show mpls traffic-eng forwarding-adjacency** command in user EXEC or privileged EXEC mode.

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

Syntax Description

ip-address	(Optional) Destination address for forwarding adjacency tunnels.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.0(16)ST	This command was integrated into Cisco IOS Release 12.0(16)ST.
12.2(18)S	This command was integrated into Cisco IOS Release 2.2(18)S.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show mpls traffic-eng forwarding-adjacency** command to display information about tunnels configured with the **tunnel mpls traffic-eng forwarding-adjacency** command.

Examples

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

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

Related Commands

Command	Description
debug mpls traffic-eng forwarding-adjacency	Displays debug messages for traffic engineering forwarding adjacency events.
tunnel mpls traffic-eng forwarding-adjacency	Advertises a TE tunnel as a link in an IGP network.

show mpls traffic-eng forwarding path-set

To display the sublabel switched paths (sub-LSPs) that originate from the headend router, use the **show mpls traffic-eng forwarding path-set** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng forwarding path-set [**brief**| **detail**]

Syntax Description

brief	(Optional) Displays information about the sub-LSPs in a table format.
detail	(Optional) Displays detailed information about the sub-LSPs.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Examples

The following example displays information about the sub-LSPs in a summary format, including the number of sub-LSPs and the number of paths from the headend router.

```
Router> show mpls traffic-eng forwarding path-set

ID       Input I/F  LSPID  InLabel  PathCnt  subLSPCnt
----     ---------  -----  -------  -------  ---------
9F000001 Tu22       1      none     2        6
```

The following example shows six sub-LSPs originating at the headend router and going to different destinations. All the sub-LSPs belong to the same path set, which is a collection of paths. The path set is given a unique ID, which is shown in the PSID column of the example:

```
Router# show mpls traffic-eng forwarding path-set brief
Sub-LSP Identifier
src_lspid[subid]->dst_tunid              InLabel Next Hop      I/F    PSID
--------------------------               ------- ------------- ------ ----
10.1.1.201_1[1]->10.1.1.203_22             none    10.0.0.205    Et0/0  9F000001
10.1.1.201_1[2]->10.1.1.206_22             none    10.0.0.205    Et0/0  9F000001
10.1.1.201_1[3]->10.1.1.213_22             none    10.0.0.205    Et0/0  9F000001
10.1.1.201_1[4]->10.1.1.214_22             none    10.0.1.202    Et0/1  9F000001
10.1.1.201_1[5]->10.1.1.216_22             none    10.0.1.202    Et0/1  9F000001
10.1.1.201_1[6]->10.1.1.217_22             none    10.0.1.202    Et0/1  9F000001
```

The **show mpls traffic-eng forwarding path-set detail** command shows more information about the sub-LSPs that originate from the headend router. For example:

```
Router# show mpls traffic-eng forwarding path-set detail
LSP: Source: 10.1.0.1, TunID: 100, LSPID: 7
  Destination: 10.2.0.1, P2MP Subgroup ID: 1
```

```
    Path Set ID: 0x30000001
    OutLabel : Serial2/0, 16
    Next Hop : 10.1.3.2
    FRR OutLabel : Tunnel666, 16
  LSP: Source: 10.1.0.1, TunID: 100, LSPID: 7
  Destination: 10.3.0.1, P2MP Subgroup ID: 2
    Path Set ID: 0x30000001
    OutLabel : Serial2/0, 16
    Next Hop : 10.1.3.2
    FRR OutLabel : Tunnel666, 16
```

The table below describes the significant fields shown in the display.

Table 15: show mpls traffic-eng forwarding path-set Field Descriptions

Field	Description
ID	Path set ID.
Input I/F	The ID assigned to the tunnel that the sub-LSPs use.
LSPID	Sub-LSP ID.
InLabel	MPLS label in the input interface.
PathCnt	Number of paths from the headend router.
subLSPCnt	Number of sub-LSPS from the headend router.
Sub-LSP Identifier src_lspid[subid]->dst_tunid	The source and destination address of the sub-LSP being protected. The P2MP ID is appended to the source address. The tunnel ID is appended to the destination address.
Next Hop	Next-hop router.
I/F	The interface that the sub-LSPs use.
PSID	Path set ID.
Source	IP address of the headend router.
TunID	The ID assigned to the tunnel that the sub-LSPs use.
Destination	IP address of the destination router.
P2MP Subgroup ID	A consecutive number assigned to each sub-LSP.
Path Set ID	Path set ID.
OutLabel	The interface from which the label exits and the MPLS label that exits the interface.
FRR OutLabel	The tunnel from which the label exits and the MPLS label that exits the tunnel.

Related Commands

Command	Description
ip path-option	Species an explicit or dynamic path option for a particular destination address in a destination list

show mpls traffic-eng forwarding statistics

To display information about Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-pultipoint (P2MP) paths and sublabel switched paths (sub-LSPs), use the **show mpls traffic-eng forwarding statistics** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng forwarding statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Examples

The following example displays information about MPLS TE P2MP paths and sub-LSPs:

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

TE P2MP:
Statistics:
    Path Set Creation:            2
    Path Set Deletion:            0
    Input Label Allocation for Path Sets:  2
    Input Label Free:             0
    Current Label Allocated:      2
    PSI Nodes Allocated:          2
    PSI Nodes Freed:              0
    Add sub-LSP to Path Set:      5
    Delete sub-LSP from Path Set  0 (prune: 0, flush: 0)
    Update Path for FRR:          4
  Failures:
    None
```

The table below describes the significant fields shown in the display.

Table 16: show mpls traffic-eng forwarding statistics Field Descriptions

Field	Description
Path Set Creation	Number of path sets created.
Path Set Deletion	Number of path sets deleted.
Input Label Allocation for Path Sets	Number of input labels allocated for the path sets.
Input Label Free	Number of free input labels.
Current Label Allocated	Number of labels allocated for forwarding.

Field	Description
PSI Nodes Allocated	Number of path set nodes allocated.
PSI Nodes Freed	Number of path set nodes freed
Add sub-LSP to Path Set	Number of sub-LSPs in the path set.
Delete sub-LSP from Path Set	Number of sub-LSPs removed from the path set, either by pruning or flushing.
Update Path for FRR	Number of paths updated for fast reroute.
Failures	Number of path set failures

Related Commands

Command	Description
show mpls traffic-eng forwarding path-set	Display the sub-LSPs that originate from the headend router.

show mpls traffic-eng link-management admission-control

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

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

Syntax Description

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

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output changed. The BW field now shows bandwidth in kBps, and it is followed by the status (reserved or held) of the bandwidth.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

```
Router # show mpls traffic-eng link-management admission-control
System Information::
    Tunnels Count:       4
    Tunnels Selected:    4
TUNNEL ID              UP IF     DOWN IF  PRIORITY STATE           BW (kbps)
10.106.0.6 1000_1      AT1/0.2   -        0/0      Resv Admitted   0
10.106.0.6 2000_1      Et4/0/1   -        1/1      Resv Admitted   0
10.106.0.6 1_2         Et4/0/1   Et4/0/2  1/1      Resv Admitted   3000       R
10.106.0.6 2_2         AT1/0.2   AT0/0.2  1/1      Resv Admitted   3000       R
```

The table below describes the significant fields shown in the display.

Table 17: show mpls traffic-eng link-management admission-control Field Descriptions

Field	Description
Tunnels Count	Total number of tunnels admitted.
Tunnels Selected	Number of tunnels to be displayed.
TUNNEL ID	Tunnel identification.
UP IF	Upstream interface that the tunnel used.
DOWN IF	Downstream interface that the tunnel used.
PRIORITY	Setup priority of the tunnel followed by the hold priority.
STATE	Admission status of the tunnel.
BW (kbps)	Bandwidth of the tunnel (in kBps). If an “R” follows the bandwidth number, the bandwidth is reserved. If an “H” follows the bandwidth number, the bandwidth is temporarily being held for a path message.

Related Commands

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

show mpls traffic-eng link-management advertisements

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

show mpls traffic-eng link-management advertisements

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The output was enhanced to show Internet Gateway Protocol (IGP) recovery status provided by the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Examples

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

```
Router# show mpls traffic-eng link-management advertisements
Flooding Status:     ready
Configured Areas:    1
IGP Area[1] ID:: isis level-1
  System Information::
    Flooding Protocol:   ISIS
  Header Information::
    IGP System ID:       0001.0000.0001.00
    MPLS TE Router ID:   10.106.0.6
    Flooded Links:       1
  Link ID:: 0
    Link IP Address:     10.1.0.6
    IGP Neighbor:        ID 0001.0000.0001.02
    Admin. Weight:       10
    Physical Bandwidth:  10000 kbits/sec
    Max Reservable BW:   5000 kbits/sec
    Downstream::
      Reservable Bandwidth[0]:       5000 kbits/sec
```

```
    Reservable Bandwidth[1]:       2000 kbits/sec
    Reservable Bandwidth[2]:       2000 kbits/sec
    Reservable Bandwidth[3]:       2000 kbits/sec
    Reservable Bandwidth[4]:       2000 kbits/sec
    Reservable Bandwidth[5]:       2000 kbits/sec
    Reservable Bandwidth[6]:       2000 kbits/sec
    Reservable Bandwidth[7]:       2000 kbits/sec
  Attribute Flags:     0x00000000
```

The table below describes the significant fields shown in the display.

Table 18: show mpls traffic-eng link-management advertisements Field Descriptions

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

The following is sample output from the **show mpls traffic-eng link-management advertisements** command with the enhanced output, which shows the "IGP recovering" status, from the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature:

```
Router# show mpls traffic-eng link-management advertisements
show mpls traffic-eng link-management advertisements
Flooding Status:      ready (IGP recovering)
Configured Areas:     1
IGP Area[1] ID::  ospf  area nil
  System Information::
    Flooding Protocol:    OSPF
  Header Information::
```

The table below describes the significant fields shown in the display.

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

Field	Description
Flooding Status	Status of the link management flooding system. The notation (IGP recovering) indicates that flooding cannot be determined because an IP routing process restart is in progress.
Configured Areas	Number of the IGP areas configured.

Related Commands

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

show mpls traffic-eng link-management bandwidth-allocation

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

show mpls traffic-eng link-management bandwidth-allocation [summary] [*interface-type interface-number*]

Syntax Description

summary	(Optional) Displays summary of bandwidth allocation.
interface-type interface-number	(Optional) The specified interface that admitted tunnels.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was modified. The **summary** *interface-name interface-number* keyword and argument combination was added.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

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

Examples

Examples

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

```
Router# show mpls traffic-eng link-management bandwidth-allocation gigabitEthernet 4/0/1
System Information::
    Links Count:         2
    Bandwidth Hold Time: max. 15 seconds
Link ID:: Ge4/0/1 (10.1.0.6)
```

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

The table below describes the significant fields shown in the display.

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

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

Field	Description
KEEP PRIORITY	Priority levels for the link's bandwidth allocations.
BW HELD	Amount of bandwidth (in kBps) temporarily held at this priority for path messages.
BW TOTAL HELD	Bandwidth held at this priority and those above it.
BW LOCKED	Amount of bandwidth reserved at this priority.
BW TOTAL LOCKED	Bandwidth locked at this priority and those above it.

Examples

The following is sample output from the **show mpls traffic-eng link-management bandwidth-allocation summary** command for all the configured interfaces:

```
Router# show mpls traffic-eng link-management bandwidth-allocation summary
  interface     Intf Max    Intf Avail  Sub Max     Sub Avail
                kbps        kbps        kbps        kbps
  Et0/0         47000       42500       42000       40500
  Et1/0         7500        7500        0           0
```

The table below describes the significant fields shown in the display.

Table 21: show mpls traffic-eng link-management bandwidth-allocation summary Field Descriptions

Field	Description
interface	Name of the interface.
Intf Max	Maximum amount of bandwidth, in kbps, available on the interface.
Intf Avail	Amount of bandwidth, in kbps, currently available on the interface.
Sub Max	Maximum amount of bandwidth, in kbps, available in the subpool.
Sub Avail	Amount of bandwidth, in kbps, currently available in the subpool.

Examples

The following is sample output from the **show mpls traffic-eng link-management bandwidth-allocation summary** command for one configured interface:

```
Router# show mpls traffic-eng link-management bandwidth-allocation summary Ethernet 0/0
interface     Intf Max    Intf Avail  Sub Max     Sub Avail
                kbps        kbps        kbps        kbps
  Et0/0         47000       42500       42000       40500
```

See the table above for an explanation of the fields.

Examples

The following is sample output from the **show mpls traffic-eng link-management bandwidth-allocation summary** command for all the configured interfaces:

```
Router# show mpls traffic-eng link-management bandwidth-allocation summary
  interface     Intf Max    BC0 Max     BC0 Avail   BC1 Max     BC1 Avail
                kbps        kbps        kbps        kbps        kbps
  Et0/0         45000       40000       37000       30000       28500
  Et1/0         0           0           0           0           0
```

The table below describes the significant fields shown in the display.

Table 22: show mpls traffic-eng link-management bandwidth-allocation summary Field Descriptions

Field	Description
interface	Name of the interface.
Intf Max	Maximum amount of bandwidth, in kbps, available on the interface.
BC0 Max	Maximum amount of bandwidth, in kbps, available in the global pool.
BC0 Avail	Amount of bandwidth, in kbps, currently available in the global pool.
BC1 Max	Maximum amount of bandwidth, in kbps, available in the subpool.
BC1 Avail	Amount of bandwidth, in kbps, currently available in the subpool.

Related Commands

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

show mpls traffic-eng link-management igp-neighbors

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

show mpls traffic-eng link-management igp-neighbors [*interface-type number*| **igp-id** {**isis** *isis-address*| **ospf** *ospf-id*}| **ip** *ip-address*]

Syntax Description

interface-type number	(Optional) Specifies the interface type and number for which the IGP neighbors are displayed.
igp-id	(Optional) Displays the IGP neighbors that are using a specified IGP identification.
isis *isis-address*	(Optional) Displays the specified IS-IS neighbor when you display neighbors by IGP ID.
ospf *ospf-id*	(Optional) Displays the specified OSPF neighbor when you display neighbors by IGP ID.
ip *ip-address*	(Optional) Displays the IGP neighbors that are using a specified IGP IP address.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The *interface-type* and *number* arguments were added.

Examples

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

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

Link ID::  Et0/2
    Neighbor ID:  0000.0024.0004.02 (area: isis level-1, IP: 10.0.0.0)
Link ID::  PO1/0/0
    Neighbor ID:  0000.0026.0001.00 (area: isis level-1, IP: 172.16.1.2)
```

The table below describes the significant fields shown in the display.

Table 23: show mpls traffic-eng link-management igp-neighbors Field Descriptions

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

Related Commands

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

show mpls traffic-eng link-management interfaces

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

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

Syntax Description

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

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.
12.2(28)SB	The command output was enhanced to display the Shared Risk Link Group (SRLG) membership of links.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

Use this command to display resource and configuration information for all configured interfaces.

Examples

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

```
Router# show mpls traffic-eng link-management interfaces Et4/0/1
System Information::
    Links Count:         2
Link ID:: Et4/0/1 (10.1.0.6)
    Link Status:
      Physical Bandwidth:  10000 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 60% out)
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   reject-huge
```

```
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  1
      IGP Neighbor:        ID 0001.0000.0001.02, IP 10.0.0.0 (Up)
      Flooding Status for each configured area [1]:
      IGP Area[1]: isis level-1: flooded
```

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

```
Router# show mpls traffic-eng link-management interfaces pos3/1
System Information::
    Links Count:         11
Link ID:: PO3/1 (10.0.0.33)
    Link Status:
      SRLGs:               1 2
      Physical Bandwidth:  2488000 kbits/sec
      Max Res Global BW:   20000 kbits/sec (reserved:0% in, 0% out)
      Max Res Sub BW:      5000 kbits/sec (reserved:0% in, 0% out)
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   allow-all
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  1
      IGP Neighbor:        ID 0000.0000.0004.00, IP 10.0.0.34 (Up)
      Flooding Status for each configured area [1]:
      IGP Area[1]: isis level-2: flooded
```

The table below describes the significant fields shown in the displays.

Table 24: show mpls traffic-eng link-management interfaces Field Descriptions

Field	Description
Links Count	Number of links that were enabled for use with Multiprotocol Label Switching (MPLS) traffic engineering.
Link ID	Index of the link.
SRLGs	The SRLGs to which the link belongs.
Physical Bandwidth	Link's bandwidth capacity, in kBps.
Max Reservable BW	Amount of reservable bandwidth, in kb/s, on this link.
Max Res Global BW	Amount of reservable bandwidth, in kb/s, available for the global pool.
Max Res Sub BW	Amount of reservable bandwidth, in kb/s, available for the subpool.
MPLS TE Link State	The status of the MPLS link.
Inbound Admission	Link admission policy for inbound tunnels.
Outbound Admission	Link admission policy for outbound tunnels.
Admin. Weight	Administrative weight associated with this link.

Field	Description
IGP Neighbor Count	Number of Interior Gateway Protocol (IGP) neighbors directly reachable over this link.
IGP Neighbor	IGP neighbor on this link.
Flooding Status for each configured area	Flooding status for the specified configured area.

Related Commands

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

show mpls traffic-eng link-management summary

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

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

Syntax Description

interface-name	Specific interface for which information will be displayed.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The output was enhanced to display Internet Gateway Protocol (IGP) recovery status provided by the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature.

Examples

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

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

```
      IGP Neighbor Count:  1
Link ID:: AT0/0.2 (10.42.0.6)
    Link Status:
      Physical Bandwidth:  155520 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 0% out)
      MPLS TE Link State:  MPLS TE on, RSVP on
      Inbound Admission:   allow-all
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  0
```

The table below describes the significant fields shown in the display.

Table 25: show mpls traffic-eng link-management summary Field Descriptions

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

Field	Description
Admin. Weight	Link administrative weight.
IGP Neighbor Count	List of the IGP neighbors directly reachable over this link.

The following is sample output from the **show mpls traffic-eng link-management summary** command with the enhanced output, which shows the "IGP recovering" status, from the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature:

```
Router# show mpls traffic-eng link-management summary
System Information::
    Links Count:          3
    Flooding System:      enabled (IGP recovering)
IGP Area ID::  ospf  area nil
    Flooding Protocol:    OSPF
    Flooding Status:      data flooded
    Periodic Flooding:    enabled (every 180 seconds)
    Flooded Links:        0
```

The table below describes the significant fields shown in the display.

Table 26: show mpls traffic-eng link-management summary Field Descriptions

Field	Description
Links Count	Number of links configured for MPLS traffic engineering.
Flooding System	Status of the MPLS traffic engineering flooding system. The notation (IGP recovering) indicates that status cannot be determined because an IP routing process restart is in progress.
IGP Area ID	Name of the IGP area being described.
Flooding Protocol	IGP being used to flood information for this area.
Flooding Status	Status of flooding for this area.
Periodic Flooding	Status of periodic flooding for this area.
Flooded Links	Number of links that were flooded.

Related Commands

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

show mpls traffic-eng lsp attributes

To display global label switched path (LSP) attribute lists, use the **show mpls traffic-eng lsp attributes** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng lsp attributes [**name** *string*] **[internal]**

Syntax Description

name	(Optional) Identifies a specific LSP attribute list.
string	Describes the string argument.
internal	(Optional) Displays LSP attribute list internal information.

Command Default

If no keywords or arguments are specified, all LSP attribute lists are displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use this command to display information about all LSP attribute lists or a specific LSP attribute list.

Examples

The following example shows output from the **show mpls traffic-eng lsp attributes** command :

```
Router# show mpls traffic-eng lsp attributes
LIST list1
    affinity 0xFF mask 0xFFFFFFFF
    auto-bw collect-bw
    bandwidth 12
    protection fast-reroute bw-protect
    lockdown
    priority 2 2
    record-route LIST 2
```

```
   bandwidth 5000
LIST hipriority
  priority 0 0
!
```

The table below describes the significant fields shown in the display.

Table 27: show mpls traffic-eng lsp attributes Field Descriptions

Field	Description
LIST	Identifies the LSP attribute list.
affinity	Indicates the LSP attribute that specifies attribute flags for LSP links. Values are 0 or 1.
mask	Indicates which attribute values should be checked.
auto-bw collect-bw	Indicates automatic bandwidth configuration.
protection fast re-route bw-protect	Indicates that the failure protection is enabled.
lockdown	Indicates that the reoptimization for the LSP is disabled.
priority	Indicates the LSP attribute that specifies LSP priority.
record-route	Indicates the record of the route used by the LSP.
bandwidth	Indicates the LSP attribute that specifies LSP bandwidth.

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.

show mpls traffic-eng nsr

To display configuration information for Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Nonstop Routing (NSR) support, use the **show mpls traffic-eng nsr** command in privileged EXEC mode.

show mpls traffic-eng nsr [**counters** | **database** {**if-autotun** | **internal** | **lsp-ac** | **lsp-frr** | **lsp-head filter** {**destination** | **lsp-id** | **source** | **tunnel-id**} | **pcalc** {**auto-mesh** | **nbr** | **node** | **srlg**} | **summary** | **tun-setup**} | **oos** | **summary**]

Syntax Description

counters	(Optional) Displays information about the data structures or states that are successfully created or removed, along with errors counts.
database	(Optional) Displays information about write and read databases supporting MPLS TE NSR.
if-autotun	Displays information about the MPLS TE NSR auto-tunnel interfaces.
internal	Displays detailed information about MPLS TE NSR.
lsp-ac	Displays information about the admission control functionality of label switched paths (LSPs).
lsp-frr	Displays information about the Fast Reroute (FRR) functionality of LSPs.
lsp-head	Displays information about LSPs at the head end.
filter	Displays information about the FRR functionality of LSP filter options.
destination	Displays LSP information filtered by the destination address of the tunnel.
lsp-id	Displays LSP information filtered by the LSP ID of the source port.
source	Displays LSP information filtered by the source address of the tunnel.

tunnel-id	Displays LSP information filtered by the tunnel ID.
pcalc	Displays information about the MPLS TE NSR topology database.
auto-mesh	Displays information for the auto-mesh topologies in the database.
nbr	Displays information for the neighbor topologies in the database.
node	Displays information for the topology nodes in the database.
srlg	Displays information for the topology of the Shared Risk Link Group (SRLG).
tune-setup	Displays options to configure the tunnel path setup.
oos	(Optional) Displays information about the out-of-sync databases supporting MPLS TE NSR.
summary	(Optional) Displays a summary of MPLS TE NSR information such as the current TE NSR state (standby-hot / recovering / staling / active), recovery time, and the recovery result (success / failure).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS Release XE 3.10S	This command was introduced.

Usage Guidelines

The write and read databases store the data that is used for recovering TE states on a standby device after Stateful Switchover (SSO).

The out of sync databases indicate the devices whose states are not in sync with each other.

Examples

The following example shows how to view information about the data structures or states that are successfully created or removed, along with errors counts:

```
enable
 show mpls traffic-eng nsr counters

State: Active

Bulk sync
  Last bulk sync was successful (entries sent: 24)
  initiated: 1

Send timer
  started: 7

Checkpoint Messages (Items) Sent
  Succeeded:      13  (101)
    Acks accepted:13  (101)
    Acks ignored:     (0)
    Nacks:        0  (0)
  Failed:         0  (0)
  Buffer alloc:   13
  Buffer freed:   13

ISSU:
  Checkpoint Messages Transformed:
    On Send:
      Succeeded:         13
      Failed:            0
      Transformations:   0
    On Recv:
      Succeeded:         0
      Failed:            0
      Transformations:   0

  Negotiation:
    Started:              1
    Finished:             1
    Failed to Start:      0
    Messages:
      Sent:
        Send succeeded:   5
        Send failed:      0
        Buffer allocated:        5
        Buffer freed:            0
        Buffer alloc failed:     0
      Received:
        Succeeded:        7
        Failed:           0
        Buffer freed:     7
  Init:
    Succeeded:            1
    Failed:               0

  Session Registration:
    Succeeded:            0
    Failed:               0

  Session Unregistration:
    Succeeded:            0
    Failed:               0

Errors:
  None
```

The following table shows the significant fields shown in the display.

Table 28: show mpls traffic-eng nsr counters Field Descriptions

Field	Description
Bulk sync	Specifies the status of the counters' last bulk synchronization attempt.
Send timer	Specifies the time lapse since the timer that counts the sent entries was started.
Checkpoint Messages	Specifies the information about the error checkpoint messages, such as the number of the messages sent, number of acknowledgments received, number of messages that failed to reach, and the buffer status.
ISSU	Specifies information about the Cisco IOS In-Service Software Upgrade (ISSU) clients, such as the checkpoint message status, negotiation message status, session registration, and so on.
Errors	Lists errors encountered during checkpointing and negotiations.

Examples

The following example shows how to view internal information pertaining to the write and read databases supporting MPLS TE NSR:

```
Device# show mpls traffic-eng nsr database internal

Write DB:
                  Checkpointed
   Entry Type       or Ack-Pending  Send-Pending
     PCALC Node                  0             0
     PCALC Link                  0             0
     PCALC Auto-Mes              0             0
     PCALC SRLG                  0             0
     lm_tunnel_t                 0             0
     NSR LSP FRR                 0             0
     nsr_if_autotun              0             0
     nsr_tspvif_set              0             0
     nsr_slsp_head               0             0

Read DB:
   Entry Type        Checkpointed
     PCALC Node                 5
     PCALC Link                12
     PCALC Auto-Mesh            0
     PCALC SRLG                 0
     lm_tunnel_t                5
     NSR LSP FRR                0
     nsr_if_autotun             0
     nsr_tspvif_setup           3
     nsr_slsp_head              5

TE NSR Sequence Bulk Sync List:
Entries: 0; next avail seq num: 132

TE NSR Sequence State Creation List:
```

```
Entries: 30; next expected seq num: 132
   Seq Num: 7  EntryPtr: 0x5A03B208
     Type: PCALC Node  Action: Add  Bundle Seq #: 1
   Seq Num: 8  EntryPtr: 0x5A0B8B38
     Type: PCALC Link  Action: Add  Bundle Seq #: 2
   Seq Num: 9  EntryPtr: 0x5A0B8DA0
     Type: PCALC Link  Action: Add  Bundle Seq #: 2
   Seq Num: 10  EntryPtr: 0x59FF1BB0
     Type: PCALC Node  Action: Add  Bundle Seq #: 1
   Seq Num: 11  EntryPtr: 0x5A0B9008
     Type: PCALC Link  Action: Add  Bundle Seq #: 2
   Seq Num: 32  EntryPtr: 0x586F2A50
     Type: PCALC Node  Action: Add  Bundle Seq #: 4
   Seq Num: 33  EntryPtr: 0x5949FC58
     Type: PCALC Link  Action: Add  Bundle Seq #: 5
   Seq Num: 34  EntryPtr: 0x5949FEC0
     Type: PCALC Link  Action: Add  Bundle Seq #: 5
   Seq Num: 60  EntryPtr: 0x5725BC30
     Type: lm_tunnel_t  Action: Add  Bundle Seq #: 12
   Seq Num: 61  EntryPtr: 0x5725BE00
     Type: nsr_tspvif_setup  Action: Add  Bundle Seq #: 12
   Seq Num: 62  EntryPtr: 0x59FC9E80
     Type: nsr_slsp_head  Action: Add  Bundle Seq #: 12
   Seq Num: 79  EntryPtr: 0x59296190
     Type: lm_tunnel_t  Action: Add  Bundle Seq #: 16
   Seq Num: 80  EntryPtr: 0x59296360
     Type: nsr_tspvif_setup  Action: Add  Bundle Seq #: 16
   Seq Num: 81  EntryPtr: 0x571EB7F8
     Type: nsr_slsp_head  Action: Add  Bundle Seq #: 16
   Seq Num: 98  EntryPtr: 0x5A04B770
     Type: lm_tunnel_t  Action: Add  Bundle Seq #: 20
   Seq Num: 99  EntryPtr: 0x59296108
     Type: nsr_tspvif_setup  Action: Add  Bundle Seq #: 20
   Seq Num: 100  EntryPtr: 0x57258670
     Type: nsr_slsp_head  Action: Add  Bundle Seq #: 20
   Seq Num: 101  EntryPtr: 0x5A060348
     Type: lm_tunnel_t  Action: Add  Bundle Seq #: 20
   Seq Num: 102  EntryPtr: 0x5A03B2B0
     Type: nsr_slsp_head  Action: Add  Bundle Seq #: 20
   Seq Num: 103  EntryPtr: 0x5B1F12B0
     Type: lm_tunnel_t  Action: Add  Bundle Seq #: 20
   Seq Num: 104  EntryPtr: 0x5A03B400
     Type: nsr_slsp_head  Action: Add  Bundle Seq #: 20
   Seq Num: 121  EntryPtr: 0x57258358
     Type: PCALC Node  Action: Add  Bundle Seq #: 21
   Seq Num: 122  EntryPtr: 0x59FAF080
     Type: PCALC Link  Action: Add  Bundle Seq #: 22
   Seq Num: 123  EntryPtr: 0x59502AC0
     Type: PCALC Link  Action: Add  Bundle Seq #: 23
   Seq Num: 124  EntryPtr: 0x594AE918
     Type: PCALC Link  Action: Add  Bundle Seq #: 21
   Seq Num: 125  EntryPtr: 0x59502120
     Type: PCALC Link  Action: Add  Bundle Seq #: 23
   Seq Num: 126  EntryPtr: 0x59FAFA20
     Type: PCALC Link  Action: Add  Bundle Seq #: 22
   Seq Num: 129  EntryPtr: 0x59FC9CC0
     Type: PCALC Node  Action: Add  Bundle Seq #: 24
   Seq Num: 130  EntryPtr: 0x5A060518
     Type: PCALC Link  Action: Add  Bundle Seq #: 24
   Seq Num: 131  EntryPtr: 0x59FAFC88
     Type: PCALC Link  Action: Add  Bundle Seq #: 24
```

The following table shows the significant fields shown in the display.

Table 29: show mpls traffic-eng nsr database Field Descriptions

Field	Description

Write DB	Specifies information about the write databases.
Read DB	Specifies information about the read databases
TE NSR Sequence Bulk Sync List	Specifies information about the sequence of the databases queued up in the list for bulk synchronization. The information includes the number of entries lined up and the next available sequence number.
TE NSR Sequence State Creation List	Specifies information about the list of sequence states being created.

Examples

The following example shows how to verify information pertaining to the out-of-sync databases supporting MPLS TE NSR:

```
enable
 show mpls traffic-eng nsr oos
  Tunnel: 4000
  Time created: 02/20/13-12:03:13
  Time synced: 02/20/13-12:03:14
  Key:
    Source:                    10.1.0.1
    Destination:               10.2.0.1
    ID:                        4000
    Ext Tun ID:                10.1.0.1
    Instance:                  4
    Slsp p2mp ID:              0
    Slsp p2mp subgroup ID:     0
    Slsp p2mp subgroup origin: 0

  RSVP States:
    Signal:       Unknown
    Fast-Reroute: Disabled
    Delete State: True

  TE States:
    Signal:       Unknown
    Fast-Reroute: Disabled
    Delete State: True

  Update History:
    Total number of updates: 2

      Update Time: 02/20/13-12:03:13
        Client Updating: RSVP
        Update State:
          Signal:       Unknown
          Fast-Reroute: Unknown
          Delete State: True

      Update Time: 02/20/13-12:03:14
        Client Updating: TE
        Update State:
          Signal:       Unknown
          Fast-Reroute: Unknown
          Delete State: True
```

The following table shows the significant fields shown in the display.

Table 30: show mpls traffic-eng nsr oos Field Descriptions

Field	Description
Key	Specifies information such as the source address, destination address, tunnel ID, database instance, LSP origin, and so on, of the out-of-sync databases.
RSVP States	Specifies information about the Resource Reservation Protocol (RSVP) states of the out-of-sync databases.
TE States	Specifies information about the TE states of the out-of-sync databases.
Update History	Specifies information about the update log of the out of sync databases. The information includes the update time, the client that is getting updated, and the state of the update (Signal/Fast-Reroute/Deletion).

Examples

The following example shows how to view a summary of MPLS TE NSR information:

```
enable
 show mpls traffic-eng nsr summary
  State:
  Graceful-Restart: Disabled
  HA state: Active
  Checkpointing: Allowed
  Messages:
   Send timer: not running (Interval: 1000 msec)
   Items sent per Interval: 200
   CF buffer size used: 3968
```

The following table shows the significant fields shown in the display.

Table 31: show mpls traffic-eng nsr summary Field Descriptions

Field	Description
State	Specifies information, if any, about the state of the write and read databases and the out of sync databases.
Graceful-Restart	Specifies information on whether Graceful Restart (GR) is Enabled or Disabled.
HA State	Specifies information about the MPLS high-availability states of the databases.
Checkpointing	Specifies information on whether checkpointing is allowed or prohibited.

Messages	Specifies different summary messages of the databases. The information displayed includes the send timer count, the number of items sent per interval, and the buffer size of the Checkpoint Facility (CF).

Related Commands

Command	Description
mpls traffic-eng nsr	Enables MPLS TE NSR support for a device.

show mpls traffic-eng process-restart iprouting

To display the status of IP routing and Multiprotocol Label Switching (MPLS) traffic engineering synchronization after an IP routing process restart, use the **show mpls traffic-eng process-restart iprouting** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng process-restart iprouting

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

This command displays information about the synchronization between the IP routing process and MPLS TE that you can provide to your technical support representative when you are reporting a problem.

All counters are set to zero when the system process initializes and are not reset no matter how often the IP routing process restarts.

The following is sample output from the **show mpls traffic-eng process-restart iprouting** command when an IP routing process has restarted normally:

```
Router# show mpls traffic-eng process-restart iprouting
IP Routing Restart Statistics:
  Current State: NORM
  Flushing State: IDLE
State Entered       Count     Timestamp            Timestamp            Timestamp
INIT                1         05/10/06-13:07:01
NORM                3         05/10/06-13:07:10    05/10/06-13:10:45   05/10/06-13:11:5
NORM-SPCT           0
AWAIT-CFG           2         05/10/06-13:10:32    05/10/06-13:11:45
CFG                 2         05/10/06-13:10:32    05/10/06-13:11:45
CMPL-FLSH           0
NCMPL-FLSH          2         05/10/06-13:10:32    05/10/06-13:11:45
NCMPL-FLSHD         2         05/10/06-13:10:32     05/10/06-13:11:45
Stuck State         Count     Timestamp             Timestamp          Timestamp
No Stuck states encountered
Counter             Count     Timestamp             Timestamp          Timestamp
Reg Succeed         40       05/10/06-13:11:51      05/10/06-13:11:45  05/10/06-13:11:45
Reg Fail             0
Incarnation          5       05/10/06-13:11:45      05/10/06-13:11:45  05/10/06-13:10:37
Flushing             2        05/10/06-13:10:32      05/10/06-13:11:45
```

The table below describes the normal output of the significant fields shown in the display. You should contact your technical support representative if your display has values other than those described in the table.

Table 32: show mpls traffic-eng process-restart iprouting Field Descriptions

Field	Description
Current State	This indicates the restart status. NORM indicates that routing convergence has occurred and that TE and the Internet Gateway Protocols (IGPs) have synchronized.
Flushing State	This indicates the flushing state. It should indicate IDLE.
Stuck State	This indicates the stuck state. The Count column should indicate that no stuck state has been encountered.
Reg Fail	This indicates a registry failure. The Count column should indicate 0.

Related Commands

Command	Description
debug mpls traffic-eng process-restart	Displays information about process restarts for reporting to your technical support representative.

show mpls traffic-eng topology

To display the Multiprotocol Label Switching (MPLS) traffic engineering global topology as currently known at the node, use the **show mpls traffic-eng topology** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng topology [**area** *area-id*| **level-1**| **level-2**] [*ip-address* [**brief**| **internal**]| **igp-id** {**isis** *nsapaddr*| **ospf** *ip-address* [**network**| **router**]} **[brief]**| **srlg**]

Syntax Description

area	(Optional) Restricts output to an Open Shortest Path First (OSPF) area.
area-id	The OSPF area ID. The range is from 0 to 4294967295.
level-1	(Optional) Restricts output to a System-to-Intermediate System (IS-IS) level-1.
level-2	(Optional) Restricts output to an IS-IS level-2.
ip-address	(Optional) The node by the IP address (router identifier to interface address).
brief	(Optional) Provides a less detailed version of the topology.
internal	(Optional) Specifies to use the internal format.
igp-id	(Optional) Specifies the node by Interior Gateway Protocol (IGP) router identifier.
isis *nsapaddr*	Specifies the node by router identification if using Intermediate IS-IS.
ospf *ip-address*	Specifies the node by router identifier if using OSPF.
network	(Optional) Specifies the node type as network.
router	(Optional) Specifies the node type as router.
srlg	(Optional) Displays Shared Risk Link Groups (SRLG) membership for each link in a topology.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(11)ST	This command was modified. The single “Reservable” column was replaced by two columns: one each for “global pool” and for “subpool.”
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(28)SB	This command was modified. The **area**, **level-1**, and **level-2** keywords were added.
12.2(33)SRA	This command was modified and integrated into Cisco IOS Release 12.2(33)SRA. The **srlg** keyword was added.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Examples

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

```
Router# show mpls traffic-eng topology
My_System_id: 0000.0000.0001.00 (isis 1 level-2)
My_System_id: 10.10.10.10 (ospf 100 area 0)
My_BC_Model_Type: MAM
Signalling error holddown: 10 sec Global Link Generation 56
IGP Id: 0000.0000.0001.00, MPLS TE Id: 10.10.10.10 Router Node  (isis 1 level-2)
  Link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0002.00, Nbr Node Id:6, gen:56
      Frag Id:0, Intf Address:10.2.2.1, Intf Id:0
       Nbr Intf Address:10.2.2.2, Nbr Intf Id:0
      TE Metric:10, IGP Metric:10, Attribute Flags:0x0
      Switching Capability:, Encoding:
      BC Model ID:MAM
      Physical BW:155520 (kbps), Max Reservable BW:1000 (kbps)
      BC0:600 (kbps) BC1:400 (kbps)
                     Total Allocated   Reservable
                     BW (kbps)         BW (kbps)
                     ---------------   -----------
        TE-class[0]:            0            600
        TE-class[1]:            0            400
        TE-class[2]:            0              0
        TE-class[3]:            0              0
        TE-class[4]:            0            600
        TE-class[5]:            0            400
        TE-class[6]:            0              0
        TE-class[7]:            0              0
  Link[1]:Point-to-Point, Nbr IGP Id:0000.0000.0002.00, Nbr Node Id:6, gen:56
      Frag Id:0, Intf Address:10.1.1.1, Intf Id:0
       Nbr Intf Address:10.1.1.2, Nbr Intf Id:0
      TE Metric:10, IGP Metric:10, Attribute Flags:0x0
      Switching Capability:, Encoding:
      BC Model ID:MAM
      Physical BW:155520 (kbps), Max Reservable BW:1000 (kbps)
      BC0:600 (kbps) BC1:400 (kbps)
                     Total Allocated   Reservable
```

```
                BW (kbps)         BW (kbps)
                ---------------   -----------
TE-class[0]:              10            590
TE-class[1]:               0            400
TE-class[2]:               0              0
TE-class[3]:               0              0
TE-class[4]:               0            600
TE-class[5]:               0            400
TE-class[6]:               0              0
TE-class[7]:               0              0
```

The table below describes significant fields shown in the display.

Table 33: show mpls traffic-eng topology Field Descriptions

Field	Description
My_System_id	Unique identifier of the IGP.
My_BC_Model_Type: MAM	Bandwidth constraints model of the local node: either Maximum Allocation Model (MAM) or Russian Dolls Model (RDM).
Signalling error holddown:	Link hold-down timer configured to handle path error events to exclude link from topology.
IGP Id	Identification of the advertising router.
MPLS TE Id	Unique MPLS traffic engineering node identifier.
Intf Id:	Interface identifier.
Router Node	Type of node.
Nbr IGP Id	Neighbor IGP router identifier.
Intf Address	The interface address of the link.
Nbr Intf Address:	IP address of the neighbor interface.
BC Model ID:	Bandwidth Constraints Model ID: RDM or MAM.
gen	Generation number of the link-state packet (LSP). This internal number is incremented when any new LSP is received.
Frag Id	IGP link-state advertisement (LSA) fragment identifier.
TE Metric	TE cost of the link.
IGP Metric	IGP cost of the link.
Attribute Flags	The requirements on the attributes of the links that the traffic crosses.

Field	Description
Physical BW	Physical line rate.
Max Reservable BW	Maximum amount of bandwidth, in kilobits per second (kb/s), that can be reserved on a link.
Total Allocated	Amount of bandwidth, in kb/s, allocated at that priority.
Reservable	Amount of available bandwidth, in kb/s, reservable for that TE-Class for two pools: BC0 (formerly called “global”) and BC1 (formerly called “sub”).

Related Commands

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

show mpls traffic-eng topology path

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

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

Syntax Description

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

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.

Release	Modification
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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

Examples

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

```
Router # show mpls traffic-eng topology path Tunnel1 bandwidth 1000
Query Parameters:
  Destination:10.112.0.12
    Bandwidth:1000
   Priorities:1 (setup), 1 (hold)
     Affinity:0x0 (value), 0xFFFF (mask)
Query Results:
  Min Bandwidth Along Path:2000 (kbps)
  Max Bandwidth Along Path:5000 (kbps)
  Hop  0:10.1.0.6       :affinity 00000000, bandwidth 2000 (kbps)
  Hop  1:10.1.0.10      :affinity 00000000, bandwidth 5000 (kbps)
  Hop  2:10.43.0.10     :affinity 00000000, bandwidth 2000 (kbps)
  Hop  3:10.112.0.12
```

The table below describes the significant fields shown in the display.

Table 34: show mpls traffic-eng topology path Field Descriptions

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

show mpls traffic-eng tunnels

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

show mpls traffic-eng tunnels[[**attributes** *list-name*]| [**destination** *address*]| [**down**]| [**interface** *type number*]| [**name** *name*]| [**name-regexp** *reg-exp*]| [**property**{**auto-tunnel**{**backup**| **mesh**| **primary**}| **backup-tunnel**| **fast-reroute**}]| [**role**{**all**| **head**| **middle**| **remote**| **tail**}]| [**source-id**{*ipaddress*[*tunnel-id*]}]| [**suboptimal constraints**{**current**| **max**| **none**}]| [**statistics**]| [**summary**]| [**up**]]**accounting**| **backup**| **brief**| **protection**

Syntax Description

attributes *list-name*	(Optional) Restricts the display to tunnels that use a matching attributes list.
destination *address*	(Optional) Restricts the display to tunnels destined to the specified IP address.
down	(Optional) Displays tunnels that are not active.
interface	(Optional) Displays information for the specified interface.
type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
name *name*	(Optional) Displays the tunnel with the specified string. The tunnel string is derived from the interface description, if specified; otherwise, it is the interface name. The tunnel string is included in the signaling message so that it is available at all hops.
name-regexp *regexp*	(Optional) Displays tunnels whose descriptions match the specified regular expression.
property	(Optional) Displays tunnels with the specified property.
auto-tunnel	Displays information about autotunnels.

backup	Displays information about Fast Reroute (FRR) protection provided by each tunnel selected by other options specified with this command. The information includes the physical interface protected by the tunnel, the number of TE label switched packets (LSPs) (that is, tunnels) protected, and the bandwidth protected.
mesh	Displays information about auto-tunnel mesh tunnel interfaces.
primary	Displays information about auto-tunnel primary tunnel interfaces.
backup-tunnel	Displays information about the FRR protection provided by each tunnel selected by other options specified with this command. The information includes the physical interface protected by the tunnel, the number of TE label switched packets (LSPs) (that is, tunnels) protected, and the bandwidth protected.
fast-reroute	Selects FRR-protected MPLS TE tunnels originating, transmitting, or terminating on this router.
role	Restricts the display to tunnels with the indicated role (all, head, middle, tail, or remote).
all	Displays all tunnels.
head	Displays tunnels with their head at this router.
middle	Displays tunnels with a midpoint at this router.
remote	Displays tunnels with their head at some other router; this is a combination of **middle** and **tail**.
tail	Displays tunnels with a tail at this router.
source-id	(Optional) Restricts the display to tunnels with a matching source IP address or tunnel number.
ipaddress	Source IP address.
tunnel-id	Tunnel number. The range is from 0 to 65535.
suboptimal	(Optional) Displays information about tunnels using a suboptimal path.
constraints	Specifies constraints for finding the best comparison path.

current	Displays tunnels whose path metric is greater than the current shortest path, constrained by the tunnel's configured options. Selected tunnels would have a shorter path if they were reoptimized immediately.
max	Displays information for the specified tunneling interface.
none	Displays tunnels whose path metric is greater than the shortest unconstrained path. Selected tunnels have a longer path than the Interior Gateway Protocol's (IGP) shortest path.
statistics	(Optional) Displays event counters for one or more tunnels.
summary	(Optional) Displays event counters accumulated for all tunnels.
up	(Optional) Displays tunnels if the tunnel interface is up. Tunnel midpoints and tails are typically up or not present.
accounting	(Optional) Displays accounting information (the rate of the traffic flow) for tunnels.
brief	(Optional) Specifies a format with one line per tunnel.
protection	(Optional) Displays information about the protection provided by each tunnel selected by other options specified with this command. The information includes whether protection is configured for the tunnel, the protection (if any) provided to the tunnel by this router, and the bandwidth protected.

Command Default General information about each MPLS TE tunnel known to the router is displayed.

Command Modes User EXEC (>) Privileged EXEC (#)

Command History

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

Release	Modification
12.1(3)T	Input and output interface information was added to the new **brief** form of the output. The **suboptimal** and **interface** keywords were added to the nonbrief format. The nonbrief, nonsummary formats contain the history of the LSP selection.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	The **property** and **protection** keywords were added. The command is supported on the Cisco 10000 series routers.
12.2(18)S	The following keywords were added: **accounting**, **attributes**, **name-regexp** , **property**, and **auto-tunnel**. The **property backup** keyword was changed to **property backup-tunnel**.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was modified. The **detail** and **dest-mode** keywords were added. The output was updated to display MPLS TE point-to-multipoint (P2MP) information. The command output was enhanced to include the configuration and status when a path option list is configured for backup path options. The output also shows information about tunnels configured with autoroute announce.
15.0(1)S	This command was modified. The command output was enhanced to include formation about P2MP LSPs and sub-LSPs.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

To select the tunnels for which information is displayed, use the **auto-tunnel**, **backup-tunnel**, **attributes**, **destination**,**interface**, **name**, **name-regexp**, **property**, **role**, **source-id**, **suboptimal constraints**, **up**, and **down** keywords singly or combined.

To select the type of information displayed about the selected tunnels, use the **accounting**, **backup**, **protection**, **statistics**, and **summary** keywords.

The **auto-tunnel**, **backup-tunnel**, and **property** keywords display the same information, except that the **property** keyword restricts the display to autotunnels, backup tunnels, or tunnels that are Fast Reroute-protected.

The **name-regexp** keyword displays output for each tunnel whose name contains a specified string. For example, if there are tunnels named iou-100-t1, iou-100-t2, and iou-100-t100, the **show mpls traffic-eng tunnels name-regexp iou-100** command displays output for the three tunnels whose name contains the string iou-100.

If you specify the **name** keyword, there is command output only if the command name is an exact match, for example, iou-100-t1.

The nonbrief and nonsummary formats of the output contain the history of the LSP selection.

The "Reroute Pending" State Changes in Cisco IOS Release 12.2(33)SRE

In releases earlier than Cisco IOS Release 12.2(33)SRE, MPLS TE P2P tunnels display "reroute pending" during reoptimization until the "delayed clean" status of the old path is complete. During the "delayed clean" process, the command output displays the following status:

```
Router# show mpls traffic-eng tunnels tunnel 534
Name: Router_t534                         (Tunnel534) Destination: 10.30.30.8
    Status:
      Admin: up         Oper: up     Path: valid       Signalling: connected
      path option 10, type explicit PRIMARY_TO_8 (Basis for Setup, path weight 30)
  !!! path option 10 delayed clean in progress
  !!!     Change in required resources detected: reroute pending
          Currently Signalled Parameters:
            Bandwidth: 300      kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
            Metric Type: TE (default)
```

In Cisco IOS Release 12.2(33)SRE and later releases, P2P and P2MP MPLS TE tunnels display "reroute pending" during reoptimization until the new path is used for forwarding. The "reroute pending" status is not displayed during the delayed clean operation. There is no change to data forwarding or tunnel creation. You might see the "reroute pending" status for a shorter time. In the following example, the "reroute pending" message appears, but the "delayed clean" message does not.

```
Router# show mpls traffic-eng tunnels tunnel 534
  Name: Router_t534                         (Tunnel534) Destination: 10.30.30.8
    Status:
      Admin: up         Oper: up     Path: valid       Signalling: connected
      path option 10, type explicit PRIMARY_TO_8 (Basis for Setup, path weight 30)
            Change in required resources detected: reroute pending
          Currently Signalled Parameters:
            Bandwidth: 300      kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
            Metric Type: TE (default)
```

Examples

The following is sample output from the **show mpls traffic-eng tunnels brief** command. It displays brief information about every MPLS TE tunnel known to the router.

```
Router# show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                  running
    Forwarding:                    enabled
    Periodic reoptimization:       every 3600 seconds, next in 1706 seconds
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t1                        10.112.0.12      -         PO4/0/1   up/up
Router_t2                        10.112.0.12      -         unknown   up/down
Router_t3                        10.112.0.12      -         unknown   admin-down
Router_t1000                     10.110.0.10      -         unknown   up/down
Router_t2000                     10.110.0.10      -         PO4/0/1   up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

The table below describes the significant fields shown in the display.

Table 35: show mpls traffic-eng tunnels Field Descriptions

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

The following is sample output from the **show mpls traffic-eng tunnels property fast-reroute brief** command. It displays brief information about all MPLS TE tunnels acting as Fast Reroute backup tunnels (**property backup-tunnel**) for interfaces on the router.

```
Router# show mpls traffic-eng tunnels property fast-reroute brief
Signalling Summary:
    LSP Tunnels Process:            running
    RSVP Process:                   running
    Forwarding:                     enabled
    Periodic reoptimization:        every 3600 seconds, next in 2231 seconds
    Periodic FRR Promotion:         every 300 seconds, next in 131 seconds
    Periodic auto-bw collection:    disabled
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t2000                     10.110.0.10      -         PO4/0/1   up/up
Router_t2                        10.112.0.12      -         unknown   up/down
Router_t3                        10.112.0.12      -         unknown   admin-down
Displayed 3 (of 9) heads, 0 (of 1) midpoints, 0 (of 0) tails
```

The following is sample output from the **show mpls traffic-eng tunnels backup** command. This command selects every MPLS TE tunnel known to the router and displays information about the Fast Reroute protection each selected tunnels provides for interfaces on this router; the command does not generate output for tunnels that do not provide Fast Reroute protection of interfaces on this router.

```
Router# show mpls traffic-eng tunnels backup
Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected I/fs: PO1/0, PO1/1, PO3/3
```

```
    Protected lsps: 1
    Backup BW: any pool unlimited; inuse: 100 kbps
Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 192.168.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected I/fs: PO1/1
    Protected lsps: 0
    Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
  LSP Head, Tunnel5711, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected I/fs: PO1/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

The following is sample output from the **show mpls traffic-eng tunnels property fast-reroute protection** command. This command selects every MPLS TE tunnel known to the router that was signaled as a Fast Reroute-protected LSP (**property fast-reroute**) and displays information about the protection this router provides each selected tunnel.

```
Router# show mpls traffic-eng tunnels property fast-reroute protection
Router_t1
  LSP Head, Tunnel1, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 25
  Fast Reroute Protection: Requested
    Outbound: FRR Ready
      Backup Tu5711 to LSP nhop
        Tu5711: out I/f: PO1/1, label: implicit-null
      LSP signalling info:
        Original: out I/f: PO1/0, label: 12304, nhop: 10.1.1.7
        With FRR: out I/f: Tu5711, label: 12304
      LSP bw: 6000 kbps, Backup level: any unlimited, type: any pool
Router_t2
  LSP Head, Tunnel2, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 2
  Fast Reroute Protection: Requested
    Outbound: FRR Ready
      Backup Tu578 to LSP nhop
        Tu578: out I/f: PO1/0, label: 12306
      LSP signalling info:
        Original: out I/f: PO3/3, label: implicit-null, nhop: 10.3.3.8
        With FRR: out I/f: Tu578, label: implicit-null
      LSP bw: 100 kbps, Backup level: any unlimited, type: any pool
r9_t1
  LSP Midpoint, signalled, connection up
  Src 10.9.9.9, Dest 10.88.88.88, Instance 2347
  Fast Reroute Protection: Requested
    Inbound:  FRR Inactive
      LSP signalling info:
        Original: in I/f: PO1/2, label: 12304, phop: 10.205.0.9
    Outbound: FRR Ready
      Backup Tu5711 to LSP nhop
        Tu5711: out I/f: PO1/1, label: implicit-null
      LSP signalling info:
        Original: out I/f: PO1/0, label: 12305, nhop: 10.1.1.7
        With FRR: out I/f: Tu5711, label: 12305
      LSP bw: 10 kbps, Backup level: any unlimited, type: any pool
```

The following is sample output from the **show mpls traffic-eng tunnels tunnel** command. This command displays information about just a single tunnel.

```
Router# show mpls traffic-eng tunnels tunnel 1
Name: swat76k1_t1                         (Tunnel1) Destination: 10.0.0.4
   Status:
     Admin: admin-down Oper: down   Path: not valid   Signalling: Down
     path option 1, type explicit gi7/4-R4
   Config Parameters:
     Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
```

```
     Metric Type: TE (default)
     AutoRoute:  disabled  LockDown: disabled  Loadshare: 0        bw-based
     auto-bw: disabled
   Shortest Unconstrained Path Info:
     Path Weight: 2 (TE)
     Explicit Route: 10.1.0.1 10.1.0.2 172.0.0.1 192.0.0.4
   History:
     Tunnel:
       Time since created: 13 days, 52 minutes
       Number of LSP IDs (Tun_Instances) used: 0 swat76k1#
swat76k1#sh mpls traf tun property ?
   auto-tunnel    auto-tunnel created tunnels
   backup-tunnel  Tunnels used as fast reroute
   fast-reroute   Tunnels protected by fast reroute
```

The following is sample output from the **show mpls traffic-eng tunnels accounting** command. This command displays the rate of traffic flow for tunnels.

```
Router# show mpls traffic-eng tunnels accounting
Tunnel1 (Destination 10.103.103.103; Name iou-100_t1)
 5 minute output rate 0 kbits/sec, 0 packets/sec
Tunnel2 (Destination 10.103.103.103; Name iou-100_t2)
 5 minute output rate 0 kbits/sec, 0 packets/sec Tunnel100 (Destination 10.101.101.101;
Name iou-100_t100)
 5 minute output rate 0 kbits/sec, 0 packets/sec Totals for 3 Tunnels
 5 minute output rate 0 kbits/sec, 0 packets/sec
```

When the MPLS TE P2MP feature is configured, the **show mpls traffic-eng tunnels** command categorizes the output as follows:

- P2P tunnels/LSPs
- P2MP tunnels
- P2MP sub-LSPs

The following **show mpls traffic-eng tunnels brief** command displays P2MP tunnel and sub-LSP information:

```
Router# show mpls traffic-eng tunnels brief
Signalling Summary:
   LSP Tunnels Process:            running
   Passive LSP Listener:           running
   RSVP Process:                   running
   Forwarding:                     enabled
   Periodic reoptimization:        every 60 seconds, next in 5 seconds
   Periodic FRR Promotion:         Not Running
   Periodic auto-bw collection:    disabled
P2P TUNNELS/LSPs:
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
p2p-LSP                          10.2.0.1         -         Se2/0     up/up
Displayed 2 (of 2) heads, 0 (of 0) midpoints, 0 (of 0) tails
P2MP TUNNELS:
                         DEST    CURRENT
INTERFACE   STATE/PROT UP/CFG TUNID LSPID
Tunnel2     up/up      3/10   2     1
Tunnel5     up/down    1/10   5     2
Displayed 2 (of 2) P2MP heads
P2MP SUB-LSPS:
SOURCE          TUNID LSPID   DESTINATION     SUBID     ST UP IF    DOWN IF
10.1.0.1        2     1       10.2.0.1        1         up head     Se2/0
10.1.0.1        2     1       10.3.0.199      2         up head     Et2/0
10.1.0.1        2     1       19.4.0.1        2         up head     s2/0
10.1.0.1        2     2       1 9.4.0.1       2         up head     s2/0
10.1.0.1        5     2       10.5.0.1        7         up head     e2/0
100.100.100.100 1     3       200.200.200.200 1         up ge2/0    s2/0
100.100.100.100 1     3       10.1.0.1        1         up e2/0     tail
Displayed 7 P2MP sub-LSPs:
          5 (of 5) heads, 1 (of 1) midpoints, 1 (of 1) tails
```

The following is sample output from the **show mpls traffic-eng tunnels** command for a tunnel named t1. The output displays the following:

- An adjustment threshold of 5 percent
- An overflow limit of 4
- An overflow threshold of 25 percent
- An overflow threshold exceeded by 1

```
Router# show mpls traffic-eng tunnels name t1

Name:tagsw4500-9_t1 (Tunnel1) Destination:10.0.0.4
 Status:
  Admin:up Oper:up Path:valid Signalling:connected
  path option 1, type explicit pbr_south (Basis for Setup, path weight 30)
  path option 2, type dynamic
Config Parameters:
 Bandwidth:13 kbps (Global) Priority:7 7 Affinity:0x0/0xFFFF
 AutoRoute: disabled LockDown:disabled Loadshare:13 bw-based
 auto-bw:(300/265) 53 Bandwidth Requested: 13
   Adjustment threshold: 5%
   Overflow Limit: 4  Overflow Threshold: 25%
  Overflow Threshold Crossed: 1
  Sample Missed: 1 Samples Collected: 1
Active Path Option Parameters:
  State: dynamic path option 1 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
 InLabel  :  -
 OutLabel : Serial3/0, 18
 RSVP Signalling Info:
   Src 10.0.0.1, Dst 10.0.0.4, Tun_Id 2, Tun_Instance 2
  RSVP Path Info:
   My Address: 10.105.0.1
   Explicit Route: 10.105.0.2 104.105.0.1 10.0.0.4
   Record   Route:   NONE
   Tspec: ave rate=13 kbits, burst=1000 bytes, peak rate=13 kbits
 Record   Route:   NONE
   Tspec: ave rate=13 kbits, burst=1000 bytes, peak rate=13 kbits
  RSVP Resv Info:
   Record   Route:   NONE
   Fspec: ave rate=13 kbits, burst=1000 bytes, peak rate=13 kbits
  Shortest Unconstrained Path Info:
   Path Weight: 128 (TE)
   Explicit Route: 10.105.0.2 104.105.0.1 10.0.0.4
History:
    Tunnel:
      Time since created: 7 days, 4 hours, 42 minutes
      Time since path change: 54 seconds
      Number of LSP IDs (Tun_Instances) used: 2
      SSO recovered <full|partial> (2 subLSP recovered, 0 failed)
    Current LSP: [ID: 2]
      Uptime: 54 seconds
      Selection: SSO recovered
    Prior LSP: [ID: 1]
      Removal Trigger: signalling shutdown
```

The following sample output from the **show mpls traffic-eng tunnels** command for Cisco IOS Release 12.2(33)SRE shows path protection information. This command displays information about a single tunnel.

```
Router# show mpls traffic-eng tunnels tunnel 1
Name: iou-100_t2 (Tunnel2) Destination: 10.10.0.2
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit primary1 (Basis for Setup, path weight 10)
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type list name secondary-list
   Inuse path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)
```

```
Config Parameters:
 Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
 Metric Type: TE (default)
 AutoRoute announce: enabled LockDown: disabled Loadshare: 0 bw-based
 auto-bw: disabled
Active Path Option Parameters:
 State: explicit path option 10 is active
 BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
InLabel : -
OutLabel : Ethernet7/0, implicit-null
RSVP Signalling Info:
 Src 100.100.100.100, Dst 10.10.0.2, Tun_Id 2, Tun_Instance 188
RSVP Path Info:
 My Address: 10.1.0.1
 Explicit Route: 10.1.0.2 10.10.0.2
 Record Route: NONE
 Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
 Record Route: NONE
 Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
 Path Weight: 10 (TE)
 Explicit Route: 10.1.0.1 10.1.0.2 10.10.0.2
History:
    Tunnel:
      Time since created: 7 days, 4 hours, 42 minutes
      Time since path change: 54 seconds
      Number of LSP IDs (Tun_Instances) used: 2
      SSO recovered <full|partial> (2 subLSP recovered, 0 failed)
    Current LSP: [ID: 2]
      Uptime: 54 seconds
      Selection: SSO recovered
    Prior LSP: [ID: 1]
      Removal Trigger: signalling shutdown
```

The following sample output from the **show mpls traffic-eng tunnels** command for Cisco IOS Release 12.2(33)SRE shows autoroute destination information.

```
Router# show mpls traffic-eng tunnel tunnel 109
Name: PE-7_t109                    (Tunnel109) Destination: 10.0.0.9
 Status:
  Admin: up   Oper: up   Path: valid Signalling: connected
  path option 1, type explicit to_109 (Basis for Setup, path weight 64)
  path option 20, type explicit to_109_alt
Config Parameters:
 Bandwidth: 0   kbps (Global   Priority: 7  7   Affinity: 0x0/0xFFFF
 Metric Type: TE (default)
 Autoroute announce: enabled LockDown: disabled   Loadshare: 0    bx-based
 auto-bw: disabled
 AutoRoute destination: enabled
```

The table below describes the significant fields shown in the display.

Table 36: show mpls traffic-eng tunnels Field Descriptions

Field	Description
LSP Tunnels Process	Status of the LSP tunnels process.
RSVP Process	Status of the RSVP process.
Forwarding	Status of forwarding (enabled or disabled).
Periodic reoptimization	Schedule for periodic reoptimization (in seconds).
TUNNEL NAME	Name of the interface configured at the tunnel head.

Field	Description
DESTINATION	Identifier of the tailend router.
UP IF	Upstream interface that the tunnel used.
DOWN IF	Downstream interface that the tunnel used.
STATE/PROT	For tunnel heads, admin-down, up, or down. For nonheads, signaled.
Adjustment threshold	Configured threshold. This field is displayed only if a threshold is explicitly configured.
Overflow Limit Overflow Threshold	These fields are displayed only if an overflow limit was specified in the **tunnel mpls traffic-eng auto-bw** command. The tunnel resizes before the end of the sampling interval if the output rate exceeds the current bandwidth by the percentage specified in the overflow threshold, or if the output rate exceeds the number of times specified in the overflow limit.
Overflow Threshold Crossed	Number of times the output rate exceeded the overflow threshold in consecutive collection intervals. This value is reset at the beginning of the automatic bandwidth sampling interval.
Number of Auto-bw Adjustment resize requests	Number of times the tunnel was resized because an output rate exceeded the adjustment threshold. This field is displayed only if the number is greater than zero and if automatic bandwidth is enabled on the tunnel. This counter is reset each time automatic bandwidth is enabled on the tunnel. You can clear this counter at any time by entering the **clear mpls traffic-eng auto-bw timer** command.
Time since last Auto-bw Adjustment resize request	The amount of time (in minutes and seconds) since the last bandwidth adjustment.
Number of Auto-bw Overflow resize requests	The number of times (in seconds) the tunnel was resized because an overflow limit was exceeded. This field is displayed only if the number is greater than zero and if an overflow limit is enabled on the tunnel. This counter is reset each time automatic bandwidth is enabled on the tunnel. You can clear this counter at any time by entering the **clear mpls traffic-eng auto-bw timer** command.
Time since last Auto-bw Overflow resize request	The amount of time (in seconds) since the tunnel was resized because an overflow limit was exceeded.

Related Commands

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

show mpls traffic-eng tunnels statistics

To display event counters for one or more Multiprotocol Label Switching (MPLS) traffic engineering tunnels, use the **show mpls traffic-eng tunnels statistics** command in user EXEC and privileged EXEC mode.

show mpls traffic-eng tunnels [**tunnel** *tunnel-name*] **statistics [summary]**

Syntax Description

tunnel *tunnel-name*	(Optional) Displays event counters accumulated for the specified tunnel.
summary	(Optional) Displays event counters accumulated for all tunnels.

Command Default

If you enter the command without any keywords, the command displays the event counters for every MPLS traffic engineering tunnel interface configured on the router.

Command Modes

User EXEC (>) Privileged EXEC mode (#)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was modified. The output was updated to display MPLS TE point-to-multipoint (P2MP) information.

Usage Guidelines

A label switching router (LSR) maintains counters for each MPLS traffic engineering tunnel headend that counts significant events for the tunnel, such as state transitions for the tunnel, changes to the tunnel path,

and various signaling failures. You can use the **show mpls traffic-eng tunnels statistics** command to display these counters for a single tunnel, for every tunnel, or for all tunnels (accumulated values). Displaying the counters is often useful for troubleshooting tunnel problems.

Examples

The following are examples of output from the **show mpls traffic-eng tunnels statistics** command:

```
Router# show mpls traffic-eng tunnels tunnel tunnel1001 statistics

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


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

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


Router# show mpls traffic-eng tunnels statistics summary
 Management statistics:
    Path: 2304 no path, 73 path no longer valid, 0 missing ip exp path
 432 path changes
    State: 300 transitions, 0 admin down, 100 oper down
 Signalling statistics:
    Opens: 200 succeeded, 0 timed out, 0 bad path spec
 0 other aborts
    Errors: 0 no b/w, 18 no route, 0 admin
 0 bad exp route, 0 rec route loop, 0 other
```

The following show mpls traffic-eng tunnels statistics command displays status information about P2MP path and LSPs for Tunnel 100:

```
Router# show mpls traffic-eng tunnels statistics
Tunnel100 (Name p2mp-1_t100)
  Management statistics:
    Path:   0 no path, 0 path no longer valid, 0 missing ip exp path
            97 path changes, 306 path lookups
            0 protection pathoption_list errors
            0 invalid inuse popt in pathoption list
            0 loose path reoptimizations, triggered by PathErrors
    State:  1 transitions, 0 admin down, 0 oper down
```

```
Signalling statistics:
  Opens:  1 succeeded, 0 timed out, 0 bad path spec
          0 other aborts
    LSP Activations: 97 succeeded
      Last Failure: No path that satisfy tunnel constraints
      Failures stats:
        5: No path that satisfy tunnel constraints
  Errors: 0 no b/w, 288 no route, 0 admin, 0 remerge detected
          0 bad exp route, 0 rec route loop, 0 frr activated
          0 other
```

The table below describes the significant fields shown in the display.

Table 37: show mpls traffic-eng tunnels statistics Field Descriptions

Field	Description
Tunnel 1001	Name of the tunnel interface.
Destination	IP address of the tunnel tailend.
Name	Internal name for the tunnel, composed of the router name and the tunnel interface number.
Path	Heading for counters for tunnel path events are as follows: • no path--Number of unsuccessful attempts to calculate a path for the tunnel. • path no longer valid--Number of times a previously valid path for the tunnel became invalid. • missing ip exp path--Number of times that attempts to use “obtain a path for the tunnel” failed because no path was configured (and there was no dynamic path option for the tunnel). • path changes--Number of times the tunnel path changed.
State	Heading for counters for tunnel state transitions.
Opens	Heading for counters for tunnel open attempt events.
Errors	Heading for various tunnel signaling errors, such as no bandwidth, no route, admin (preemption), a bad explicit route, and a loop in the explicit route.

Related Commands

Command	Description
clear mpls traffic-eng tunnel counters	Clears the counters for all MPLS traffic engineering tunnels.

show mpls traffic-eng tunnels summary

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

show mpls traffic-eng tunnels summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	This command output was updated to display periodic Fast Reroute information. The command is supported on the Cisco 10000 series ESRs.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	The command output was modified to display the number of tunnels that were attempted and successful in being recovered following a failover.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was modified. The output was updated to display Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) point-to-multipoint (P2MP) information.
15.0(1)S	This command was modified. The command output was updated to display stateful switchover (SSO) recovery information for MPLS TE P2MP tunnels.

Usage Guidelines

Use the**show mpls traffic-eng tunnels summary** command to display the number of tunnel headends that were attempted and successful at being recovered following SSO.

Examples

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

```
Router# show mpls traffic-eng tunnels summary
Signalling Summary:
    LSP Tunnels Process:            running
    Passive LSP Listener:           running
```

```
RSVP Process:                   running
Forwarding:                     enabled
Periodic reoptimization:        every 3600 seconds, next in 1420 seconds
Periodic FRR Promotion:         Not Running
Periodic auto-bw collection:    every 300 seconds, next in 234 seconds
P2P:
  Head: 1 interfaces,   1 active signalling attempts, 1 established
        1 activations,  0 deactivations
        1 SSO recovery attempts, 1 SSO recovered
  Midpoints: 0, Tails: 0
P2MP:
  Head: 1 interfaces,   2 active signalling attempts, 2 established
        2 sub-LSP activations,  0 sub-LSP deactivations
        1 LSP successful activations,  0 LSP deactivations
        1 SSO recovery attempts, LSP Recovered: 1 full, 0 partial, 0 fail
  Midpoints: 0, Tails: 0
```

The table below describes the significant fields shown in the display.

Table 38: show mpls traffic-eng tunnels summary Field Descriptions

Field	Description
LSP Tunnels Process	Multiprotocol Label Switching (MPLS) traffic engineering has or has not been enabled.
Passive LSP Listener	The device listens for LSPs and can terminate them, if desired.
RSVP Process	Resource Reservation Protocol (RSVP) has or has not been enabled. (This feature is enabled as a consequence of MPLS traffic engineering being enabled.)
Forwarding	Indicates whether appropriate forwarding is enabled. (Appropriate forwarding on a router is Cisco Express Forwarding switching.)

Field	Description
Head	Summary information about tunnel heads at this device. Information includes: • interfaces--Number of MPLS traffic engineering tunnel interfaces. • active signalling attempts--Number of LSPs currently successfully signaled or being signaled. • established--Number of LSPs currently signaled. • activations--Number of signaling attempts initiated. • deactivations--Number of signaling attempts terminated. • SSO recovery attempts--Number of MPLS traffic engineering tunnel headend LSPs that were attempted to be recovered following an SSO event. • SSO recovered--Number of MPLS traffic engineering tunnel headend LSPs that were successfully recovered following an SSO event.
Midpoints	Number of midpoints at this device.
Tails	Number of tails at this device.
Periodic reoptimization	Frequency of periodic reoptimization and time (in seconds) until the next periodic reoptimization.
Periodic FRR Promotion	Frequency that scanning occurs to determine if link-state packets (LSPs) should be promoted to better backup tunnels, and time (in seconds) until the next scanning.
Periodic auto-bw collection	Frequency of automatic bandwidth collection and time left (in seconds) until the next collection.

Related Commands

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

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

show mpls ttfib

To display information about the Multiprotocol Label Switching (MPLS) TTFIB table, use the **show mpls ttfib** command in privileged EXEC mode.

show mpls ttfib [**detail [hardware]**| **vrf** *instance* **[detail]**]

Syntax Description

detail	(Optional) Displays detailed information.
hardware	(Optional) Displays detailed hardware information.
vrf *instance*	(Optional) Displays entries for a specified Virtual Private Network (VPN) routing and forwarding instance (VRF).

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display information about the MPLS TTFIB table:

```
Router# show mpls ttfib
Local  Outgoing    Packets Tag          LTL   Dest.   Destination    Outgoing
Tag    Tag or VC   Switched             Index Vlanid  Mac Address    Interface
4116   21          0                    0xE0  1020    0000.0400.0000 PO4/1*
       34          0                    0x132 1019    00d0.040d.380a GE5/3
       45          0                    0xE3  4031    0000.0430.0000 PO4/4
4117   16          0                    0x132 1019    00d0.040d.380a GE5/3*
       17          0                    0xE0  1020    0000.0400.0000 PO4/1
       18          0                    0xE3  4031    0000.0430.0000 PO4/4
4118   21          0                    0xE0  1020    0000.0400.0000 PO4/1*
       56          0                    0xE3  4031    0000.0430.0000 PO4/4
4119   35          0                    0xE3  4031    0000.0430.0000 PO4/4*
       47          0                    0xE0  1020    0000.0400.0000 PO4/1
```

show platform software ethernet f0 efp

To display the Ethernet Flow Point (EFP) information in slot 0 of a Cisco ASR 1000 Series Aggregation Services Router's embedded service processor (ESP), use the **show platform software ethernet f0 efp** command in privileged EXEC mode.

show platform software ethernet f0 efp {**brief**| **detail**| **id** *efp-id* **interface** *interface-name*| **interface** *interface-name* {**brief**| **detail**}| **summary**}

Syntax Description

brief	Displays brief information about the EFP.
detail	Displays detailed information about the EFP.
id *efp-id*	EFP ID. The range is from 1 to 8000.
interface *interface-name*	Interface name of the EFP.
brief	Displays brief information about the EFP interface.
detail	Displays detailed information about the EFP interface.
summary	Displays summarized information about the EFP.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **show platform software ethernet f0 efp** command displays the EFP information in slot 0 of a Cisco ASR 1000 Series Aggregation Services Router's ESP, irrespective of whether the slot is in the active state or the standby state.

Examples

The following is sample output from the **show platform software ethernet f0 efp detail** command:

```
Router# show platform software ethernet f0 efp detail

Forwarding Manager Ethernet Flow Points

EFP: ID: 1, DPIDB: 0x1020010, Data Type: static
     Interface: 8 (GigabitEthernet0/0/0)
     QFPIDX: 22
     QFPifname: GigabitEthernet0/0/0.EFP1
  State: AdminDown, Priority: 10
  First tag encap: dot1q, vlan-type: 0x8100
        vlan list: 1-4094
  DOT1AD Port Type: UNI
  Storm ctrl u_cir: 8000, m_cir: 980000000, b_cir: 1500000
  Bridge-domain: 1, Split-Horizon: None
    MAC-limit: 65536
```

The following table describes the significant fields shown in the display.

Table 39: show platform software ethernet f0 efp Field Descriptions

Field	Description
Storm ctrl u_cir	The unknown unicast threshold value.
m_cir	The multicast threshold value.
b_cir	The broadcast threshold value.

Related Commands

Command	Description
show platform software ethernet f1 efp detail	Displays the EFP information in slot 1 of a Cisco ASR 1000 Series Aggregation Services Router's ESP.

show platform software ethernet f1 efp

To display the Ethernet Flow Point (EFP) information in slot 1 of a Cisco ASR 1000 Series Aggregation Services Router's embedded service processor (ESP), use the **show platform software ethernet f1 efp** command in privileged EXEC mode.

show platform software ethernet f1 efp {**brief**| **detail**| **id** *efp-id* **interface** *interface-name*| **interface** *interface-name* {**brief**| **detail**}| **summary**}

brief	Displays brief information about the EFP.
detail	Displays detailed information about the EFP.
id *efp-id*	EFP ID. The range is from 1 to 8000.
interface *interface-name*	Interface name of the EFP.
brief	Displays brief information about the EFP interface.
detail	Displays detailed information about the EFP interface.
summary	Displays summarized information about the EFP.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **show platform software ethernet f1 efp** command displays the EFP information in slot 1 of a Cisco ASR 1000 Series Aggregation Services Router's ESP, irrespective of whether the slot is in the active state or the standby state.

Examples

The following is sample output from the **show platform software ethernet f1 efp detail** command:

```
Router# show platform software ethernet f1 efp detail

Forwarding Manager Ethernet Flow Points

EFP: ID: 1, DPIDB: 0x1020010, Data Type: static
     Interface: 8 (GigabitEthernet0/0/0)
     QFPIDX: 22
     QFPifname: GigabitEthernet0/0/0.EFP1
  State: AdminDown, Priority: 10
  First tag encap: dot1q, vlan-type: 0x8100
        vlan list: 1-4094
  DOT1AD Port Type: UNI
  Storm ctrl u_cir: 8000, m_cir: 980000000, b_cir: 1500000
  Bridge-domain: 1, Split-Horizon: None
    MAC-limit: 65536
```

The following table describes the significant fields shown in the display.

Table 40: show platform software ethernet f1 efp Field Descriptions

Field	Description
Storm ctrl u_cir	The unknown unicast threshold value.
m_cir	The multicast threshold value.
b_cir	The broadcast threshold value.

Related Commands

Command	Description
show platform software ethernet f0 efp detail	Displays the EFP information in slot 0 of a Cisco ASR 1000 Series Aggregation Services Router's ESP.

show platform software mpls

To display information pertaining to the replicated Output Chain Elements (OCEs) on the Forwarding Manager, use the **show platform software mpls** command in the privileged EXEC mode.

show platform software mpls rp | **fp** *act-status* **replicate**

Syntax Description

rp	Displays information about the the Route Processor (RP).
fp	Displays information about the Forwarding Processor (FP).
act-status	Status of the processor. It can be one of the following values: • **active—**Displays information about the active processors. • **standby—**Displays information about the standby processors.
replicate	Displays information pertaining to the replicated OCEs on the Forwarding Manager.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show platform software mpls rp** *act-status* **replicate** command displaying information pertaining to all the replicated OCEs on the Forwarding Manager RP:

```
Router# show platform software mpls rp active replicate
Replicate-oce-list: 0x400000d2 (1 OCEs)
OM: 0x42269b64
Replicate-oce-list: 0x400000d3 (1 OCEs)
OM: 0x43ba2aec
Replicate-oce-list: 0x400000d4 (0 OCEs)
OM: 0x422659bc
Replicate-oce-list: 0x400000d5 (0 OCEs)
OM: 0x422658ac
```

The following is sample output from the **show platform software mpls fp** command displaying all the replicated OCEs on the Forwarding Manager FP:

```
Router# show platform software mpls fp active replicate
Replicate-oce-list: 0x400000d2 (1 OCEs)
AOM obj: 352887, HW list: 0x11a65628 (created)
Replicate-oce-list: 0x400000d3 (1 OCEs)
AOM obj: 352889, HW list: 0x10d4a518 (created)
Replicate-oce-list: 0x400000d4 (0 OCEs)
AOM obj: 352891, HW list: 0x139e3d90 (created)
Replicate-oce-list: 0x400000d5 (0 OCEs)
AOM obj: 352894, HW list: 0x139e7cb8 (created)
```

show platform software vpn

To display information about the platform software for IPv6 Virtual Private Networks (VPNs), use the **show platform software vpn** command in privileged EXEC mode.

show platform software vpn [**status**| **mapping ios**]

Syntax Description

status	(Optional) Displays the VPN status.
mapping ios	(Optional) Displays the Cisco IOS mapping information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB1	This command was introduced on the Cisco 7600 series routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If no keyword is used, then all VPN information is displayed.

Examples

The following example shows output regarding platform software for all VPNs:

```
Router# show platform software vpn
```

show policy-map interface

To display the statistics and the configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command in user EXEC or privileged EXEC mode.

ATM Shared Port Adapters

show policy-map interface *slot*/*subslot*/*port* **.**[*subinterface*]

Cisco CMTS Routers

show policy-map interface *interface-type slot/subslot/port*

Cisco 3660, 3845, 7200, 7400, 7500, Cisco ASR 903 Series Routers, and Cisco ASR 1000 Series Routers

show policy-map interface *type type-parameter* [**vc** [*vpi*]**[/]***vci*] [**dlci** *dlci*] [**input**| **output**] [**class** *class-name*]

Cisco 6500 Series Switches

show policy-map interface [*interface-type interface-number*| **vlan** *vlan-id*] **[detailed]** [{**input**| **output**} [**class** *class-name*]]

show policy-map interface [**port-channel** *channel-number* [**class** *class-name*]]

Cisco 7600 Series Routers

show policy-map interface [*interface-type interface-number*| **null 0**| **vlan** *vlan-id*] [**input**| **output**]

Syntax Description

slot	(CMTS and ATM shared port adapter only) Chassis slot number. See the appropriate hardware manual for slot information. For SIPs, see the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
/subslot	(CMTS and ATM shared port adapter only) Secondary slot number on an SPA interface processor (SIP) where a SPA is installed. See the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on an SPA” topic in the platform-specific SPA software configuration guide for subslot information.

port	(CMTS and ATM shared port adapter only) Port or interface number. See the appropriate hardware manual for port information. For SPAs, see the corresponding "Specifying the Interface Address" topics in the platform-specific SPA software configuration guide.
.*subinterface*	(ATM shared port adapter only—Optional) Subinterface number. The number that precedes the period must match the number to which this subinterface belongs. The range is 1 to 4,294,967,293.
type	Type of interface or subinterface whose policy configuration is to be displayed.
type-parameter	Port, connector, interface card number, class-map name or other parameter associated with the interface or subinterface type.
vc	(Optional) For ATM interfaces only, shows the policy configuration for a specified PVC.
vpi **/**	(Optional) ATM network virtual path identifier (VPI) for this permanent virtual circuit (PVC). On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. The absence of both the forward slash (/) and a *vpi* value defaults the *vpi* value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed.
vci	(Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **atmvc-per-vp** command. Typically, the lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance [OAM], switched virtual circuit [SVC] signaling, Integrated Local Management Interface [ILMI], and so on) and should not be used. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.

dlci	(Optional) Indicates a specific PVC for which policy configuration will be displayed.
dlci	(Optional) A specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC will be displayed when a DLCI is specified.
input	(Optional) Indicates that the statistics for the attached input policy will be displayed.
output	(Optional) Indicates that the statistics for the attached output policy will be displayed.
class *class-name*	(Optional) Displays the QoS policy actions for the specified class.
interface-type	(Optional) Interface type; possible valid values are **atm**, **ethernet**, **fastethernet**, **ge-wan gigabitethernet**, **pos**, **pseudowire** and **tengigabitethernet**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
detailed	(Optional) Displays additional statistics.
port-channel *channel-number*	(Optional) Displays the EtherChannel port-channel interface.
null 0	(Optional) Specifies the null interface; the only valid value is 0.

Command Default

This command displays the packet statistics of all classes that are configured for all service policies on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface.

When used with the ATM shared port adapter, this command has no default behavior or values.

Command Modes

Privileged EXEC (#)

ATM Shared Port Adapter
User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(28)S	This command was modified for the QoS: Percentage-Based Policing feature to include milliseconds when calculating the committed (conform) burst (bc) and excess (peak) burst (be) sizes.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(2)T	This command was modified to display information about the policy for all Frame Relay PVCs on the interface or, if a DLCI is specified, the policy for that specific PVC. This command was also modified to display the total number of packets marked by the quality of service (QoS) set action.
12.1(3)T	This command was modified to display per-class accounting statistics.
12.2(4)T	This command was modified for two-rate traffic policing and can display burst parameters and associated actions.
12.2(8)T	This command was modified for the Policer Enhancement—Multiple Actions feature and the WRED—Explicit Congestion Notification (ECN) feature. For the Policer Enhancement—Multiple Actions feature, the command was modified to display the multiple actions configured for packets conforming to, exceeding, or violating a specific rate. For the WRED—Explicit Congestion Notification (ECN) feature, the command displays ECN marking information.

Release	Modification
12.2(13)T	The following modifications were made: • This command was modified for the Percentage-Based Policing and Shaping feature. • This command was modified for the Class-Based RTP and TCP Header Compression feature. • This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes in policy maps can now be configured to discard packets belonging to a specified class. • This command was modified to display the Frame Relay DLCI number as a criterion for matching traffic inside a class map. • This command was modified to display Layer 3 packet length as a criterion for matching traffic inside a class map. • This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.
12.2(14)SX	This command was modified. Support for this command was introduced on Cisco 7600 series routers.
12.2(15)T	This command was modified to display Frame Relay voice-adaptive traffic-shaping information.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.3(14)T	This command was modified to display bandwidth estimation parameters.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. This command was modified to display aggregate WRED statistics for the ATM shared port adapter. Note that changes were made to the syntax, defaults, and command modes. These changes are labelled “ATM Shared Port Adapter.”
12.4(4)T	This command was modified. The **typeaccess-control** keywords were added to support flexible packet matching.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, and the following modifications were made: • This command was modified to display either legacy (undistributed processing) QoS or hierarchical queueing framework (HQF) parameters on Frame Relay interfaces or PVCs. • This command was modified to display information about Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnel marking.

Release	Modification
12.2(31)SB2	The following modifications were made: • This command was enhanced to display statistical information for each level of priority service configured and information about bandwidth-remaining ratios, and this command was implemented on the Cisco 10000 series router for the PRE3. • This command was modified to display statistics for matching packets on the basis of VLAN identification numbers. As of Cisco IOS Release 12.2(31)SB2, matching packets on the basis of VLAN identification numbers is supported on Cisco 10000 series routers only.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(15)T2	This command was modified to display information about Generic Routing Encapsulation (GRE) tunnel marking. **Note** As of this release, GRE-tunnel marking is supported on the Cisco MGX Route Processor Module (RPM-XF) platform *only* .
12.2(33)SB	This command was modified to display information about GRE-tunnel marking, and support for the Cisco 7300 series router was added.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1 and was implemented on the Cisco ASR 1000 series router.
12.4(20)T	This command was modified. Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).
12.2(33)SXI	This command was implemented on the Catalyst 6500 series switch and modified to display the strict level in the priority feature and the counts per level.
12.2(33)SRE	This command was modified to automatically round off the bc and be values, in the MQC police policy map, to the interface's MTU size.
Cisco IOS XE Release 2.6	The command output was modified to display information about subscriber QoS statistics.
12.2(54)SG	This command was modified to display only the applicable count of policer statistics.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
Cisco IOS XE Release 3.7S	This command was implemented on Cisco ASR 903 Series Routers.
Cisco IOS XE Release 3.8S	This command was modified. The *pseudowire* interface type was added.

Release	Modification
Cisco IOS XE Release 3.8S	This command was modified. The *pseudowire* interface type was added on Cisco 1000 Series Routers.
Cisco IOS Release 15.3(1)S	This command was modified. The *pseudowire* interface type was added.

Usage Guidelines

Cisco 3660, 3845, 7200, 7400, 7500, Cisco ASR 903 Series Routers, and Cisco ASR 1000 Series Routers

The **show policy-map interface** command displays the packet statistics for classes on the specified interface or the specified PVC only if a service policy has been attached to the interface or the PVC.

The counters displayed after the **show policy-map interface** command is entered are updated only if congestion is present on the interface.

The **show policy-map interface** command displays policy information about Frame Relay PVCs only if Frame Relay Traffic Shaping (FRTS) is enabled on the interface.

The **show policy-map interface** command displays ECN marking information only if ECN is enabled on the interface.

To determine if shaping is active with HQF, check the queue depth field of the "(queue depth/total drops/no-buffer drops)" line in the **show policy-map interface** command output.

In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and the bytes delayed counters were removed for traffic shaping classes.

Cisco 7600 Series Routers and Catalyst 6500 Series Switches

The pos, atm, and ge-wan interfaces are not supported on Cisco 7600 series routers or Catalyst 6500 series switches that are configured with a Supervisor Engine 720

Cisco 7600 series routers and Catalyst 6500 series switches that are configured with a Supervisor Engine 2 display packet counters.

Cisco 7600 series routers and Catalyst 6500 series switches that are configured with a Supervisor Engine 720 display byte counters.

The output does not display policed-counter information; 0 is displayed in its place (for example, 0 packets, 0 bytes). To display dropped and forwarded policed-counter information, enter the **show mls qos** command.

On the Cisco 7600 series router, for OSM WAN interfaces only, if you configure policing within a policy map, the hardware counters are displayed and the class-default counters are not displayed. If you do not configure policing within a policy map, the class-default counters are displayed.

On the Catalyst 6500 series switch, the **show policy-map interface** command displays the strict level in the priority feature and the counts per level.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

HQF

When you configure HQF, the **show policy-map interface** command displays additional fields that include the differentiated services code point (DSCP) value, WRED statistics in bytes, transmitted packets by WRED, and a counter that displays packets output/bytes output in each class.

Examples

This section provides sample output from typical **show policy-map interface** commands. Depending upon the interface or platform in use and the options enabled, the output you see may vary slightly from the ones shown below.

Examples

The following sample output of the **show policy-map interface** command displays the statistics for the serial 3/1 interface, to which a service policy called mypolicy (configured as shown below) is attached. Weighted fair queueing (WFQ) has been enabled on this interface. See the table below for an explanation of the significant fields that commonly appear in the command output.

```
policy-map mypolicy
 class voice
  priority 128
 class gold
  bandwidth 100
 class silver
  bandwidth 80
  random-detect
Router# show policy-map interface serial3/1 output

 Serial3/1
  Service-policy output: mypolicy
    Class-map: voice (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 5
      Weighted Fair Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 128 (kbps) Burst 3200 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0
    Class-map: gold (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 2
      Weighted Fair Queueing
        Output Queue: Conversation 265
        Bandwidth 100 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
    Class-map: silver (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 1
      Weighted Fair Queueing
        Output Queue: Conversation 266
        Bandwidth 80 (kbps)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
         exponential weight: 9
         mean queue depth: 0
class     Transmitted       Random drop      Tail drop    Minimum Maximum  Mark
          pkts/bytes        pkts/bytes       pkts/bytes    thresh  thresh  prob
0             0/0               0/0              0/0          20      40  1/10
1             0/0               0/0              0/0          22      40  1/10
2             0/0               0/0              0/0          24      40  1/10
3             0/0               0/0              0/0          26      40  1/10
4             0/0               0/0              0/0          28      40  1/10
5             0/0               0/0              0/0          30      40  1/10
6             0/0               0/0              0/0          32      40  1/10
7             0/0               0/0              0/0          34      40  1/10
```

```
rsvp          0/0               0/0               0/0           36      40  1/10
Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Examples

The following sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called p1 (configured as shown below) is attached. Traffic shaping has been enabled on this interface. See the table below for an explanation of the significant fields that commonly appear in the command output.

Note In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
policy-map p1
 class c1
  shape average 320000
Router# show policy-map interface serial3/2 output

 Serial3/2
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0
      Traffic Shaping
        Target    Byte   Sustain   Excess    Interval  Increment Adapt
        Rate      Limit  bits/int  bits/int  (ms)      (bytes)   Active
        320000    2000   8000      8000      25        1000      -
        Queue     Packets   Bytes     Packets   Bytes     Shaping
        Depth                         Delayed   Delayed   Active
        0         0         0         0         0         no
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

The table below describes significant fields commonly shown in the displays. The fields in the table are grouped according to the relevant QoS feature. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Table 41: show policy-map interface Field Descriptions

Field	Description
Fields Associated with Classes or Service Policies	
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.

Field	Description
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Note In distributed architecture platforms (such as the Cisco 7500 series platform), the value of the transfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically deviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyser equipment.	
Match	Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* .
Fields Associated with Queueing (if Enabled)	

Field	Description
Output Queue	The weighted fair queueing (WFQ) conversation to which this class of traffic is allocated.
Bandwidth	Bandwidth, in either kbps or percentage, configured for this class and the burst size.
pkts matched/bytes matched	Number of packets (also shown in bytes) matching this class that were placed in the queue. This number reflects the total number of matching packets queued at any time. Packets matching this class are queued only when congestion exists. If packets match the class but are never queued because the network was not congested, those packets are not included in this total. However, if process switching is in use, the number of packets is always incremented even if the network is not congested.
depth/total drops/no-buffer drops	Number of packets discarded for this class. No-buffer indicates that no memory buffer exists to service the packet.
Fields Associated with Weighted Random Early Detection (WRED) (if Enabled)	
exponential weight	Exponent used in the average queue size calculation for a WRED parameter group.
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
class	IP precedence level.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. **Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level.

Field	Description
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level.
Minimum thresh	Minimum threshold. Minimum WRED threshold in number of packets.
Maximum thresh	Maximum threshold. Maximum WRED threshold in number of packets.
Mark prob	Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold.
Fields Associated with Traffic Shaping (if Enabled)	
Target Rate	Rate used for shaping traffic.
Byte Limit	Maximum number of bytes that can be transmitted per interval. Calculated as follows: ((Bc+Be) /8) x 1
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).
Increment (bytes)	Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.
Queue Depth	Current queue depth of the traffic shaper.
Packets	Total number of packets that have entered the traffic shaper system.
Bytes	Total number of bytes that have entered the traffic shaper system.
Packets Delayed	Total number of packets delayed in the queue of the traffic shaper before being transmitted.
Bytes Delayed	Total number of bytes delayed in the queue of the traffic shaper before being transmitted.
Shaping Active	Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field.

Examples

The following sample output of the **show policy-map interface** command displays the statistics for the ATM shared port adapter interface 4/1/0.10, to which a service policy called prec-aggr-wred (configured as shown below) is attached. Because aggregate WRED has been enabled on this interface, the classthrough Mark Prob statistics are aggregated by subclasses. See the table below for an explanation of the significant fields that commonly appear in the command output.

```
Router(config)# policy-map prec-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect aggregate
Router(config-pmap-c)# random-detect precedence values 0 1 2 3 minimum thresh 10
maximum-thresh 100 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 4 5 minimum-thresh 40 maximum-thresh
 400 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 6 minimum-thresh 60 maximum-thresh
600 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 7 minimum-thresh 70 maximum-thresh
700 mark-prob 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface ATM4/1/0.10 point-to-point
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# pvc 10/110
Router(config-if)# service-policy output prec-aggr-wred

Router# show policy-map interface atm4/1/0.10

 ATM4/1/0.10: VC 10/110 -
  Service-policy output: prec-aggr-wred
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 0
        class       Transmitted     Random drop      Tail drop     Minimum   Maximum  Mark
 pkts/bytes pkts/bytes pkts/bytes thresh thresh prob

        0  1  2  3       0/0              0/0              0/0           10     100  1/10
        4  5             0/0              0/0              0/0           40     400  1/10
        6                0/0              0/0              0/0           60     600  1/10
        7                0/0              0/0              0/0           70     700  1/10
```

Examples

The following sample output of the **show policy-map interface** command displays the statistics for the ATM shared port adapter interface 4/1/0.11, to which a service policy called dscp-aggr-wred (configured as shown below) is attached. Because aggregate WRED has been enabled on this interface, the class through Mark Prob statistics are aggregated by subclasses. See the table below for an explanation of the significant fields that commonly appear in the command output.

```
Router(config)# policy-map dscp-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
10 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 0 1 2 3 4 5 6 7 minimum-thresh 10
maximum-thresh 20 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 8 9 10 11 minimum-thresh 10 maximum-thresh
 40 mark-prob 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface ATM4/1/0.11 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
```

```
Router(config-subif)# pvc 11/101
Router(config-subif)# service-policy output dscp-aggr-wred
Router# show policy-map interface atm4/1/0.11

 ATM4/1/0.11: VC 11/101 -
  Service-policy output: dscp-aggr-wred
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        Exp-weight-constant: 0 (1/1)
        Mean queue depth: 0
        class       Transmitted     Random drop      Tail drop     Minimum   Maximum  Mark
                   pkts/bytes pkts/bytes pkts/bytes thresh thresh prob
        default          0/0              0/0             0/0            1      10  1/10
        0  1  2  3
        4  5  6  7       0/0              0/0             0/0           10      20  1/10
        8  9  10 11      0/0              0/0             0/0           10      40  1/10
```

The table below describes the significant fields shown in the display when aggregate WRED is configured for an ATM shared port adapter.

Table 42: show policy-map interface Field Descriptions—Configured for Aggregate WRED on ATM Shared Port Adapter

Field	Description
exponential weight	Exponent used in the average queue size calculation for a Weighted Random Early Detection (WRED) parameter group.
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
Note When Aggregate Weighted Random Early Detection (WRED) is enabled, the following WRED statistics will be aggregated based on their subclass (either their IP precedence or differentiated services code point (DSCP) value).	
class	IP precedence level or differentiated services code point (DSCP) value.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. **Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter.

Field	Description
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level or DSCP value.
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level or DSCP value.
Minimum thresh	Minimum threshold. Minimum WRED threshold in number of packets.
Maximum thresh	Maximum threshold. Maximum WRED threshold in number of packets.
Mark prob	Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold.

Examples

The following sample output shows that Frame Relay voice-adaptive traffic shaping is currently active and has 29 seconds left on the deactivation timer. With traffic shaping active and the deactivation time set, this means that the current sending rate on DLCI 201 is minCIR, but if no voice packets are detected for 29 seconds, the sending rate will increase to CIR.

Note In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy interface Serial3/1.1

 Serial3/1.1:DLCI 201 -
  Service-policy output:MQC-SHAPE-LLQ1

    Class-map:class-default (match-any)
      1434 packets, 148751 bytes
      30 second offered rate 14000 bps, drop rate 0 bps
      Match:any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
            63000/63000     1890   7560      7560      120       945

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                        Delayed   Delayed   Active
        BECN   0         1434      162991    26        2704      yes
        Voice Adaptive Shaping active, time left 29 secs
```

The table below describes the significant fields shown in the display. Significant fields that are not described in the table below are described in the table above (for “show policy-map interface Field Descriptions”).

Table 43: show policy-map interface Field Descriptions—Configured for Frame Relay Voice-Adaptive Traffic Shaping

Field	Description
Voice Adaptive Shaping active/inactive	Indicates whether Frame Relay voice-adaptive traffic shaping is active or inactive.
time left	Number of seconds left on the Frame Relay voice-adaptive traffic shaping deactivation timer.

Examples

The following is sample output from the **show policy-map interface** command when two-rate traffic policing has been configured. In the example below, 1.25 Mbps of traffic is sent ("offered") to a policer class.

```
Router# show policy-map interface serial3/0


 Serial3/0
  Service-policy output: policy1
   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps
   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
```

The two-rate traffic policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming will be sent as is, and packets marked as exceeding will be marked with IP Precedence 2 and then sent. Packets marked as violating the specified rate are dropped.

The table below describes the significant fields shown in the display.

Table 44: show policy-map interface Field Descriptions—Configured for Two-Rate Traffic Policing

Field	Description
police	Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size, peak information rate (PIR), and peak burst size used for marking packets.
conformed	Displays the action to be taken on packets conforming to a specified rate. Displays the number of packets and bytes on which the action was taken.

Field	Description
exceeded	Displays the action to be taken on packets exceeding a specified rate. Displays the number of packets and bytes on which the action was taken.
violated	Displays the action to be taken on packets violating a specified rate. Displays the number of packets and bytes on which the action was taken.

Examples

The following is sample output from the **show policy-map** command when the Policer Enhancement—Multiple Actions feature has been configured. The sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called "police" (configured as shown below) is attached.

```
policy-map police
 class class-default
  police cir 1000000 pir 2000000
   conform-action transmit
   exceed-action set-prec-transmit 4
   exceed-action set-frde-transmit
   violate-action set-prec-transmit 2
   violate-action set-frde-transmit

Router# show policy-map interface serial3/2

Serial3/2: DLCI 100 -
Service-policy output: police
    Class-map: class-default (match-any)
      172984 packets, 42553700 bytes
      5 minute offered rate 960000 bps, drop rate 277000 bps
      Match: any
     police:
         cir 1000000 bps, bc 31250 bytes, pir 2000000 bps, be 31250 bytes
       conformed 59679 packets, 14680670 bytes; actions:
         transmit
exceeded 59549 packets, 14649054 bytes; actions:
         set-prec-transmit 4
         set-frde-transmit
       violated 53758 packets, 13224468 bytes; actions:
         set-prec-transmit 2
         set-frde-transmit
       conformed 340000 bps, exceed 341000 bps, violate 314000 bps
```

The sample output from **show policy-map interface** command shows the following:

- 59679 packets were marked as conforming packets (that is, packets conforming to the CIR) and were transmitted unaltered.
- 59549 packets were marked as exceeding packets (that is, packets exceeding the CIR but not exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 4, the discard eligibility (DE) bit was set to 1, and the packets were transmitted with these changes.
- 53758 packets were marked as violating packets (that is, exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 2, the DE bit was set to 1, and the packets were transmitted with these changes.

Note Actions are specified by using the *action* argument of the **police** command. For more information about the available actions, see the **police** command reference page.

The table below describes the significant fields shown in the display.

Table 45: show policy-map interface Field Descriptions—Configured for Multiple Traffic Policing Actions

Field	Description
police	Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size (BC), PIR, and peak burst size (BE) used for marking packets.
conformed, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as conforming to a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.
exceeded, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as exceeding a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.
violated, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as violating a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.

Examples

The following is sample output from the **show policy-map interface** command when the WRED **—** Explicit Congestion Notification (ECN) feature has been configured. The words “explicit congestion notification” included in the output indicate that ECN has been enabled.

```
Router# show policy-map interface Serial4/1

 Serial4/1
  Service-policy output:policy_ecn
        Class-map:prec1 (match-all)
          1000 packets, 125000 bytes
          30 second offered rate 14000 bps, drop rate 5000 bps
          Match:ip precedence 1
          Weighted Fair Queueing
            Output Queue:Conversation 42
            Bandwidth 20 (%)
            Bandwidth 100 (kbps)
            (pkts matched/bytes matched) 989/123625
        (depth/total drops/no-buffer drops) 0/455/0
             exponential weight:9
             explicit congestion notification
             mean queue depth:0
     class   Transmitted  Random drop  Tail drop   Minimum     Maximum     Mark
             pkts/bytes   pkts/bytes    pkts/bytes threshold   threshold   probability
       0       0/0          0/0          0/0          20          40        1/10
```

```
  1      545/68125       0/0           0/0           22            40          1/10
  2        0/0           0/0           0/0           24            40          1/10
  3        0/0           0/0           0/0           26            40          1/10
  4        0/0           0/0           0/0           28            40          1/10
  5        0/0           0/0           0/0           30            40          1/10
  6        0/0           0/0           0/0           32            40          1/10
  7        0/0           0/0           0/0           34            40          1/10
rsvp       0/0           0/0           0/0           36            40          1/10
class    ECN Mark
       pkts/bytes
  0      0/0
  1     43/5375
  2      0/0
  3      0/0
  4      0/0
  5      0/0
  6      0/0
  7      0/0
rsvp     0/0
```

The table below describes the significant fields shown in the display.

Table 46: show policy-map interface Field Descriptions—Configured for ECN

Field	Description
explicit congestion notification	Indication that Explicit Congestion Notification is enabled.
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
class	IP precedence value.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. **Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence value.
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence value.
Minimum threshold	Minimum WRED threshold in number of packets.

Field	Description
Maximum threshold	Maximum WRED threshold in number of packets.
Mark probability	Fraction of packets dropped when the average queue depth is at the maximum threshold.
ECN Mark pkts/bytes	Number of packets (also shown in bytes) marked by ECN.

Examples

The following sample output from the **show policy-map interface** command shows the RTP header compression has been configured for a class called “prec2” in the policy map called “p1”.

The **show policy-map interface** command output displays the type of header compression configured (RTP), the interface to which the policy map called “p1” is attached (Serial 4/1), the total number of packets, the number of packets compressed, the number of packets saved, the number of packets sent, and the rate at which the packets were compressed (in bits per second (bps)).

In this example, User Datagram Protocol (UDP)/RTP header compressions have been configured, and the compression statistics are included at the end of the display.

```
Router# show policy-map interface Serial4/1

Serial4/1
Service-policy output:p1
    Class-map:class-default (match-any)
      1005 packets, 64320 bytes
      30 second offered rate 16000 bps, drop rate 0 bps
      Match:any
compress:
          header ip rtp
          UDP/RTP Compression:
          Sent:1000 total, 999 compressed,
                41957 bytes saved, 17983 bytes sent
                3.33 efficiency improvement factor
                99% hit ratio, five minute miss rate 0 misses/sec, 0 max
                 rate 5000 bps
```

The table below describes the significant fields shown in the display.

Table 47: show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.

Field	Description
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
UDP/RTP Compression	Indicates that RTP header compression has been configured for the class.
Sent total	Count of every packet sent, both compressed packets and full-header packets.
Sent compressed	Count of number of compressed packets sent.
bytes saved	Total number of bytes saved (that is, bytes not needing to be sent).
bytes sent	Total number of bytes sent for both compressed and full-header packets.
efficiency improvement factor	The percentage of increased bandwidth efficiency as a result of header compression. For example, with RTP streams, the efficiency improvement factor can be as much as 2.9 (or 290 percent).
hit ratio	Used mainly for troubleshooting purposes, this is the percentage of packets found in the context database. In most instances, this percentage should be high.
five minute miss rate	The number of new traffic flows found in the last five minutes.
misses/sec max	The average number of new traffic flows found per second, and the highest rate of new traffic flows to date.

Field	Description
rate	The actual traffic rate (in bits per second) after the packets are compressed.

Note A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Examples

The following sample output from the **show policy-map interface** command displays the statistics for the Serial2/0 interface, to which a policy map called "policy1" is attached. The discarding action has been specified for all the packets belonging to a class called "c1." In this example, 32000 bps of traffic is sent ("offered") to the class and all of them are dropped. Therefore, the drop rate shows 32000 bps.

```
Router# show policy-map interface

 Serial2/0
 Serial2/0
  Service-policy output: policy1
    Class-map: c1 (match-all)
       10184 packets, 1056436 bytes
       5 minute offered rate 32000 bps, drop rate 32000 bps
       Match: ip precedence 0
       drop
```

The table below describes the significant fields shown in the display.

Table 48: show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.

Field	Description
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Note In distributed architecture platforms (such as the Cisco 7500), the value of the transfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically deviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyser equipment.	
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* .
drop	Indicates that the packet discarding action for all the packets belonging to the specified class has been configured.

Note A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Examples

The following sample output from the **show policy-map interface** command shows traffic policing configured using a CIR based on a bandwidth of 20 percent. The CIR and committed burst (Bc) in milliseconds (ms) are included in the display.

```
Router# show policy-map interface Serial3/1

  Service-policy output: mypolicy
    Class-map: gold (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      police:
          cir 20 % bc 10 ms
          cir 2000000 bps, bc 2500 bytes
          pir 40 % be 20 ms
          pir 4000000 bps, be 10000 bytes
     conformed 0 packets, 0 bytes; actions:
      transmit
     exceeded 0 packets, 0 bytes; actions:
       drop
      violated 0 packets, 0 bytes; actions:
       drop
      conformed 0 bps, exceed 0 bps, violate 0 bps
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Table 49: show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping.

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.

Field	Description
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
police	Indicates that traffic policing based on a percentage of bandwidth has been enabled. Also, displays the bandwidth percentage, the CIR, and the committed burst (Bc) size in ms.
conformed, actions	Displays the number of packets and bytes marked as conforming to the specified rates, and the action to be taken on those packets.
exceeded, actions	Displays the number of packets and bytes marked as exceeding the specified rates, and the action to be taken on those packets.

Examples

The following sample output from the **show policy-map interface** command (shown below) displays the statistics for the serial 3/2 interface. Traffic shaping has been enabled on this interface, and an average rate of 20 percent of the bandwidth has been specified.

Note In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy-map interface Serial3/2

Serial3/2
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
```

```
Match: any
Traffic Shaping
  Target/Average      Byte   Sustain    Excess      Interval  Increment  Adapt
  Rate              Limit  bits/int  bits/int    (ms)     (bytes)   Active
   20 %                        10 (ms)    20 (ms)
  201500/201500       1952   7808       7808        38         976       -
  Queue     Packets   Bytes     Packets   Bytes     Shaping
  Depth                         Delayed   Delayed   Active
  0         0         0         0         0         no
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Table 50: show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled).

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.

Field	Description
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Quality of Service Solutions Configuration Guide*.
Traffic Shaping	Indicates that traffic shaping based on a percentage of bandwidth has been enabled.
Target/Average Rate	Rate (percentage) used for shaping traffic and the number of packets meeting that rate.
Byte Limit	Maximum number of bytes that can be transmitted per interval. Calculated as follows: ((Bc+Be) /8) x 1
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).
Increment (bytes)	Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.
Adapt Active	Indicates whether adaptive shaping is enabled.
Queue Depth	Current queue depth of the traffic shaper.
Packets	Total number of packets that have entered the traffic shaper system.
Bytes	Total number of bytes that have entered the traffic shaper system.
Packets Delayed	Total number of packets delayed in the queue of the traffic shaper before being transmitted. **Note** In Cisco IOS Release 12.4(20)T, this counter was removed.
Bytes Delayed	Total number of bytes delayed in the queue of the traffic shaper before being transmitted. **Note** In Cisco IOS Release 12.4(20)T, this counter was removed.

Field	Description
Shaping Active	Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field.

Examples

The following sample output from the **show policy-map interface** command displays the packet statistics for the Ethernet4/1 interface, to which a service policy called “mypolicy” is attached. The Layer 3 packet length has been specified as a match criterion for the traffic in the class called “class1”.

```
Router# show policy-map interface Ethernet4/1

  Ethernet4/1
  Service-policy input: mypolicy
    Class-map: class1 (match-all)
       500 packets, 125000 bytes
       5 minute offered rate 4000 bps, drop rate 0 bps
       Match: packet length min 100 max 300
       QoS Set
         qos-group 20
           Packets marked 500
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy input name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Table 51: show policy-map interface Field Descriptions—Configured for Packet Classification Based on Layer 3 Packet Length.

Field	Description
Service-policy input	Name of the input service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.

Field	Description
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups.
QoS Set, qos-group, Packets marked	Indicates that class-based packet marking based on the QoS group has been configured. Includes the qos-group number and the number of packets marked.

Examples

The following sample output of the **show policy-map interface** command shows the service policies attached to a FastEthernet subinterface. In this example, a service policy called “policy1” has been attached. In “policy1”, a table map called “table-map1” has been configured. The values in “table-map1” will be used to map the precedence values to the corresponding class of service (CoS) values.

```
Router# show policy-map interface

 FastEthernet1/0.1
  Service-policy input: policy1
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        precedence cos table table-map1
          Packets marked 0
```

The table below describes the fields shown in the display. A number in parentheses may appear next to the service-policy input name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Table 52: show policy-map interface Field Descriptions—Configured for Enhanced Packet Marking.

Field	Description
Service-policy input	Name of the input service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of the packets coming into the class.
Match	Match criteria specified for the class of traffic. Choices include criteria such as Precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Quality of Service Solutions Configuration Guide*.
QoS Set	Indicates that QoS group (set) has been configured for the particular class.
precedence cos table table-map1	Indicates that a table map (called "table-map1") has been used to determine the precedence value. The precedence value will be set according to the CoS value defined in the table map.
Packets marked	Total number of packets marked for the particular class.

Examples

The following is sample output from the **show policy-map interface** command. This sample displays the statistics for the serial 2/0 interface on which traffic policing has been enabled. The committed (conform) burst (bc) and excess (peak) burst (be) are specified in milliseconds (ms).

```
Router# show policy-map interface serial2/0
```

```
Serial2/0
 Service-policy output: policy1 (1050)
   Class-map: class1 (match-all) (1051/1)
     0 packets, 0 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: ip precedence 0  (1052)
     police:
         cir 20 % bc 300 ms
         cir 409500 bps, bc 15360 bytes
         pir 40 % be 400 ms
         pir 819000 bps, be 40960 bytes
       conformed 0 packets, 0 bytes; actions:
         transmit
       exceeded 0 packets, 0 bytes; actions:
         drop
       violated 0 packets, 0 bytes; actions:
         drop
       conformed 0 bps, exceed 0 bps, violate 0 bps
   Class-map: class-default (match-any) (1054/0)
     0 packets, 0 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: any  (1055)
       0 packets, 0 bytes
       5 minute rate 0 bps
```

In this example, the CIR and PIR are displayed in bps, and both the committed burst (bc) and excess burst (be) are displayed in bits.

The CIR, PIR bc, and be are calculated on the basis of the formulas described below.

Examples

When calculating the CIR, the following formula is used:

- CIR percentage specified (as shown in the output from the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output from the**show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router# show interfaces serial2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the CIR:

20 % * 2048 kbps = 409600 bps

Examples

When calculating the PIR, the following formula is used:

- PIR percentage specified (as shown in the output from the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output from the**show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router# show interfaces serial2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the PIR:

40 % * 2048 kbps = 819200 bps

Note Discrepancies between this total and the total shown in the output from the **show policy-map interface** command can be attributed to a rounding calculation or to differences associated with the specific interface configuration.

Examples

When calculating the bc, the following formula is used:

- The bc in milliseconds (as shown in the **show policy-map** command) * the CIR in bits per seconds = total number bytes

The following values are used for calculating the bc:

300 ms * 409600 bps = 15360 bytes

Examples

When calculating the bc and the be, the following formula is used:

- The be in milliseconds (as shown in the **show policy-map** command) * the PIR in bits per seconds = total number bytes

The following values are used for calculating the be:

400 ms * 819200 bps = 40960 bytes

The table below describes the significant fields shown in the display.

Table 53: show policy-map interface Field Descriptions

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.

Field	Description
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Quality of Service Solutions Configuration Guide* .
police	Indicates that traffic policing has been enabled. Display includes the CIR, PIR (in both a percentage of bandwidth and in bps) and the bc and be in bytes and milliseconds. Also displays the optional conform, exceed, and violate actions, if any, and the statistics associated with these optional actions.

Examples

The following sample output from the **show policy-map interface** command displays statistics for the Fast Ethernet 0/1 interface on which bandwidth estimates for quality of service (QoS) targets have been generated.

The Bandwidth Estimation section indicates that bandwidth estimates for QoS targets have been defined. These targets include the packet loss rate, the packet delay rate, and the timeframe in milliseconds. Confidence refers to the drop-one-in value (as a percentage) of the targets. Corvil Bandwidth means the bandwidth estimate in kilobits per second.

When no drop or delay targets are specified, "none specified, falling back to drop no more than one packet in 500" appears in the output.

```
Router# show policy-map interface FastEthernet0/1

 FastEthernet0/1
  Service-policy output: my-policy
    Class-map: icmp (match-all)
      199 packets, 22686 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      Bandwidth Estimation:
        Quality-of-Service targets:
          drop no more than one packet in 1000 (Packet loss < 0.10%)
          delay no more than one packet in 100 by 40 (or more) milliseconds
            (Confidence: 99.0000%)
        Corvil Bandwidth: 1 kbits/sec
    Class-map: class-default (match-any)
      112 packets, 14227 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Bandwidth Estimation:
        Quality-of-Service targets:
          <none specified, falling back to drop no more than one packet in 500
        Corvil Bandwidth: 1 kbits/sec
```

Examples

The following sample output from the **show policy-mapinterface** command shows that shaping is active (as seen in the queue depth field) with HQF enabled on the serial 4/3 interface. All traffic is classified to the class-default queue.

Note In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy-map interface serial4/3

 Serial4/3
  Service-policy output: shape
    Class-map: class-default (match-any)
      2203 packets, 404709 bytes
      30 second offered rate 74000 bps, drop rate 14000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 64/354/0
      (pkts output/bytes output) 1836/337280
      shape (average) cir 128000, bc 1000, be 1000
      target shape rate 128000
        lower bound cir 0,  adapt to fecn 0
      Service-policy : LLQ
        queue stats for all priority classes:

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
        Class-map: c1 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Priority: 32 kbps, burst bytes 1500, b/w exceed drops: 0
        Class-map: class-default (match-any)
          2190 packets, 404540 bytes
          30 second offered rate 74000 bps, drop rate 14000 bps
          Match: any
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 63/417/0
          (pkts output/bytes output) 2094/386300
```

Examples

Note As of Cisco IOS Release 12.2(31)SB2, matching packets on the basis of VLAN ID numbers is supported on the Catalyst 1000 platform only.

The following is a sample configuration in which packets are matched and classified on the basis of the VLAN ID number. In this sample configuration, packets that match VLAN ID number 150 are placed in a class called “class1.”

```
Router# show class-map

Class Map match-all class1 (id 3)
Match vlan 150
```

Class1 is then configured as part of the policy map called “policy1.” The policy map is attached to Fast Ethernet subinterface 0/0.1.

The following sample output of the **show policy-map interface** command displays the packet statistics for the policy maps attached to Fast Ethernet subinterface 0/0.1. It displays the statistics for policy1, in which class1 has been configured.

```
Router# show policy-map interface

FastEthernet0/0.1
! Policy-map name.
Service-policy input: policy1
! Class configured in the policy map.
Class-map: class1 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
! VLAN ID 150 is the match criterion for the class.
Match: vlan 150
police:
cir 8000000 bps, bc 512000000 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0 bps, exceed 0 bps
Class-map: class-default (match-any)
10 packets, 1140 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any
10 packets, 1140 bytes
5 minute rate 0 bps
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy input name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Table 54: show policy-map interface Field Descriptions—Packets Matched on the Basis of VLAN ID Number.

Field	Description
Service-policy input	Name of the input service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of the packets coming into the class.

Field	Description
Match	Match criteria specified for the class of traffic. Choices include criteria such as VLAN ID number, precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* .

Examples

The following example shows how to display the statistics and the configurations of all the input and output policies that are attached to an interface on a Cisco 7600 series router:

```
Router# show policy-map interface

 FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class ipp5
    police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
oliced-dscp-transmit
```

The following example shows how to display the input-policy statistics and the configurations for a specific interface on a Cisco 7600 series router:

```
Router# show policy-map interface fastethernet 5/36 input

 FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class ipp5
    police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
oliced-dscp-transmit
```

The table below describes the significant fields shown in the display.

Table 55: show policy-map interface Field Descriptions—Cisco 7600 Series Routers

Field	Description
service-policy input	Name of the input service policy applied to the specified interface.
class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.

Field	Description
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
minute rate	Rate, in kbps, of the packets coming into the class.
match	Match criteria specified for the class of traffic. Choices include criteria such as VLAN ID number, precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* .
class	Precedence value.
police	Indicates that the **police** command has been configured to enable traffic policing.

Examples

The following example shows the automatic rounding-off of the **bc** and **be** values, in the MQC police policy-map, to the interface's MTU size in a Cisco 7200 series router. The rounding-off is done only when the bc and be values are lesser than the interface's MTU size.

```
Router# show policy-map interface

Service-policy output: p2
Service-policy output: p2
    Class-map: class-default (match-any)
      2 packets, 106 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
        2 packets, 106 bytes
        30 second rate 0 bps
      police:
          cir 10000 bps, bc 4470 bytes
          pir 20000 bps, be 4470 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps, violate 0000 bps
```

Examples

The following sample output from the show policy-map interface command shows the types of statistical information that displays when multiple priority queues are configured. Depending upon the interface in use and the options enabled, the output that you see may vary slightly from the output shown below.

```
Router# show policy-map interface

Serial2/1/0
Service-policy output: P1
Queue statistics for all priority classes:
.
.
.
Class-map: Gold (match-all)
0 packets, 0 bytes   /*Updated for each priority level configured.*/
5 minute offered rate 0 bps, drop rate 0 bps
Match: ip precedence 2
Priority: 0 kbps, burst bytes 1500, b/w exceed drops: 0
Priority Level 4:
0 packets, 0 bytes
```

Examples

The following sample output from the show policy-map interface command indicates that bandwidth-remaining ratios are configured for class queues. As shown in the example, the classes precedence_0, precedence_1, and precedence_2 have bandwidth-remaining ratios of 20, 40, and 60, respectively.

```
Router# show policy-map interface GigabitEthernet1/0/0.10

  Service-policy output: vlan10_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      bandwidth remaining ratio 10
      Service-policy : child_policy
        Class-map: precedence_0 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 62 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 20
        Class-map: precedence_1 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Queueing
          queue limit 62 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 40
        Class-map: precedence_2 (match-all)
          0 packets, 0 bytes
```

```
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 2
    Queueing
    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    shape (average) cir 500000, bc 2000, be 2000
    target shape rate 500000
    bandwidth remaining ratio 60
  Class-map: class-default (match-any)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps

    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
```

The table below describes the significant fields shown in the display.

Table 56: show policy-map interface Field Descriptions—Configured for Bandwidth-Remaining Ratios

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
bandwidth remaining ratio	Indicates the ratio used to allocate excess bandwidth.

Examples

In this sample output of the **show policy-map interface** command, the character string “ip dscp tunnel 3” indicates that L2TPv3 tunnel marking has been configured to set the DSCP value to 3 in the header of a tunneled packet.

```
Router# show policy-map interface

 Serial0
  Service-policy input: tunnel
    Class-map: frde (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: fr-de
      QoS Set
        ip dscp tunnel 3
          Packets marked 0
    Class-map: class-default (match-any)
      13736 packets, 1714682 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
```

```
        13736 packets, 1714682 bytes
        30 second rate 0 bps
```

The table below describes the significant fields shown in the display.

Table 57: show policy-map interface Field Descriptions—Configured for Tunnel Marking

Field	Description
service-policy input	Name of the input service policy applied to the specified interface.
class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
match	Match criteria specified for the class of traffic. In this example, the Frame Relay Discard Eligible (DE) bit has been specified as the match criterion. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
ip dscp tunnel	Indicates that tunnel marking has been configured to set the DSCP in the header of a tunneled packet to a value of 3.

Examples

The following output from the show policy-map interface command indicates that ATM overhead accounting is enabled for shaping and disabled for bandwidth:

```
Router# show policy-map interface

Service-policy output:unit-test
Class-map: class-default (match-any)
100 packets, 1000 bytes
30 second offered rate 800 bps, drop rate 0 bps
Match: any
shape (average) cir 154400, bc 7720, be 7720
target shape rate 154400
```

```
overhead accounting: enabled
bandwidth 30% (463 kbps)
overhead accounting: disabled
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(packets output/bytes output) 100/1000
```

The table below describes the significant fields shown in the display.

Table 58: show policy-map interface Field Descriptions—Configured for Traffic Shaping Overhead Accounting for ATM

Field	Description
service-policy output	Name of the output service policy applied to the specified interface.
class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
match	Match criteria specified for the class of traffic. In this example, the Frame Relay Discard Eligible (DE) bit has been specified as the match criterion. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
target shape rate	Indicates that traffic shaping is enabled at the specified rate.
overhead accounting	Indicates whether overhead accounting is enabled or disabled for traffic shaping.
bandwidth	Indicates the percentage of bandwidth allocated for traffic queueing.
overhead accounting:	Indicates whether overhead accounting is enabled or disabled for traffic queueing.

Examples

The following output from the show policy-map interface command displays the configuration for Fast Ethernet interface 0/0:

Note In HQF images for Cisco IOS Releases 12.4(20)T and later releases, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy-map interface FastEthernet0/0
 FastEthernet0/0

  Service-policy output: test1

    Class-map: class-default (match-any)
      129 packets, 12562 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 129/12562
      shape (average) cir 1536000, bc 6144, be 6144
      target shape rate 1536000

      Service-policy : test2

        queue stats for all priority classes:

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0

        Class-map: RT (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp ef (46)
          Priority: 20% (307 kbps), burst bytes 7650, b/w exceed drops: 0


        Class-map: BH (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp af41 (34)
          Queueing
          queue limit 128 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 40% (614 kbps)

        Class-map: BL (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp af21 (18)
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 35% (537 kbps)
            Exp-weight-constant: 9 (1/512)
            Mean queue depth: 0 packets
            dscp     Transmitted   Random drop   Tail drop   Minimum   Maximum   Mark
                     pkts/bytes    pkts/bytes    pkts/bytes  thresh    thresh    prob

            af21     0/0           0/0           0/0         100       400       1/10

        Class-map: class-default (match-any)
          129 packets, 12562 bytes
```

```
30 second offered rate 0 bps, drop rate 0 bps
Match: any

queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 129/12562
```

The table below describes the significant fields shown in the display.

Table 59: show policy-map interface Field Descriptions—Configured for HQF

Field	Description
FastEthernet	Name of the interface.
service-policy output	Name of the output service policy applied to the specified interface.
class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. **Note** For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
Queueing	Indicates that queueing is enabled.
queue limit	Maximum number of packets that a queue can hold for a class policy configured in a policy map.
bandwidth	Indicates the percentage of bandwidth allocated for traffic queueing.

Field	Description
dscp	Differentiated services code point (DSCP). Values can be the following: • 0 to 63—Numerical DSCP values. The default value is 0. • af1 to af43—Assured forwarding (AF) DSCP values. • cs1 to cs7—Type of service (ToS) precedence values. • default—Default DSCP value. • ef—Expedited forwarding (EF) DSCP values.

Examples

The following example shows the new output fields associated with the QoS: Policies Aggregation Enhancements feature beginning in Cisco IOS XE Release 2.6 for subscriber statistics. The new output fields begin with the label "Account QoS Statistics."

```
Router# show policy-map interface port-channel 1.1

Port-channel1.1
   Service-policy input: input_policy
     Class-map: class-default (match-any)
       0 packets, 0 bytes
       5 minute offered rate 0000 bps, drop rate 0000 bps
       Match: any
       QoS Set
       dscp default
       No packet marking statistics available
   Service-policy output: Port-channel_1_subscriber
     Class-map: EF (match-any)
       105233 packets, 6734912 bytes
       5 minute offered rate 134000 bps, drop rate 0000 bps
       Match: dscp ef (46)
       Match: access-group name VLAN_REMARK_EF
       Match: qos-group 3
       Account QoS statistics
         Queueing
           Packets dropped 0 packets/0 bytes
       QoS Set
       cos 5
       No packet marking statistics available
       dscp ef
       No packet marking statistics available
     Class-map: AF4 (match-all)
       105234 packets, 6734976 bytes
       5 minute offered rate 134000 bps, drop rate 0000 bps
       Match: dscp cs4 (32)
       Account QoS statistics
         Queueing
           Packets dropped 0 packets/0 bytes
       QoS Set
       cos 4
       No packet marking statistics available
     Class-map: AF1 (match-any)
       315690 packets, 20204160 bytes
       5 minute offered rate 402000 bps, drop rate 0000 bps
       Match: dscp cs1 (8)
```

```
    Match: dscp af11 (10)
    Match: dscp af12 (12)
    Account QoS statistics
      Queueing
        Packets dropped 0 packets/0 bytes
    QoS Set
    cos 1
    No packet marking statistics available
  Class-map: class-default (match-any) fragment Port-channel_BE
    315677 packets, 20203328 bytes
    5 minute offered rate 402000 bps, drop rate 0000 bps
    Match: any
    Queueing
      queue limit 31250 bytes
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 315679/20203482
      bandwidth remaining ratio 1
```

Examples

The following example shows how to display the policer statistics (the packet and byte count). The output displays only the applicable count (either packets or bytes) with the actual number.

```
Router# show policy-map interface GigabitEthernet 3/1 input

GigabitEthernet3/1
  Service-policy input: in1
    Class-map: p1 (match-all)
      0 packets
      Match:  precedence 1
           QoS Set
             ip precedence 7
      police:
          cir 20 %
          cir 200000000 bps, bc 6250000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps
    Class-map: class-default (match-any)
      10000000 packets
      Match: any
      police:
          cir 20 %
          cir 200000000 bps, bc 6250000 bytes
        conformed 174304448 bytes; actions:
          transmit
        exceeded 465695552 bytes; actions:
          drop
        conformed 4287000 bps, exceed 11492000 bps
```

Examples

The following example shows how to display the statistics and the configurations of the input and output service policies that are attached to an interface:

```
Router# show policy-map interface GigabitEthernet 1/2/0

Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *23:02:40.857 pst Thu Mar 3 2011

 GigabitEthernet1/2/0

  Service-policy input: policy-in

    Class-map: class-exp-0 (match-all)
      6647740 packets, 9304674796 bytes
      30 second offered rate 3234000 bps, drop rate 0 bps
      Match: mpls experimental topmost 0
      QoS Set
```

```
      precedence 3
        Packets marked 6647740

  Class-map: class-default (match-any)
    1386487 packets, 1903797872 bytes
    30 second offered rate 658000 bps, drop rate 0 bps
    Match: any

Service-policy output: policy-out

  Class-map: class-pre-1 (match-all)
    2041355 packets, 2857897000 bytes
    30 second offered rate 986000 bps, drop rate 0 bps

    Match: ip precedence 1
    QoS Set
      mpls experimental topmost 1
        Packets marked 2041355

  Class-map: class-default (match-any)
    6129975 packets, 8575183331 bytes
    30 second offered rate 2960000 bps, drop rate 0 bps
    Match: any
```

The table below describes the significant fields shown in the display.

Table 60: show policy-map interface Field Descriptions—Cisco Catalyst 4000 Series Routers

Field	Description
class-map	Displays the class of traffic. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
conformed	Displays the action to be taken on packets conforming to a specified rate. Also displays the number of packets and bytes on which the action was taken.
drop	Indicates that the packet discarding action for all the packets belonging to the specified class has been configured.
exceeded	Displays the action to be taken on packets exceeding a specified rate. Displays the number of packets and bytes on which the action was taken.
match	Match criteria specified for the class of traffic.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
police	Indicates that the **police** command has been configured to enable traffic policing. Also displays the specified CIR, conform burst size, peak information rate (PIR), and peak burst size used for marking packets.

Field	Description
QoS Set	Indicates that QoS group (set) has been configured for the particular class.
service-policy input	Name of the input service policy applied to the specified interface.

Examples

The following example shows how to display the class maps configured for a pseudowire interface:

```
Router# show policy-map interface pseudowire2
 pseudowire2
  Service-policy output: pw_brr

    Class-map: prec1 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 1
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 1

    Class-map: prec2 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 2
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 2

    Class-map: prec3 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 3
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 3

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 4
Device#
```

The table below describes the significant fields shown in the display.

Table 61: show policy-map interface Field Descriptions—Pseudowire Policy Map Information

Field	Description
bandwidth	Indicates the percentage of bandwidth allocated for traffic queueing.
Class-map	Displays the class of traffic. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
Match	Match criteria specified for the class of traffic.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
Queueing	Indicates that queueing is enabled.
queue limit	Maximum number of packets that a queue can hold for a class policy configured in a policy map.
service-policy output	Name of the output service policy applied to the specified interface.

Related Commands

Command	Description
bandwidth remaining ratio	Specifies a bandwidth-remaining ratio for class queues and subinterface-level queues to determine the amount of unused (excess) bandwidth to allocate to the queue during congestion.
class-map	Creates a class map to be used for matching packets to a specified class.
compression header ip	Configures RTP or TCP IP header compression for a specific class.
drop	Configures a traffic class to discard packets belonging to a specific class.
match fr-dlci	Specifies the Frame Relay DLCI number as a match criterion in a class map.
match packet length (class-map)	Specifies the length of the Layer 3 packet in the IP header as a match criterion in a class map.

Command	Description
police	Configures traffic policing.
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
police (two rates)	Configures traffic policing using two rates, the CIR and the PIR.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Specifies that low-latency behavior must be given to a traffic class and configures multiple priority queues.
random-detect ecn	Enables ECN.
shape (percent)	Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface.
show class-map	Display all class maps and their matching criteria.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on a router or access server.
show mls qos	Displays MLS QoS information.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
show table-map	Displays the configuration of a specified table map or of all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

show pw-udp vc

To display information about pseudowire User Datagram Protocol (UDP) virtual circuits (VCs), use the **show pw-udp vc** command in user EXEC or privileged EXEC mode.

show pw-udp vc [**vcid** *id* [*max-vc*]] [**destination** *address*] [**detail**| **ssm id**]

Syntax Description

vcid *id*	(Optional) Specifies the minimum VC ID. The range is 1 to 4294967295.
max-vc	(Optional) Maximum VC ID. The range is 1 to 4294967295.
destination *address*	(Optional) Specifies the destination hostname or IP address of the VC.
detail	(Optional) Displays detailed information about the UDP VCs.
ssm id	(Optional) Displays the Source Specific Multicast (SSM) information.

Command Default

If no arguments or keywords are specified, information about all pseudowire UDP VCs is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced.

Examples

The following is sample output for the **show pw-udp vc** command:

```
Router# show pw-udp vc 100 200 detail
Local intf        Local circuit              VC ID      Status
----------------- -------------------------- ---------- ---------------
CE4/2/0:0         CESoPSN Basic              100        established
  LAddr: 10.1.1.151      LPort: 50100
  RAddr: 10.1.1.153      RPort: 50100
  VC statistics:
    transit packet totals: receive 770614, send 770613
    transit byte totals:   receive 151040344, send 50089845
    transit packet drops:  receive 0, send 0, seq error 0
CE4/2/1:0         CESoPSN Basic              200        established
  LAddr: 10.1.1.151      LPort: 50200
  RAddr: 10.1.1.153      RPort: 50200
```

```
VC statistics:
  transit packet totals: receive 770614, send 770613
  transit byte totals:   receive 151040344, send 50089845
  transit packet drops:  receive 0, send 0, seq error 0
```

The table below describes the significant fields shown in the display.

Table 62: show pw-udp vc Field Descriptions

Field	Description
Local intf	Name of the access circuit (AC) interface.
Local circuit	Interface type. For example, CESoPSN Basic.
VC ID	Virtual circuit ID.
Status	State of the pseudowire VC with the following possible values: • Provisioned-Pseudowire has been provisioned but the data plane is not up. • Checkpoint wait-Pseudowire has been provisioned but still waiting for the checkpoint information from the active RP(need this information to proceed to the activating state). This state is applicable only on the standby RP. • Activating-Data plane has been activated, but not yet turned active. • Established-Data plane has been established and ready to forward traffic.

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.

show running interface auto-template

To display configuration information for a tunnel's interface, use the **show running interface auto-template** command in privileged EXEC mode.

show running interface auto-template *num*

Syntax Description

num	Number of the tunnel interface for which you want to display information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The space before the *num* argument is optional.

Examples

The following is output from the **show running interface auto-template** command:

```
Router# show running interface auto-template 1
interface auto-template1
 ip unnumbered Loopback0
 no ip directed-broadcast
 no keepalive
 tunnel destination access-list 1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 dynamic
```

The table below describes the significant fields shown in the display.

Table 63: show running interface auto-template Field Descriptions

Field	Description
ip unnumbered Loopback0	Indicates the type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.

Field	Description
no ip directed-broadcast	Indicates that no IP broadcast addresses are used for the autotunnel interface.
no keepalive	Indicates that no keepalives are set for the autotunnel interface.
tunnel destination access-list 1	Indicates that access list 1 is the access list that the template interface will use for obtaining the autotunnel interface destination address.
tunnel mode mpls traffic-eng	Indicates that the mode of the autotunnel is set to Multiprotocol Label Switching (MPLS) for traffic engineering.
tunnel mpls traffic-eng autoroute announce	Indicates that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation.
tunnel mpls traffic-eng path-option 1 dynamic	Indicates that a path option (path-option1) for the label switch router (LSR) for the MPLS traffic engineering (TE) mesh tunnel is configured dynamically.

Related Commands

Command	Description
interface auto-template	Creates the template interface.
tunnel destination access-list	Specifies the access list that the template interface will use for obtaining the mesh tunnel interface destination address.

show running-config vrf

To display the subset of the running configuration of a router that is linked to a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance or to all VRFs configured on the router, use the **show running-config vrf** command in user EXEC or privileged EXEC mode.

show running-config vrf [*vrf-name*]

Syntax Description

vrf-name	(Optional) Name of the VRF configuration that you want to display.

Command Default

If you do not specify a *vrf-name* argument, the running configurations of all VRFs on the router are displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was modified. It was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **show running-config vrf** command to display a specific VRF configuration or to display all VRF configurations on the router. To display the configuration of a specific VRF, enter the name of the VRF as an argument to the command.

This command displays the following elements of the VRF configuration:

- The VRF submode configuration
- The routing protocol and static routing configurations associated with the VRF
- The configuration of the interfaces in the VRF, which includes the configuration of any owning controller and physical interface for a subinterface

Examples

The following is sample output from the **show running-config vrf** command. It includes a base VRF configuration for VRF vpn3 and Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) configurations associated with VRF vpn3.

```
Router# show running-config
 vrf vpn3
Building configuration...
Current configuration : 604 bytes
ip vrf vpn3
 rd 100:3
 route-target export 100:3
 route-target import 100:3
!
!
interface Loopback1
 ip vrf forwarding vpn3
 ip address 10.43.43.43 255.255.255.255
!
interface Ethernet6/0
 ip vrf forwarding vpn3
 ip address 172.17.0.1 255.0.0.0
 no ip redirects
 duplex half
!
router bgp 100
!
address-family ipv4 vrf vpn3
 redistribute connected
 redistribute ospf 101 match external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
 !
router ospf 101 vrf vpn3
 log-adjacency-changes
 area 1 sham-link 10.43.43.43 10.23.23.23 cost 10
 network 172.17.0.0 0.255.255.255 area 1
!
end
```

The table below describes the significant fields shown in the display.

Table 64: show running-config vrf Field Descriptions

Field	Description
Current configuration: 604 bytes	Number of bytes (604) in the VRF vpn3 configuration.
ip vrf vpn3	Name of the VRF (vpn3) for which the configuration is displayed.
rd 100:3	Identifies the route distinguisher (100:3) for VRF vpn3.

Field	Description
route-target export 100:3 route-target import 100:3	Specifies the route-target extended community for VRF vpn3. • Routes tagged with route-target export 100:3 are exported from VRF vpn3. • Routes tagged with the route-target import 100:3 are imported into VRF vpn3.
interface Loopback1	Virtual interface associated with VRF vpn3.
ip vrf forwarding vpn3	Associates VRF vpn3 with the named interface.
ip address 10.43.43.43 255.255.255.255	IP address of the loopback interface.
interface Ethernet6/0	Interface associated with VRF vpn3.
ip address 172.17.0.1 255.0.0.0	IP address of the Ethernet interface.
router bgp 100	Sets up a BGP routing process for the router with autonomous system number 100.
address-family ipv4 vrf vpn3	Sets up a routing session for VRF vpn3 using standard IP Version 4 address prefixes.
redistribute connected	Redistributes routes automatically established by IP on an interface into the BGP routing domain.
redistribute ospf 101 match external 1 external 2	Redistribute routes from the OSPF 101 routing domain into the BGP routing domain.
router ospf 101 vrf vpn3	Set up an OSPF routing process and associates VRF vpn3 with OSPF VRF processes.
area 1 sham-link 10.43.43.43 10.23.23.23 cost 10	Configure a sham-link interface on a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) VPN backbone. • 1 is the ID number of the OSPF area assigned to the sham-link. • 10.43.43.43 is the IP address of the source PE router. • 10.23.23.23 is the IP address of the destination PE router. • 10 is the OSPF cost to send IP packets over the sham-link interface.

Field	Description
network 172.17.0.0 0.255.255.255 area 1	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip interface	Displays the usability status of interfaces configured for IP.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
show running-config interface	Displays the configuration for a specific interface.

show spanning-tree mst

To display the information about the Multiple Spanning Tree (MST) protocol, use the **showspanning-treemst** command in privileged EXEC mode.

show spanning-tree mst [*instance-id-number* **[detail]** [*interface*]| **configuration [digest]**| **detail**| **interface** *interface* **[detail]**]

Syntax Description

instance-id-number	(Optional) Instance identification number; valid values are from 0 to 4094.
detail	(Optional) Displays detailed information about the MST protocol.
interface	(Optional) Displays the information about the interfaces. The valid interface are **atm**, **gigabitethernet**, **port-channel**, and **vlan**. See the "Usage Guidelines" section for valid number values.
configuration	(Optional) Displays information about the region configuration.
digest	(Optional) Displays information about the message digest 5 (MD5) algorithm included in the current MST configuration identifier (MSTCI).
interface	(Optional) Displays information about the interface type; possible interface types are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, **ge-wan**, **port-channel**, and **vlan**.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command was added for the Supervisor Engine 2.

Release	Modification

12.2(18)SXF	This command was modified. The changes were as follows:
	• The range of valid values for the instance-id-number changed to 0 to 4094.
	• The output of the **show spanning-tree mst configuration** command changed as follows:
	  • Displays the instance identification from 0 to 4094.
	  • Displays the number of the currently configured instances from 0 to 65.
	  • Adds the **digest** keyword to display the MD5 digest of the VLAN-to-instance mapping of the MST configuration.
	• The output of the **show spanning-tree mst detail** command changed as follows:
	  • The Regional Root field replaced the IST Master field.
	  • The Internal Path field replaced the Path Cost field.
	  • The Designated Regional Root field replaced the Designated IST Master field.
	  • The txholdcount field was added in the Operational parameter line.
	• Displays new roles for all MST instances on the common and internal spanning tree (CIST) root port.
	• Displays the prestandard flag.

12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

The valid values for the *interface* argument depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

The number of valid values for **port-channel** *number* are a maximum of 64 values ranging from 1 to 282. The **port-channel** *number* values from 257 to 282 are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

The number of valid values for **vlan** are from 1 to 4094.

In the output display of the **show spanning-tree mst configuration** command, a warning message may be displayed. This message appears if you do not map secondary VLANs to the same instance as the associated

primary VLAN. The display includes a list of the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

In the output display of the **show spanning-tree mst configuration digest** command, if the output applies to both standard and prestandard bridges at the same time on a per-port basis, two different digests are displayed.

If you configure a port to transmit prestandard PortFast bridge protocol data units (BPDUs) only, the prestandard flag displays in the **show spanning-tree** commands. The variations of the prestandard flag are as follows:

- Pre-STD (or pre-standard in long format)--This flag is displayed if the port is configured to transmit prestandard BPDUs and if a prestandard neighbor bridge has been detected on this interface.
- Pre-STD-Cf (or pre-standard (config) in long format)--This flag is displayed if the port is configured to transmit prestandard BPDUs but a prestandard BPDU has not been received on the port, the autodetection mechanism has failed, or a misconfiguration, if there is no prestandard neighbor, has occurred.
- Pre-STD-Rx (or prestandard (rcvd) in long format)--This flag is displayed when a prestandard BPDU has been received on the port, but it has not been configured to send prestandard BPDUs. The port will send prestandard BPDUs, but Cisco recommends that you change the port configuration so that the interaction with the prestandard neighbor does not rely only on the autodetection mechanism.

If the configuration is not prestandard compliant (for example, a single MST instance has an ID that is greater than or equal to 16,) the prestandard digest is not computed and the following output is displayed:

```
Device# show spanning-tree mst configuration digest

Name      [region1]
Revision  2     Instances configured 3
Digest          0x3C60DBF24B03EBF09C5922F456D18A03
Pre-std Digest  N/A, configuration not pre-standard compatible
```

MST BPDUs include an MSTCI that consists of the region name, region revision, and an MD5 digest of the VLAN-to-instance mapping of the MST configuration.

See the **show spanning-tree mst** command field description table for output descriptions.

Examples

The following example shows how to display information about the region configuration:

```
Device# show spanning-tree mst configuration

Name      [train]
Revision  2702
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-9,11-19,21-29,31-39,41-4094
1         10,20,30,40
---------------------------------------------------------------------------
```

The following example shows how to display additional MST-protocol values:

```
Device# show spanning-tree mst 3 detail

###### MST03 vlans mapped: 3,3000-3999
Bridge address 0002.172c.f400 priority 32771 (32768 sysid 3)
Root this switch for MST03
GigabitEthernet1/1 of MST03 is boundary forwarding
Port info port id 128.1 priority 128
cost 20000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port
id 128.1
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 4, received 0
```

```
FastEthernet4/1 of MST03 is designated forwarding
Port info port id 128.193 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 254, received 1
FastEthernet4/2 of MST03 is backup blocking
Port info port id 128.194 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 2 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 3, received 252
```

The following example shows how to display MST information for a specific interface:

```
Device# show spanning-tree mst 0 interface fastethernet 4/1 detail

Edge port: no (trunk) port guard : none
(default)
Link type: point-to-point (point-to-point) bpdu filter: disable
(default)
Boundary : internal bpdu guard : disable
(default)
FastEthernet4/1 of MST00 is designated forwarding
Vlans mapped to MST00 1-2,4-2999,4000-4094
Port info port id 128.193 priority 128 cost
200000
Designated root address 0050.3e66.d000 priority 8193
cost 20004
Designated ist master address 0002.172c.f400 priority 49152
cost 0
Designated bridge address 0002.172c.f400 priority 49152 port id
128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 492, received 3
```

The following example shows how to display the MD5 digest included in the current MSTCI:

```
Device# show spanning-tree mst configuration digest

Name      [mst-config]
Revision  10    Instances configured 25
Digest          0x40D5ECA178C657835C83BBCB16723192
Pre-std Digest  0x27BF112A75B72781ED928D9EC5BB4251
```

The following example displays the new master role for all MST instances at the boundary of the region on the port that is a CIST root port:

```
Device# show spanning-tree mst interface fastethernet4/9

FastEthernet4/9 of MST00 is root forwarding
Edge port: no             (default)        port guard : none        (default)
Link type: point-to-point (auto)           bpdu filter: disable     (default)
Boundary : boundary       (RSTP)           bpdu guard : disable     (default)
Bpdus sent 3428, received 6771
Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- --------------------------------
0        Root FWD 200000    128.201  2-7,10,12-99,101-999,2001-3999,4001-4094
8        Mstr FWD 200000    128.201  8,4000
9        Mstr FWD 200000    128.201  1,9,100
11       Mstr FWD 200000    128.201  11,1000-2000
```

The table below describes the significant fields shown in the displays.

Table 65: show spanning-tree mst Field Descriptions

Field	Description
Name	Name of the configured MST.
Revision	Revision number.
Digest	Digest number of the instance.
Instance	Instance number.
Timers	Summary of the timers set for the MST.
Edge port	Status of the port fast.
port guard	Type of port guard.
Link type	The link type.
bpdu filter	Status of the BPDU filter.
Boundary	Boundary type.
bpdu guard	Status of the BPDU guard.
Role	Role of the instance.
Sts	Status of the instance.
Cost	Path cost of the port.
Prio.Nbr	Priority number.
Vlans mapped	Mapped VLANs.

Related Commands

Command	Description
spanning-tree mst	Sets the path cost and port-priority parameters for any MST instance.
spanning-tree mst forward-time	Sets the forward-delay timer for all the instances on the Cisco 7600 series router.
spanning-tree mst hello-time	Sets the hello-time delay timer for all the instances on the Cisco 7600 series router.

Command	Description
spanning-tree mst max-hops	Specifies the number of possible hops in the region before a BPDU is discarded.
spanning-tree mst root	Designates the primary and secondary root, sets the bridge priority, and sets the timer value for an instance.

show ssm group

To display information about groups in the source-specific mapping (SSM) database, use the **show ssm group** command in user EXEC mode.

show ssm group peer ip address group id

Syntax Description

peer ip address	Displays information about groups in the SSM database associated with the specified peer ip address.
group id	Displays information about the specified group in the SSM database associated with the specified peer ip address.

Command Modes

User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.

Examples

The following example lists the active and standby segment pairs associated with each peer IP address and group identifier.

```
Device# show ssm group

Active              Standby
IP Address       Group ID       Segment/Switch      Segment/Switch
==========================================================================
2.1.1.2             6            8215/4115           4116/8210
```

The following example displays the number of active and standby segment pairs associated with each peer IP address and group identifier:

```
Device# show ssm group 2.1.1.2 6 summary

IP Address        Group ID      Group Members
=============================================
2.1.1.2              6              1
```

Related Commands

Command	Description
show platform	Displays platform information.
show atm vc	Displays all ATM permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) and traffic information.

show tech-support mpls

To generate a report of all Multiprotocol Label Switching (MPLS)-related information, use the **show tech-support mpls** command in privileged EXEC mode.

show tech-support mpls [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays MPLS information about the specified VPN routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command is useful when you contact technical support personnel with questions regarding MPLS. The show tech-support mpls command generates a series of reports. The show tech-support mpls command is equivalent to issuing the following commands:

MPLS Forwarding Information Commands

show adjacency detail show cef drop show cef events show cef not-cef-switched show cef state show interface accounting | exclude sab show interfaces statistic | exclude sabl show ip cef adjacency discard show ip cef adjacency drop show ip cef adjacency glean show ip cef adjacency null show ip cef adjacency punt show ip cef detail internal show ip cef inconsistency show ip cef summary show ip cef unresolved internal show ip interfaces show ip route show ip traffic show mpls forwarding-table detail show mpls interfaces all show mpls interfaces all internal show mpls label range show mpls static binding

MPLS Forwarding: Cell Mode (LC-ATM) Commands

Note These commands are not supported on Cisco 10000 series routers.

show atm vc show controller vsi descriptor show controller vsi session show controller vsi status show XTagATM cross-connect show XTagATM cross-connect traffic show XTagATM vc

MPLS Forwarding: Quality of Service (QoS) Commands

Note These commands are not supported on Cisco 10000 series routers.

show interfaces fair-queue show interfaces mpls-exp show interfaces precedence

MPLS Label Distribution Protocol (LDP) Commands

show mpls atm-ldp bindings show mpls atm-ldp bindwait show mpls atm-ldp capability show mpls atm-ldp summary <===== Not supported on Cisco 10000 series routers**show mpls ip binding detail show mpls ldp backoff show mpls ldp discovery all detail show mpls ldp neighbor all show mpls ldp neighbor detail show mpls ldp parameters**

MPLS LDP: Stateful Switchover/Nonstop Forwarding (SSO/NSF) Support and Graceful Restart Commands

show mpls checkpoint label-binding show mpls ldp checkpoint show mpls ldp graceful-restart show mpls ldp neighbor graceful-restart

MPLS Traffic Engineering Commands

show ip ospf database opaque-area show ip ospf database opaque-link show ip ospf mpls traffic-eng fragment show ip ospf mpls traffic-eng link show ip rsvp fast-reroute detail show ip rsvp installed show ip rsvp interface show ip rsvp neighbor show ip rsvp reservation show ip rsvp sender show isis mpls traffic-eng adjacency-log show isis mpls traffic-eng advertisements show isis mpls traffic-eng tunnel show mpls traffic-end link-management interfaces show mpls traffic-eng autoroute show mpls traffic-eng fast-reroute database detail show mpls traffic-eng fast-reroute log reroutes show mpls traffic-eng forwarding adjacency show mpls traffic-eng link-management admission-control show mpls traffic-eng link-management advertisements show mpls traffic-eng link-management bandwidth-allocation show mpls traffic-eng link-management summary show mpls traffic-eng topology show mpls traffic-eng tunnels show mpls traffic-eng tunnels brief show mpls traffic-eng tunnels statics summary

MPLS VPN Commands

show ip bgp labels show ip bgp neighbors show ip bgp vpnv4 all show ip bgp vpnv4 all labels show ip bgp vpnv4 all summary show ip vrf detail show ip vrf interfaces show ip vrf select

Any Transport over MPLS (AToM) Commands

show mpls l2transport binding show mpls l2transport hw-capability show mpls l2transport summary show mpls l2transport vc detail

MPLS VPN VRF-Specific Commands

show ip bgp vpnv4 vpn-name **dampening flap-statistics show ip bgp vpnv4**vpn-name **labels show ip bgp vpnv4**vpn-name **peer-group show ip bgp vpnv4**vpn-name **summary show ip bgp vpnv4 vrf**vpn-name **neighbors show ip vrf detail**vpn-name**show ip vrf interfaces**vpn-name**show ip vrf select**vpn-name

MPLS VPN VRF-Specific Forwarding Commands

show ip cef vrf vpn-name **adjacency discard show ip cef vrf**vpn-name **adjacency drop show ip cef vrf**vpn-name **adjacency glean show ip cef vrf**vpn-name **adjacency null show ip cef vrf**vpn-name **adjacency punt show ip cef vrf**vpn-name **inconsistency show ip cef vrf**vpn-name **internal show ip cef vrf**vpn-name **summary show ip route vrf**vpn-name**show ip vrf interfaces**vpn-name **show mpls forwarding-table vrf**vpn-name**show mpls interface vrf**vpn-name **detail**

MPLS LDP VRF-Specific Commands

show mpls ip binding vrf vpn-name **atm detail show mpls ip binding vrf**vpn-name **detail show mpls ip binding vrf**vpn-name **local show mpls ip binding vrf**vpn-name **summary show mpls ldp discovery vrf**vpn-name **detail show mpls ldp neighbor vrf**vpn-name **detail**

MPLS LDP VRF Graceful Restart-Specific Commands

show mpls ldp neighbor vrf vpn-name **graceful-restart**

These commands are documented in individual feature modules or Cisco IOS Release 12.2 command references. Refer to the individual commands for information about the output these commands generate.

Examples

The following example displays an abbreviated version of the **show tech-support mpls** command output:

```
Router# show tech-support mpls
------------------ show version ------------------
Cisco IOS Software, 7300 Software (C7300-P-M), Version 12.2(27)SBC, RELEASE SOF)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Sat 10-Sep-05 17:44 by ssearch
.
.
.
------------------ show running-config ------------------
Building configuration...
Current configuration : 1827 bytes
.
.
.
------------------ show mpls ldp graceful-restart ------------------
LDP Graceful Restart is disabled
Neighbor Liveness Timer: 120 seconds
Max Recovery Time: 120 seconds
Forwarding State Holding Time: 600 seconds
```

Related Commands

Command	Description
show tech-support	Displays the equivalent of the show buffers, show controllers, show interfaces, show process, show process memory, show running-config, show stacks, and show version commands.

show vfi

To display information related to a virtual forwarding instance (VFI), use the **show vfi** command in privileged EXEC mode.

show vfi [**checkpoint [summary]**| **mac static address**| **memory [detail]**| **name** *vfi-name* [**checkpoint**| **mac static address**]| **neighbor** *ip-addr* **vcid** *vcid* **mac static address**]

Syntax Description

checkpoint	(Optional) Displays VFI checkpoint information.
summary	(Optional) Displays a summary of VFI checkpoint information.
mac static address	(Optional) Displays static MAC addresses in a bridge domain.
memory	(Optional) Displays VFI memory usage.
detail	(Optional) Displays details of VFI memory usage.
name	(Optional) Displays information for the specified VFI.
vfi-name	(Optional) Name of a specific VFI.
neighbor	(Optional) Displays VFI neighbor information.
ip-addr	(Optional) IP address of the neighbor (remote peer).
vcid	(Optional) Displays the virtual circuit (VC) ID for a peer.
vcid	(Optional) Integer from 1 to 4294967295 that identifies the virtual circuit.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRA	This command was updated to display the Virtual Private Network (VPN) ID.
12.2(33)SRC	This command was modified. The **name** keyword was added.
12.2(33)SRE	This command was modified. The following keywords and arguments were added: **address**, **checkpoint**, **detail**, **mac**, **memory**, **neighbor** *ip-addr*, **static**, **summary**, and **vcid** *vcid*.

Release	Modification
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Use this command to verify VFI configurations and for troubleshooting.

Examples

The following example shows status for a VFI named VPLS-2. The VC ID in the output represents the VPN ID; the virtual circuit is identified by the combination of the destination address and the virtual circuit ID.

```
Router# show vfi name VPLS-2
VFI name: VPLS-2, state: up
  VPN ID: 100
  Local attachment circuits:
    Vlan2
  Neighbors connected via pseudowires:
  Peer Address     VC ID     Split-horizon
  10.1.1.1          2             Y
  10.1.1.2          2             Y
  10.2.2.3          2             N
```

The table below describes the significant fields shown in the display.

Table 66: show vfi name Field Descriptions

Field	Description
VFI name	The name assigned to the VFI.
state	The status of the VFI (up or down).
Local attachment circuits	The interface or VLAN assigned to the VFI.
Peer Address	The IP address of the peer router.
VC ID	The VC ID assigned to the pseudowire.
Split-horizon	Indicates whether split horizon is enabled (Y) or disabled (N).

The following is sample output from the show vfi command. For the Virtual Private LAN Service (VPLS) autodiscovery feature, the command output from the command output includes autodiscovery information, as shown in the following example:

Note VPLS autodiscovery is not supported in Cisco IOS Release 12.2(50)SY.

```
Router# show vfi
```

```
Legend: RT= Route-target, S=Split-horizon, Y=Yes, N=No
VFI name: VPLS1, state: up, type: multipoint
  VPN ID: 10, VPLS-ID: 9:10
  RD: 9:10, RT: 10.10.10.10:150
  Local attachment circuits:
    Ethernet0/0.2
  Neighbors connected via pseudowires:
  Peer Address      VC ID       Discovered Router ID       S
  10.7.7.1           10          10.7.7.1                  Y
  10.7.7.2           10          10.1.1.2                  Y
  10.7.7.3           10          10.1.1.3                  Y
  10.7.7.4           10          10.1.1.4                  Y
  10.7.7.5           10          -                         Y
VFI name: VPLS2 state: up, type: multipoint
  VPN ID: 11, VPLS-ID: 10.9.9.9:2345
  RD: 10:11, RT: 10.4.4.4:151
  Local attachment circuits:
    Ethernet0/0.3
  Neighbors connected via pseudowires:
  Peer Address      VC ID       Discovered Router ID      S
  10.7.7.1           11          10.7.7.1                 Y
  10.7.7.2           11          10.1.1.5                 Y
```

The table below describes the significant fields in the output related to VPLS autodiscovery.

Table 67: show vfi Field Descriptions for VPLS Autodiscovery

Field	Description
VPLS-ID	The identifier of the VPLS domain. VPLS autodiscovery automatically generates a VPLS ID using the Border Gateway Protocol (BGP) autonomous system number and the configured VFI VPN ID.
RD	The route distinguisher (RD) to distribute endpoint information. VPLS autodiscovery automatically generates an RD using the BGP autonomous system number and the configured VFI VPN ID.
RT	The route target (RT). VPLS autodiscovery automatically generates a route target using the lower 6 bytes of the RD and VPLS ID.
Discovered Router ID	A unique identifier assigned to the PE router. VPLS autodiscovery automatically generates the router ID using the Multiprotocol Label Switching (MPLS) global router ID.

The following is sample output from the **show vfi** command for a specified VFI named H-VPLS-A-VFI. Because the optional **name** keyword is entered, the checkpoint information for the specific VFI is displayed.

```
Router# show vfi name H-VPLS-A-VFI checkpoint
VFI Active RP
Checkpointing: Allowed
ISSU Client id: 2092, Session id: 65543, Compatible with peer
VFI VFI AC VFI PW
Bulk-sync 1 1 3
Checkpoint failures: 0 3 21
Recovered at switchover: 0 0 0
Recovery failures: 0 0 0
```

```
Legend: C=Checkpointed
VFI name: H-VPLS-A-VFI, state: up, type: multipoint
VPN ID: 12, Internal ID 1 C
Local attachment circuits:
Vlan200 16387 / 8195 C
Neighbors connected via pseudowires:
Peer ID VC ID SSM IDs
10.0.0.12 12 4096 / 12292 C
10.0.0.15 12 8193 / 16389 C
10.0.0.14 12 12290 / 20486 C
```

The table below describes the significant fields shown in the display.

Table 68: show vfi name checkpointing Field Descriptions

Field	Description
Checkpointing	Specifies whether checkpointing is allowed on this VFI.
ISSU Client id	The ID number assigned to the In-Service Software Upgrade (ISSU) client.
Session id	The current VFI session ID number.
VFI	Status of the VFI.
VFI AC	Status of the Attachment Circuit (AC).
VFI PW	Status of the pseudowire for this VFI.
Checkpoint failures	The number of checkpoint failures on this interface.
Recovered at switchover	The number of checkpoint failures recovered on this interface at switchover.
Recovery failures	The number of checkpoint failures recovered on this interface.
VFI name	The name assigned to the VFI.
state	Status of the VFI (up or down).
type	VFI type.
VPN ID	The ID number of the VPN.
Local attachment circuits	The Interface or VLAN assigned to the VFI.
Peer ID	The IP address of the peer router.
VC ID	The VC ID assigned to the pseudowire.

The following is sample output from the **show vfi** command using the **memory** and **detail** keywords.

```
Router# show vfi memory detail
  VFI memory                  In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  VFI structs                 In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  vfi_context_t           :        --        --/--           --    52   --/--
  vfi_circuit_retry       :        --        --/--           --    24   --/--
  Total allocated: 0.000 Mb, 0 Kb, 0 bytes
```

The table below describes the significant fields shown in the display.

Table 69: show vfi memory detail Field Descriptions

Field	Description
VFI memory	Amount of memory available for use.
In-use	Amount of memory actively used.
Asked-For/Allocated	Amount of memory originally requested/amount of memory allocated.
Count	Number of pieces of this named memory that exist.
Size	Size of the memory allocated by the system for this chunk.
Config/Max	Number of chunklets per chunk.
VFI structs	Data structures being used.
Total allocated	Total allocated memory.

Related Commands

Command	Description
show checkpoint	Displays information about the Checkpoint Facility (CF) subsystem on a Cisco CMTS.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

show vrf

To display the defined Virtual Private Network (VPN) routing and forwarding (VRF) instances, use the **show vrf** command in user EXEC or privileged EXEC mode.

show vrf [**ipv4**| **ipv6**] [**interface**| **brief**| **detail**| **id**| **select**| **lock**] [*vrf-name*]

Syntax Description

ipv4	(Optional) Displays IPv4 address family-type VRF instances.
ipv6	(Optional) Displays IPv6 address family-type VRF instances.
interface	(Optional) Displays the interface associated with the specified VRF instances.
brief	(Optional) Displays brief information about the specified VRF instances.
detail	(Optional) Displays detailed information about the specified VRF instances.
id	(Optional) Displays VPN-ID information for the specified VRF instances.
select	(Optional) Displays selection information for the specified VRF instances.
lock	(Optional) Displays VPN lock information for the specified VRF instances.
vrf-name	(Optional) Name assigned to a VRF.

Command Default

If you do not specify any arguments or keywords, the command displays concise information about all configured VRFs.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. When backup paths have been created either through the Prefix Independent Convergence or Best External feature, the output of the **show vrf detail** command displays the following line: Prefix protection with additional path enabled
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **show vrf** command to display information about specified VRF instances or all VRF instances. Specify no arguments or keywords to display information on all VRF instances.

Examples

The following sample output from the **show vrf** command displays brief information about all configured VRF instances:

```
Router# show vrf

  Name                              Default RD          Protocols   Interfaces
  N1                                100:0               ipv4,ipv6
  V1                                1:1                 ipv4        Lo1
  V2                                2:2                 ipv4,ipv6   Et0/1.1
                                                                    Et0/1.2
                                                                    Et0/1.3
  V3                                3:3                 ipv4        Lo3
                                                                    Et0/1.4
```

The table below describes the significant fields shown in the display.

Table 70: show vrf Field Descriptions

Field	Description
Name	Name of the VRF instance.
Default RD	The default route distinguisher (RD) for the specified VRF instances.
Protocols	The address family protocol type for the specified VRF instance.
Interfaces	The network interface associated with the VRF instance.

The following sample output from the **show vrf detail** command that displays information for a VRF named cisco:.

```
Router# show vrf detail

VRF cisco1; default RD 100:1; default VPNID <not set>
  Interfaces:
    Ethernet0/0                 Loopback10
Address family ipv4 (Table ID = 0x1):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
Address family ipv6 (Table ID = 0xE000001):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
```

The table below describes the significant fields shown in the display.

Table 71: show vrf detail Field Descriptions

Field	Description
default RD 100:1	The RD given to this VRF.
Interfaces:	Interfaces to which the VRF is attached.
Export VPN route-target communities RT:100:1	Route-target VPN extended communities to be exported.
Import VPN route-target communities RT:100:1	Route-target VPN extended communities to be imported.

The following example displays output from the **show vrf detail** command when backup paths have been created either through the Prefix Independent Convergence or Best External feature. The output of the **show vrf detail** command displays the following line:

Prefix protection with additional path enabled

```
Router# show vrf detail

VRF vpn1 (VRF Id = 1); default RD 1:1; default VPNID <not set>
  Interfaces:
    Et1/1
Address family ipv4 (Table ID = 1 (0x1)):
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No export route-map
```

```
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix

Prefix protection with additional path enabled
Address family ipv6 not active.
```

The following sample output from the **show vrf lock** command displays VPN lock information:

```
Router# show vrf lock

VRF Name: Mgmt-intf; VRF id = 4085 (0xFF5)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :108
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
VRF Name: vpn1; VRF id = 1 (0x1)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :100
         Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
```

Related Commands

Command	Description
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.
vrf forwarding	Associates a VRF instance with an interface or subinterface.

show xconnect

To display information about xconnect attachment circuits and pseudowires, use the **show xconnect** command in user EXEC or privileged EXEC mode.

show xconnect {{**all**| **interface** *type number*} **[detail]**| **peer** *ip-address* {**all**| **vcid** *vcid-value*} **[detail]**| **pwmib** [**peer** *ip-address vcid-value*]}

Cisco IOS SR and S Trains

show xconnect {{**all**| **interface** *type number*| **memory**| **rib**} **[detail] [checkpoint]**| **peer** *ip-address* {**all**| **vcid** *vcid-value*} **[detail]**| **pwmib** [**peer** *ip-address vcid-value*]}**monitor**

Cisco uBR10012 Router and Cisco uBR7200 Series Universal Broadband Routers

show xconnect {**all**| **peer** *ip-address* {**all**| **vcid** *vcid-value*}| **pwmib** [**peer** *ip-address vcid-value*]} **[detail]**

Syntax Description

all	Displays information about all xconnect attachment circuits and pseudowires.
interface	Displays information about xconnect attachment circuits and pseudowires on the specified interface.

type	Interface type. For more information, use the question mark (?) online help function. Valid values for the *type* argument are as follows: • **atm** *number*—Displays xconnect information for a specific ATM interface or subinterface. • **atm** *number* **vp** *vpi-value*—Displays virtual path (VP) xconnect information for a specific ATM virtual path identifier (VPI). The **show xconnect atm** *number* **vp** *vpi-value* command will not display information about virtual circuit (VC) xconnects using the specified VPI. • **atm** *number* **vc** *vpi-value*/*vci-value*—Displays VC xconnect information for a specific ATM VPI and virtual circuit identifier (VCI) combination. • **ethernet** *number*—Displays port-mode xconnect information for a specific Ethernet interface or subinterface. • **fastethernet** *number*—Displays port-mode xconnect information for a specific Fast Ethernet interface or subinterface. • **serial** *number*—Displays xconnect information for a specific serial interface. • **serial** *number dlci-number*—Displays xconnect information for a specific Frame Relay data-link connection identifier (DLCI).
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
detail	(Optional) Displays detailed information about the specified xconnect attachment circuits and pseudowires.
peer	Displays information about xconnect attachment circuits and pseudowires associated with the specified peer.
ip-address	The IP address of the peer.
all	Displays all xconnect information associated with the specified peer IP address.

vcid	Displays xconnect information associated with the specified peer IP address and the specified VC ID.
vcid-value	The VC ID value.
pwmib	Displays information about the pseudowire MIB.
memory	Displays information about the xconnect memory usage.
rib	Displays information about the pseudowire Routing Information Base (RIB).
checkpoint	(Optional) Displays the autodiscovered pseudowire information that is checkpointed to the standby Route Processor (RP).
monitor	Displays information about xconnect monitor usage for bidirectional forwarding detection (BFD).

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was modified. The **rib** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **pwmib** keyword was added.
12.2(33)SRC	This command was modified in a release earlier than Cisco IOS Release 12.2(33)SRC. The **memory** keyword was added.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Release	Modification
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S. The output of the **show xconnect rib** command and the **show xconnect rib detail** command was modified to support dynamic pseudowire switching on Autonomous System Boundary Routers (ASRBs). The **checkpoint** keyword was added.
12.2(33)SCF	This command was modified. The output was changed to display backup pseudowire information.
15.1(3)S	This command was integrated into Cisco IOS Release 15.1(3)S. The**monitor** keyword was added.

Usage Guidelines

You can use the **show xconnect** command to display, sort, and filter basic information about all xconnect attachment circuits and pseudowires.

You can use the **show xconnect** command output to help determine the appropriate steps required to troubleshoot an xconnect configuration problem. More specific information about a particular type of xconnect can be displayed using the commands listed in the “Related Commands” table.

Examples

The following example shows the **show xconnect all** command output in the brief (default) display format:

```
Router# show xconnect all

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, SB=Standby, RV=Recovering, NH=No Hardware
XC ST     Segment 1                         S1 Segment 2                            S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Et0/0(Ethernet)              UP mpls 10.55.55.2:1000              UP
UP     ac   Se7/0(PPP)                   UP mpls 10.55.55.2:2175              UP
UP pri ac   Se6/0:230(FR DLCI)           UP mpls 10.55.55.2:2230              UP
IA sec ac   Se6/0:230(FR DLCI)           UP mpls 10.55.55.3:2231              DN
UP     ac   Se4/0(HDLC)                 UP mpls 10.55.55.2:4000              UP
UP     ac   Se6/0:500(FR DLCI)          UP l2tp 10.55.55.2:5000              UP
UP     ac   Et1/0.1:200(Eth VLAN)       UP mpls 10.55.55.2:5200              UP
UP pri ac   Se6/0:225(FR DLCI)           UP mpls 10.55.55.2:5225              UP
IA sec ac   Se6/0:225(FR DLCI)           UP mpls 10.55.55.3:5226              DN
IA pri ac   Et1/0.2:100(Eth VLAN)        UP ac   Et2/0.2:100(Eth VLAN)        UP
UP sec ac   Et1/0.2:100(Eth VLAN)        UP mpls 10.55.55.3:1101              UP
UP     ac   Se6/0:150(FR DLCI)          UP ac   Se8/0:150(FR DLCI)           UP
```

The following example shows the **show xconnect all** command output in the detailed display format:

```
Router# show xconnect all detail

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, SB=Standby, RV=Recovering, NH=No HardwareXC
ST     Segment 1                         S1 Segment 2                            S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Et0/0(Ethernet)              UP mpls 10.55.55.2:1000              UP
            Interworking: ip                    Local VC label 16
                                                Remote VC label 16
                                                pw-class: mpls-ip
UP     ac   Se7/0(PPP)                   UP mpls 10.55.55.2:2175              UP
            Interworking: ip                    Local VC label 22
                                                Remote VC label 17
                                                pw-class: mpls-ip
UP pri ac   Se6/0:230(FR DLCI)           UP mpls 10.55.55.2:2230              UP
```

```
            Interworking: ip                    Local VC label 21
                                                Remote VC label 18
pw-class: mpls-ip
IA sec ac   Se6/0:230(FR DLCI)          UP mpls 10.55.55.3:2231             DN
            Interworking: ip                    Local VC label unassigned
                                                Remote VC label 19
                                                pw-class: mpls-ip
SB ac   Se4/0:100(FR DLCI)           UP mpls 10.55.55.2:4000              SB
            Interworking: none                  Local VC label 18
                                                Remote VC label 19
                                                pw-class: mpls
UP     ac   Se6/0:500(FR DLCI)          UP l2tp 10.55.55.2:5000             UP
            Interworking: none                  Session ID: 34183
                                                Tunnel ID: 62083
                                                Peer name: pe-iou2
                                                Protocol State: UP
                                                Remote Circuit State: UP
                                                pw-class: l2tp
UP     ac   Et1/0.1:200(Eth VLAN)       UP mpls 10.55.55.2:5200             UP
            Interworking: ip                    Local VC label 17
                                                Remote VC label 20
                                                pw-class: mpls-ip
UP pri ac   Se6/0:225(FR DLCI)          UP mpls 10.55.55.2:5225             UP
            Interworking: none                  Local VC label 19
                                                Remote VC label 21
                                                pw-class: mpls
IA sec ac   Se6/0:225(FR DLCI)          UP mpls 10.55.55.3:5226             DN
            Interworking: none                  Local VC label unassigned
                                                Remote VC label 22
                                                pw-class: mpls
IA pri ac   Et1/0.2:100(Eth VLAN)       UP ac   Et2/0.2:100(Eth VLAN)       UP
            Interworking: none                  Interworking: none
UP sec ac   Et1/0.2:100(Eth VLAN)       UP mpls 10.55.55.3:1101             UP
            Interworking: none                  Local VC label 23
                                                Remote VC label 17
                                                pw-class: mpls
UP     ac   Se6/0:150(FR DLCI)          UP ac   Se8/0:150(FR DLCI)          UP
            Interworking: none                  Interworking: none
```

Examples

The following is sample output from the **show xconnect all** command in the brief (default) display format for all xconnect attachment circuits and pseudowires on a Cisco uBR10012 router:

```
Router# show xconnect all

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down           AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering     NH=No Hardware
XC ST  Segment 1                        S1 Segment 2                       S2
------+--------------------------------+--+--------------------------------+--
UP     ac   Bu254:2001(DOCSIS)          UP mpls 10.76.1.1:2001              UP
UP     ac   Bu254:2002(DOCSIS)          UP mpls 10.76.1.1:2002              UP
UP     ac   Bu254:2004(DOCSIS)          UP mpls 10.76.1.1:2004              UP
DN     ac   Bu254:22(DOCSIS)            UP mpls 101.1.0.2:22                DN
```

Examples

The following is sample output from the **show xconnect** command in the brief (default) display format for all xconnect attachment circuits and pseudowires on a Cisco uBR10012 router in Cisco IOS Release 12.2(33)SCF:

```
Router# show xconnect all

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down           AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering     NH=No Hardware
XC ST  Segment 1                        S1 Segment 2                       S2
------+--------------------------------+--+--------------------------------+--
DN     ac   Bu254:55(DOCSIS)            DN mpls 10.2.3.4:55                 DN
```

```
UP     ac   Bu254:1000(DOCSIS)          UP mpls 10.2.3.4:1000               UP
UP     ac   Bu254:400(DOCSIS)           UP mpls 10.76.2.1:400               UP
DN     ac   Bu254:600(DOCSIS)           DN mpls 10.76.2.1:600               DN
UP     ac   Bu254:1800(DOCSIS)          UP mpls 10.76.2.1:1800              UP
DN     ac   Bu254:45454(DOCSIS)         DN mpls 10.76.2.1:45454             DN
```

Examples

The following is sample output from the **show xconnect** command in the detailed display format for all xconnect attachment circuits and pseudowires on a Cisco uBR10012 router:

```
Router# show xconnect all detail

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering      NH=No Hardware
XC ST  Segment 1                         S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Bu254:2001(DOCSIS)           UP mpls 10.76.1.1:2001              UP
            Interworking: ethernet               Local VC label 40
                                                 Remote VC label 110
                                                 pw-class:
UP     ac   Bu254:2002(DOCSIS)           UP mpls 10.76.1.1:2002              UP
            Interworking: ethernet               Local VC label 41
                                                 Remote VC label 88
                                                 pw-class:
UP     ac   Bu254:2004(DOCSIS)           UP mpls 10.76.1.1:2004              UP
            Interworking: ethernet               Local VC label 42
                                                 Remote VC label 111
                                                 pw-class:
DN     ac   Bu254:22(DOCSIS)             UP mpls 101.1.0.2:22                DN
            Interworking: ethernet               Local VC label 39
                                                 Remote VC label unassigned
                                                 pw-class:
```

Examples

The following is sample output from the **show xconnect** command in the detailed display format for all xconnect attachment circuits and pseudowires on a Cisco uBR10012 router in Cisco IOS Release 12.2(33)SCF:

```
Router# show xconnect all detail

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering      NH=No Hardware
XC ST  Segment 1                         S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
DN     ac   Bu254:55(DOCSIS)             DN mpls 10.2.3.4:55                 DN
            Interworking: ethernet               Local VC label unassigned
                                                 Remote VC label unassigned
                                                 pw-class:
UP     ac   Bu254:1000(DOCSIS)           UP mpls 10.2.3.4:1000               UP
            Interworking: ethernet               Local VC label 33
                                                 Remote VC label 36
                                                 pw-class:
UP     ac   Bu254:400(DOCSIS)            UP mpls 10.76.2.1:400               UP
            Interworking: ethernet               Local VC label 35
                                                 Remote VC label 194
                                                 pw-class:
DN     ac   Bu254:600(DOCSIS)            DN mpls 10.76.2.1:600               DN
            Interworking: ethernet               Local VC label unassigned
                                                 Remote VC label 120
                                                 pw-class:
UP     ac   Bu254:1800(DOCSIS)           UP mpls 10.76.2.1:1800              UP
            Interworking: ethernet               Local VC label 24
                                                 Remote VC label 132
                                                 pw-class:
DN     ac   Bu254:45454(DOCSIS)          DN mpls 10.76.2.1:45454             DN
            Interworking: ethernet               Local VC label unassigned
```

```
                                                    Remote VC label 54
                                                    pw-class:
```

The table below describes the significant fields shown in the displays.

Table 72: show xconnect all Field Descriptions

Field	Description
XC ST	State of the xconnect attachment circuit or pseudowire. The valid states are: • DN—The xconnect attachment circuit or pseudowire is down. Either segment 1, segment 2, or both segments are down. • IA—The xconnect attachment circuit or pseudowire is inactive. This state is valid only when pseudowire redundancy is configured. • NH—One or both segments of this xconnect no longer have the required hardware resources available to the system. • UP—The xconnect attachment circuit or pseudowire is up. Both segment 1 and segment 2 must be up for the xconnect to be up.
Segment1 or Segment2	Information about the type of xconnect, the interface type, and the IP address the segment is using. The types of xconnects are as follows: • ac—Attachment circuit • l2tp—Layer 2 Tunnel Protocol • mpls—Multiprotocol Label Switching • pri ac—Primary attachment circuit • sec ac—Secondary attachment circuit
S1 or S2	State of the segment. The valid states are: • AD—The segment is administratively down. • DN—The segment is down. • HS—The segment is in hot standby mode. • RV—The segment is recovering from a graceful restart. • SB—The segment is in a standby state. • UP—The segment is up.

The additional fields displayed in the detailed output are self-explanatory.

Examples

For the VPLS Autodiscovery feature, issuing the **show xconnect rib** command provides RIB details, as shown in the following example:

```
Router# show xconnect rib

Local Router ID: 10.0.0.0
+- Origin of entry                              (I=iBGP/e=eBGP)
| +- Imported without a matching route target  (Yes/No)?
| | +- Provisioned                              (Yes/No)?
| | | +- Stale entry                            (Yes/No)?
| | | |
v v v v
O I P S        VPLS-ID         Target ID       Next-Hop       Route-Target
-+-+-+-+----------------------+---------------+--------------+-------------
I Y N N        66:66           10.0.0.1       10.1.1.2        66:66
I Y N N        66:66           10.1.1.2         10.1.1.3        66:66
I N Y N        1:1             10.1.1.1         10.1.1.1        2:2
I N Y N        1:1             10.1.1.1         10.1.1.3        2:2
I N Y N
```

The table below describes the significant fields shown in the display.

Table 73: show xconnect rib Field Descriptions

Field	Description
Local Router ID	A unique router identifier. Virtual Private LAN Service (VPLS) Autodiscovery automatically generates a router ID using the MPLS global router ID.
Origin of entry	Origin of the entry. The origin can be “I” for internal Border Gateway Protocol (BGP) or “e” for external BGP.
Imported without a matching route target	Specifies whether the route was imported prior to configuring a route target.
Provisioned	Specifies whether the pseudowire has been provisioned using a learned route.
VPLS/WPWS-ID	Virtual Private LAN Service (VPLS) domain. VPLS Autodiscovery automatically generates a VPLS ID using the BGP autonomous system number and the configured VFI VPN ID.
Target ID	Target ID. The IP address of the destination router.
Next-Hop	IP address of the next hop router.
Route-Target	Route target (RT). VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the route distinguisher (RD) and VPN ID.

For VPLS Autodiscovery, issuing the **show xconnect rib detail** command provides more information about the routing information base, as shown in the following example:

```
Router# show xconnect rib detail

Local Router ID: 10.9.9.9
VPLS-ID 10:123, TID 10.7.7.7
  Next-Hop: 10.7.7.7
  Hello-Source: 10.9.9.9
  Route-Target: 10:123
  Incoming RD: 10:10
  Forwarder: vfi VPLS1
  Origin: BGP
  Provisioned: Yes
VPLS-ID 10:123, TID 10.7.7.8
  Next-Hop: 10.7.7.8
  Hello-Source: 10.9.9.9
  Route-Target: 10:123
  Incoming RD: 10:11
  Forwarder: vfi VPLS1
  Origin: BGP
  Provisioned: No
VPLS-ID 10.100.100.100:1234, TID 0.0.0.2
  Next-Hop: 10.2.2.2, 10.3.3.3, 10.4.4.4
  Hello-Source: 10.9.9.9
  Route-Target: 10.111.111.111:12345, 10.8.8.8:345
  Incoming RD: 10:12
  Forwarder: vfi VPLS2
  Origin: BGP
  Provisioned: Yes
VPLS-ID 10.100.100.100:1234, TID 10.13.1.1
  Next-Hop: 10.1.1.1
  Hello-Source: 10.9.9.9
  Route-Target: 10.111.111.111:12345
  Incoming RD: 10:13
  Forwarder: vfi VPLS2
  Origin: BGP
  Provisioned: Yes
```

The table below describes the significant fields shown in the display.

Table 74: show xconnect rib detail Field Descriptions

Field	Description
Hello-Source	Source IP address used when Label Distribution Protocol (LDP) hello messages are sent to the LDP peer for the autodiscovered pseudowire.
Incoming RD	Route distinguisher for the autodiscovered pseudowire.
Forwarder	VFI to which the autodiscovered pseudowire is attached.

Examples

The following is sample output from the **show xconnect rib** command when used in a Layer 2 Virtual Private Network (L2VPN) VPLS Inter-AS Option B configuration:

```
Router# show xconnect rib

Local Router ID: 10.9.9.9
+- Origin of entry  (I=iBGP/e=eBGP)
| +- Provisioned    (Yes/No)?
| | +- Stale entry  (Yes/No)?
| | |
v v v
O P S        VPLS-ID         Target ID       Next-Hop        Route-Target
-+-+-+------+---------------+---------------+---------------+-------------
I Y N        1:1             10.11.11.11     10.11.11.11     1:1
I Y N        1:1             10.12.12.12     10.12.12.12     1:1
```

The table below describes the significant fields shown in the display.

Table 75: show xconnect rib Field Descriptions

Field	Description
Local Router ID	A unique router identifier. Virtual Private LAN Service (VPLS) Autodiscovery automatically generates a router ID using the MPLS global router ID.
Origin of entry	Origin of the entry. The origin can be “I” for internal BGP or “e” for external BGP.
Provisioned	Specifies whether the pseudowire has been provisioned using a learned route; Yes or No.
Stale entry	Specifies whether it is a stale entry; Yes or No.
VPLS-ID	VPLS domain. VPLS Autodiscovery automatically generates a VPLS ID using the BGP autonomous system number and the configured VFI VPN ID.
Target ID	IP address of the destination router.
Next-Hop	IP address of the next hop router.
Route-Target	VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the route distinguisher (RD) and VPN ID.

The following is sample output from the **show xconnect rib detail** command when used in an ASBR configuration. On an ASBR, the **show xconnect rib detail** command displays the Layer 2 VPN BGP network

layer reachability information (NLRI) received from the BGP peers. The display also shows the signaling messages received from the targeted LDP sessions for a given target attachment individual identifier (TAII).

```
Router# show xconnect rib detail

Local Router ID: 10.1.1.3
VPLS-ID: 1:1, Target ID: 10.1.1.1
  Next-Hop: 10.1.1.1
  Hello-Source: 10.1.1.3
  Route-Target: 2:2
  Incoming RD: 10.0.0.0:1
  Forwarder:
  Origin: BGP
  Provisioned: Yes
  SAII: 10.0.0.1, LDP Peer Id: 10.255.255.255, VC Id: 1001 ***
  SAII: 10.1.0.1, LDP Peer Id: 10.255.255.255, VC Id: 1002 ***
```

After the passive TPE router receives the BGP information (and before the passive TPE router receives the LDP label), the peer information will be displayed in the output of the **show xconnect rib** command. The peer information will not be displayed in the **show mpls l2transport vc** command because the VFI AToM xconnect has not yet been provisioned.

Therefore, for passive TPEs, the entry “Passive : Yes” is added to the output from the **show xconnect rib detail** command. In addition, the entry “Provisioned: Yes” is displayed after the neighbor xconnect is successfully created (without any retry attempts).

In the sample output, the two lines beginning with “SAII” show that this ASBR is stitching two provider PE routers (10.0.0.1 and 10.1.0.1) to the TAII 10.1.1.1.

The table below describes the significant fields shown in the display.

Table 76: show xconnect rib detail (for the ASBR) Field Descriptions

Field	Description
VPLS-ID	VPLS identifier.
Target ID	IP address of the destination router.
Next-Hop	IP address of the next hop router.
Hello-Source	The source IP address used when LDP hello messages are sent to the LDP peer for the autodiscovered pseudowire.
Route-Target	VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the route distinguisher (RD) and VPN ID.
Incoming RD	Specifies the route distinguisher for the autodiscovered pseudowire.
Forwarder	The VFI to which the autodiscovered pseudowire is attached.
Origin	Origin of the entry.

Field	Description
Provisioned	Indicates whether the neighbor xconnect was successfully created (without any retry attempts).
SAII	Specifies the source attachment individual identifier.

The following is sample output from the **show xconnect rib checkpoint** command. Autodiscovered pseudowire information is checkpointed to the standby Route Processor (RP). The **show xconnect rib checkpoint** command displays that pseudowire information.

```
Router# show xconnect rib checkpoint

Xconnect RIB Active RP:
Checkpointing   : Allowed
Checkpointing epoch: 1
ISSU Client id: 2102, Session id: 108, Compatible with peer
Add entries send ok     :         14
Add entries send fail   :          0
Delete entries send ok  :          2
Delete entries send fail:          0
+- Checkpointed to standby                    (Yes/No)?
| +- Origin of entry                         (I=iBGP/e=eBGP)
| | +- Imported without a matching route target (Yes/No)?
| | |
v v v
C O I       VPLS-ID         Target ID       Next-Hop       Route-Target
-+-+-+---------------------+---------------+--------------+----------------
N I Y 66:66                 10.1.1.1         10.1.1.3        66:66
N I Y 66:66                 10.1.1.2         10.1.1.3        66:66
Y I N 1:1                   10.1.1.1         10.1.1.1        2:2
Y I N 1:1                   10.1.1.1         10.1.1.3        2:2
Y I N 1:1                   10.1.1.2         10.1.1.3        2:2
```

The table below describes the significant fields shown in the display.

Table 77: show xconnect rib checkpoint Field Descriptions

Field	Description
Checkpointing	Indicates whether checkpointing is allowed.
Checkpointing epoch	Indicates the checkpointing epoch number.
Checkpointed to standby	Indicates whether the autodiscovered pseudowire information is checkpointed to the standby RP.
Origin of entry	Origin of the entry. The origin can be “I” for internal BGP or “e” for external BGP.
Imported without a matching route target	Specifies whether the route was imported prior to configuring a route target.
VPLS-ID	The VPLS identifier.
Target ID	IP address of the destination router.

Field	Description
Next-Hop	IP address of the next hop router.

The following is sample output from the **show xconnect monitor** command.

```
Router# show xconnect monitor

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0% Time source is hardware calendar,
 *21:00:39.098 GMT Fri May 6 2011

Peer IP          Local IP                         State VC Refs
---------------- -------------------------------- ----- -------
10.1.1.2          10.1.1.1                         Up    1
10.1.1.3          10.1.1.1                         Up    1
```

Table 78: show xconnect monitor Field Descriptions

Field	Description
Peer IP	IP address of the peer. The peer IP address and the Local IP address are the loopback addresses to which a multihop session is associated.
Local IP	Local IP address. The peer IP address and the Local IP address are the loopback addresses to which a multihop session is associated.
State	State of the session.
VC Refs	Number of virtual circuits (VCs) that are tied to the multihop session represented by the peer IP address and the local IP address.

Note The following is the expected output for the **show xconnect monitor** command in different scenarios:

- When you remove a Bidirectional Forwarding Detection (BFD) map that associates timers and authentication with multihop templates using the **no bfd map** command, the session state is Down.
- When you unbind a single hop BFD template from an interface using the **no bfd template** command, the session state is Down.
- When you shut down the AC circuit, the session state is Up.
- When you disable pseudowire fast-failure detection using the **no monitor peer bfd** command, the VC entry associated with the pseudowire class in the **show xconnect monitor** command output is removed. If multiple VCs are present for a session, the VC Refs field of the command output shows the decrement in the number of VCs. The session state is Down for that VC.

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.
show atm vc	Displays all ATM PVCs and SVCs and traffic information.
show atm vp	Displays the statistics for all VPs on an interface or for a specific VP.
show connect	Displays configuration information about drop-and-insert connections that have been configured on a router.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show l2tun session	Displays the current state of Layer 2 sessions and protocol information about L2TP control channels.
show mpls l2transport binding	Displays VC label binding information.
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

show xtagatm cos-bandwidth-allocation

Note Effective with Cisco IOS Release 12.4(20)T, the **show xtagatm cos-bandwidth-allocation** command is not available in Cisco IOS software.

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** command in user EXEC or privileged EXEC mode.

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

Syntax Description

xtagatm	(Optional) Specifies the XTagATM interface number.
interface-number	Number of the XTagATM interface. Range: 0 to 2147483647.

Command Default

Available 50 percent, control 50 percent.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(20)T	This command was removed.

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%
```

The table below describes the significant fields shown in the display.

Table 79: show xtagatm cos-bandwidth-allocation Field Descriptions

Field	Description
CoS	Class of service for transmitted packets.
Bandwidth Allocation	Percentage bandwidth allocated to each QoS traffic category.

show xtagatm cross-connect

Note Effective with Cisco IOS Release 12.4(20)T, the **show xtagatm cross-connect** command is not available in Cisco IOS software.

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

traffic	(Optional) Displays receive and transmit cell counts for each connection.
interface *interface*	(Optional) Displays only connections with an endpoint of the specified interface.
vpi vci	(Optional) Displays only detailed information on the endpoint with the specified virtual path identifier (VPI)/virtual channel identifier (VCI) on the specified interface.
descriptor *descriptor*	(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.
12.4(20)T	This command was removed.

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
```

```
10.1.0       1/37        ->     10.3.0       1/35        UP
10.1.0       1/34        ->     10.3.0       1/33        UP
10.1.0       1/33        <->    10.2.0       0/32        UP
10.1.0       1/32        <->    10.3.0       0/32        UP
10.1.0       1/35        <-     10.3.0       1/34        UP
10.2.0       1/57        ->     10.3.0       1/49        UP
10.2.0       1/53        ->     10.3.0       1/47        UP
10.2.0       1/48        <-     10.1.0       1/50        UP
10.2.0       0/32        <->    10.1.0       1/33        UP
10.3.0       1/34        ->     10.1.0       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        <-     10.1.0       1/38        UP
10.3.0       1/35        <-     10.1.0       1/37        UP
10.3.0       1/33        <-     10.1.0       1/34        UP
10.3.0       0/32        <->    10.1.0       1/32        UP
```

The table below describes the significant fields shown in the display.

Table 80: 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.

Field	Description
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: • DOWN • ABOUT_TO_DOWN • ABOUT_TO_CONNECT • CONNECTING • ABOUT_TO_RECONNECT • RECONNECTING • ABOUT_TO_RESYNC • RESYNCING • NEED_RESYNC_RETRY • ABOUT_TO_RESYNC_RETRY RETRYING_RESYNC • ABOUT_TO_DISCONNECT • DISCONNECTING

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
```

The table below describes the significant fields shown in the display.

Table 81: 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.

Field	Description
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: • DOWN ABOUT_TO_DOWN ABOUT_TO_CONNECT • CONNECTING • ABOUT_TO_RECONNECT • RECONNECTING • ABOUT_TO_RESYNC • RESYNCING • NEED_RESYNC_RETRY • ABOUT_TO_RESYNC_RETRY • RETRYING_RESYNC • ABOUT_TO_DISCONNECT • DISCONNECTING

Field	Description
Conn-type	Input--Indicates an ingress endpoint where traffic is only expected to be received into the switch. Output--Indicates an egress endpoint, where traffic is only expected to be sent from the interface. Input/output--Indicates that traffic is expected to be both send and received at this endpoint.
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

Note Effective with Cisco IOS Release 12.4(20)T, the **show xtagatm vc** command is not available in Cisco IOS software.

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

vcd	(Optional) Virtual circuit descriptor (virtual circuit number). If you specify the >*vcd* argument , information displays about all VCs with that >*virtual circuit descriptor (VCD)* . If you do not specify the >*vcd* argument , a summary description of all VCs on all XTagATM interfaces displays.
interface	(Optional) Interface number. If you specify the >*interface* and the >*vcd* 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.
12.4(20)T	This command was removed.

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
```

The table below describes the significant fields shown in the display.

Table 82: 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
show atm vc	Displays information about private ATM VCs.
show xtagatm cross-connect	Displays information about remotely connected ATM switches.

shutdown (mpls)

To bring down an active service, interface, or configuration, use the **shutdown** command in the appropriate configuration mode. To bring up the service, interface, or configuration, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The service, interface, or configuration is active.

Command Modes

Interface configuration (config-if)

L2 VFI configuration (config-vfi)

Xconnect configuration (config-xconnect)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support.
15.3(1)S	This command was integrated as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support.

Usage Guidelines

Use the **shutdown** command in interface configuration mode to bring down an active pseudowire interface.

Use the **shutdown** command in L2 VFI configuration mode to bring down all existing pseudowires in the virtual forwarding interface (VFI). If the VFI is shut down, information about active services is not advertised. However, information about already autodiscovered peers is not lost.

Use the **shutdown** command in xconnect configuration mode to bring down any L2VPN services that are defined by the L2VPN cross connect.

Examples

The following example shows how to bring down an active pseudowire interface:

```
Device(config)# interface pseudowire 100
Device(config-if)# shutdown
```

The following example shows how to bring down all existing pseudowires in the VFI:

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# shutdown
```

The following example shows how to bring down L2VPN services in xconnect configuration mode:

```
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# shutdown
```

signaling protocol

To specify the signaling protocol to be used for signaling labels, use the **signaling protocol** command in interface configuration mode. To remove the signaling protocol, use the **no** form of this command.

signaling protocol {**ldp**| **none**}

no signaling protocol

Syntax Description

ldp	Specifies that the Label Distribution Protocol (LDP) signaling protocol will be used.
none	Specifies that no signaling protocol will be used for signaling labels (labels are configured statistically).

Command Default

The default protocol is Multiprotocol Label Switching (MPLS).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command will replace **ldp** and **none** keywords in the **protocol** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Examples

The following example shows how to specify a signaling protocol:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# neighbor 10.0.0.1 100
Device(config-if)# signaling protocol none
Device(config-if)# label 1000 2000
```

Related Commands

Command	Description
protocol	Specifies the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session and to cause control plane configuration settings to be taken from a specified L2TP class.
source template type pseudowire	Specifies the name of a pseudowire class and enters pseudowire class configuration mode.

snmp mib mpls vpn

To configure Simple Network Management Protocol (SNMP) controls for Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) notification thresholds, use the **snmp mib mpls vpn** command in global configuration mode. To disable SNMP controls for MPLS VPN thresholds, use the **no** form of this command.

snmp mib mpls vpn {**illegal-label** *number*| **max-threshold** *seconds*}

no snmp mib mpls vpn {**illegal-label| max-threshold**}

Syntax Description

illegal-label	Controls MPLS VPN illegal label threshold exceeded notifications.
number	Number of illegal labels allowed before SNMP sends an illegal label threshold notification. The valid range is 1 to 4,294,967,295. The default is 0.
max-threshold	Controls MPLS VPN maximum threshold exceeded notifications.
seconds	Time in seconds before SNMP resends maximum threshold notifications. The range is 0 to 4,294,967,295. The default is 0.

Command Default

SNMP controls are not configured for MPLS VPN routing and forwarding (VRF) tables.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to configure the number of illegal labels allowed for routes in the MPLS VRF before SNMP sends an illegal label threshold notification, or to configure the time elapsed before SNMP resends a maximum threshold notification.

Use the **snmp mib mpls vpn illegal-label** command to indicate how many illegal MPLS VPN labels you want to allow before you receive a notification. Once this number is exceeded, SNMP sends an illegal-label notification to a network management system (NMS), if you have one configured; otherwise, the router issues

a syslog error message. If you do not configure this command, SNMP sends an illegal label notification on the first occurrence of an illegal label.

Use the **snmp mib mpls vpn max-threshold** command if you want to receive maximum threshold notifications periodically when attempts are made to add routes to the VRF after the maximum threshold is exceeded. If you do not configure this command, SNMP sends a single maximum threshold notification at the time that the maximum threshold is exceeded. Notifications are sent to an NMS if you configured one; otherwise, the router issues a syslog error message. Another notification is not sent until the number of routes goes below the maximum threshold and then exceeds the threshold again.

Examples

The following example shows how to configure an illegal label threshold of 50 labels:

```
configure terminal
!
snmp mib mpls vpn illegal-label 50
```

The following example shows how to configure the time interval of 600 seconds for resending maximum threshold notifications:

```
configure terminal
!
smnp mib mpls vpn max-threshold 600
```

Related Commands

Command	Description
ip vrf	Specifies a name for a VRF routing table and enters VRF configuration mode (for IPv4 VRF only).
maximum routes	Limits the maximum number of routes in a VRF to prevent a PE router from importing too many routes.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

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*| *extended-access-list-number*| *access-list-name*]

no snmp-server community *string*

Syntax Description

string	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. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
view	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community.
view-name	(Optional) Name of a previously defined view.
ro	(Optional) Specifies read-only access. Authorized management stations can retrieve only MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.
ipv6	(Optional) Specifies an IPv6 named access list.
nacl	(Optional) IPv6 named access list.
access-list-number	(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.

Command Modes Global configuration (config)

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.
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 **ipv6** *nacl* keyword and argument pair was added to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
12.3(14)T	The **ipv6** *nacl* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T to support assignment of IPv6 named access lists. This keyword and 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.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Aggregation Series Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SRE	This command was modified. The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, is changed. The **snmp-server community** command has to be manually configured.

Release	Modification
15.1(0)M	This command was modified. The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, is changed. The **snmp-server community** command has to be manually configured.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

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).

Note In Cisco IOS Release 12.0(3) to 12.2(33)SRD, if a community string was not defined using the **snmp-server community** command prior to using the **snmp-server host** command, the default form of the **snmp-server community** command was automatically inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** was same as specified in the **snmp-server host** command. However, in Cisco IOS Release 12.2(33)SRE and later releases, you have to manually configure the **snmp-server community** command.

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

Note The @ symbol 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. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

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 to SNMP and allow read-write access 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 list1 and links an SNMP community string with this access list:

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# exit
Router(config)# snmp-server community comaccess rw ipv6 list1
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
show snmp community	Displays SNMP community access strings.
snmp-server enable traps	Enables the router to send SNMP notification messages to a designated network management workstation.
snmp-server host	Specifies the targeted recipient of an SNMP notification operation.
snmp-server view	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*]

Syntax Description

notification-type	

(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 *notification-type* (family name) in the **snmp-server enable traps**command:

- **bgp** --Sends Border Gateway Protocol (BGP) state change notifications.
- **config** --Sends configuration notifications.
- **entity** --Sends entity MIB modification notifications.
- envmon--Sends Cisco enterprise-specific environmental monitor notifications whenever certain environmental thresholds are exceeded. *Notification-option* arguments (below) can be specified in combination with thiskeyword.
- **frame-relay** --Sends Frame Relay notifications.
- **hsrp** --Sends Hot Standby Routing Protocol (HSRP) notifications.
- isdn--Sends ISDN notifications. *Notification-option* arguments (see examples below) can be specified in combination with thiskeyword.
- repeater--Sends Ethernet repeater (hub) notifications. *Notification-option* arguments (see examples below) can be specified in combination with thiskeyword.
- **rsvp** --Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr** --Sends Service Assurance Agent/Response Time Reporter (RTR) notifications.
- **snmp** [**authentication**]--Sends RFC 1157 SNMP notifications. Using the **authentication** keyword produces the same effect as not using it. Both the **snmp-server enable traps snmp** and the **snmp-server enable traps snmp authentication**forms of this command globally enable the following SNMP notifications (or, if you are using the **no** form of the command, disables such notifications): **authenticationFailure**, **linkUp**, **linkDown**, and **warmstart**.

	• **syslog** --Sends system error message (syslog) notifications. You can specify the level of messages to be sent using the **logging history level** command.
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 thiskeyword. • **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 thiskeyword.

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.

Command Default

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 **snmp-server enable traps snmp authentication** form of this command was introduced to replace the **snmp-server trap-authentication** command.
12.0(17)ST	The **mpls traffic-eng**keyword was added to define a class or family of specific SNMP notifications for use with the *notification-type*and *notification-option*parameters of the **snmp-server enable traps**command.
12.0(21)ST	The **mpls ldp** keyword was added to define a class or family of specific SNMP notifications for use with the *notification-type*and *notification-option*parameters of the **snmp-server enable traps**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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

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, usingthe 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 host1 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
snmp-server host	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) Simple Network Management Protocol (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 [pv-limit] [session-down] [session-up] [threshold]

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

Syntax Description

pv-limit	(Optional) Enables or disables path-vector (PV) limit notifications (mplsLdpPathVectorLimitMismatch).
session-down	(Optional) Enables or disables LDP session down notifications (mplsLdpSessionDown).
session-up	(Optional) Enables or disables LDP session up notifications (mplsLdpSessionUp).
threshold	(Optional) Enables or disables PV Limit notifications (mplsLdpFailedInitSessionThresholdExceeded).

Command Default

The sending of SNMP notifications is disabled. If you do not specify an optional keyword, all four types of LDP notifications are enabled on the label switching router (LSR).

Command Modes

Global configuration (config)

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.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

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 limits.

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 0 up to 255 indicates that loop detection is on and 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 an 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 software and cannot be changed using either the command line interface (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.

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 or other vendor LSRs in an MPLS network. Among these incompatibilities, for example, are the following:

- Nonoverlapping ATM VPI/VCI ranges (as noted) or nonoverlapping Frame Relay data-link connection identifier (DLCI) ranges between LSRs attempting to set up an LDP session
- Unsupported label distribution method
- Dissimilar protocol data unit (PDU) sizes
- 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.

If the **pv-limit** keyword is used, a message is generated when the router establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path-vector limits.

If the **session-down** keyword is used, a session-down message is generated when an LDP session between the router and its adjacent LDP peer is terminated.

If the **session-up** keyword is used, a message is generated when the router establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).

If the **threshold** keyword is used, a message is generated after eight failed attempts to establish an LDP session between the router and an LDP peer. The failures can be caused by any type of incompatibility between the devices.

All four keywords can be used in the same command in any combination.

Note An mplsLdpEntityFailedInitSessionThreshold trap is supported only on an LC-ATM.

Examples

In the following example, LDP-specific informs are enabled and will be sent to the host myhost.cisco.com through use of 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
snmp-server host	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 p2mp-traffic-eng

To enable the sending of Multiprotocol Label Switching (MPLS) Point to Multi-point (P2MP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps mpls p2mp-traffic-eng** 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 p2mp-traffic-eng [**down**| **up**]

no snmp-server enable traps mpls p2mp-traffic-eng [**down**| **up**]

Syntax Description

down	(Optional) Enables or disables MPLS TE tunnel down trap notifications (mplsTeP2mpTunnelDestDown). This message is generated when a MPLS Point to Multi-Point MPLS-TE tunnel between the device and its destination is terminated.
up	(Optional) Enables or disables MPLS TE tunnel up trap notifications (mplsTeP2mpTunnelDestUp). This notification is generated when the device establishes a MPLS Point to Multi-Point MPLS-TE tunnel between the device and its destination is established.

Command Default

The sending of SNMP notifications is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

If you do not specify an optional keyword, all MPLS TE notifications are enabled.

The **snmp-server enable traps mpls p2mp-traffic-eng** 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, the SNMP server host is configured for MPLS P2MP-specific trap notifications. And these notifications are enabled and are be sent to the host myhost.cisco.com through use of community string defined as public:

```
Device(config)# snmp-server host myhost.cisco.com public udp-port 162 p2mp-traffic-eng
Device(config)# snmp-server enable traps mpls p2mp-traffic-eng
```

Related Commands

Command	Description
snmp-server host	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 rfc ldp

To enable the sending of Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Simple Network Management Protocol (SNMP) notifications defined in RFC 3815, use the **snmp-server enable traps mpls rfc 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 rfc ldp [**pv-limit**| **session-down**| **session-up**| **threshold**]

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

Syntax Description

pv-limit	(Optional) Enables or disables MPLS RFC LDP path-vector (PV) limit mismatch notifications (mplsLdpPathVectorLimitMismatch).
session-down	(Optional) Enables or disables MPLS RFC LDP session down notifications (mplsLdpSessionDown).
session-up	(Optional) Enables or disables MPLS RFC LDP session up notifications (mplsLdpSessionUp).
threshold	(Optional) Enables or disables MPLS RFC LDP threshold exceeded notifications (mplsLdpInitSessionThresholdExceeded).

Command Default

The sending of SNMP notifications is disabled by default. If you do not specify an optional keyword, all four types of MPLS RFC LDP notifications are enabled on the label switch router (LSR).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to enable the LDP notifications supported in *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP),* RFC 3815.

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 limits. We recommend that all LDP-enabled routers in the network be configured with the same path vector limits.

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 0 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 an 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 eight. This default value is implemented in Cisco IOS software and cannot be changed using either the command-line interface (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 Virtual Path Identifier (VPI) and Virtual Channel Identifier (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.

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 or between Cisco routers and other vendor LSRs in an MPLS network. Among these incompatibilities, for example, are the following:

- Nonoverlapping ATM VPI and VCI ranges (as noted) or nonoverlapping Frame Relay Data Link Connection Identifier (DLCI) ranges between LSRs attempting to configure an LDP session
- Unsupported label distribution method
- Dissimilar protocol data unit (PDU) sizes
- Dissimilar LDP feature support

The **snmp-server enable traps mpls rfc 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.

If the **pv-limit** keyword is used, a message is generated when the router establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path vector limits.

If the **session-down** keyword is used, a session-down message is generated when an LDP session between the router and its adjacent LDP peer is terminated.

If the **session-up** keyword is used, a message is generated when the router establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).

If the **threshold** keyword is used, a message is generated after eight failed attempts to establish an LDP session between the router and an LDP peer. The failures can be caused by any type of incompatibility between the devices.

Examples

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

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

Related Commands

Command	Description
snmp-server host	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 rfc vpn

To enable the sending of Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Simple Network Management Protocol (SNMP) notifications defined in RFC 4382, use the **snmp-server enable traps mpls rfc vpn** command in global configuration mode. To disable the sending of MPLS VPN notifications, use the **no** form of this command

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

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

Syntax Description

illegal-label	(Optional) Enables or disables an MPLS RFC VPN notification for any illegal labels received on a VPN routing and forwarding (VRF) instance interface.
max-thresh-cleared	(Optional) Enables or disables an MPLS RFC VPN notification when the number of routes attempts to exceed the maximum limit and then drops below the maximum number of routes.
max-threshold	(Optional) Enables or disables an MPLS RFC VPN notification when a route creation attempt was unsuccessful because the maximum route limit was reached.
mid-threshold	(Optional) Enables or disables an MPLS RFC VPN warning when the number of routes created has exceeded the warning threshold.
vrf-down	(Optional) Enables or disables an MPLS RFC VPN notification when the last interface associated with a VRF transitions to the down state.
vrf-up	(Optional) Enables or disables an MPLS RFC VPN notification when the first interface associated with a VRF transitions to the up state when previously all interfaces were in the down state.

Command Default

The sending of SNMP notifications is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

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

The **illegal-label** keyword enables a notification for 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.

When the **max-thresh-cleared** keyword is used and you attempt to create a route on a VRF that already contains the maximum number of routes, the mplsL3VpnVrfNumVrfRouteMaxThreshExceeded notification is sent (if enabled).

When you remove routes from the VRF so that the number of routes falls below the set limit, the mplsL3VpnNumVrfRouteMaxThreshCleared notification is sent. You can clear all routes from the VRF by using the **clear ip route vrf** command.

The **max-threshold** keyword 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 **maximum routes** command in VRF configuration mode. If both IPv4 and IPv6 address-family configurations are present in the VRF, the threshold is an aggregate of the maximum threshold values. An mplsL3VpnVrfNumVrfRouteMaxThreshExceeded notification is not sent until the second address family reaches its maximum route threshold. Routes are not added to the address family that has already reached its maximum route threshold.

Note If you configure a single address-family VRF with a maximum and middle threshold, and later add the other address-family configuration to your VRF without configuring a maximum threshold, you no longer receive a maximum threshold notification for the original address family when the threshold is reach, but routes would no longer be added to the routing table for this address family.

The warning that the **mid-threshold** keyword enables is sent only at the time the warning threshold is exceeded. If both IPv4 and IPv6 address-family configurations are present in the VRF, the threshold is an aggregate of the middle or warning threshold values. An mplsL3VpnVrfRouteMidThreshExceeded notification is not sent until the second address family reaches its warning threshold.

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

The **maximum routes** command gives you two options in the VRF address family configuration mode:

- 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 rfc 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* **warning-only**--generates a warning message when the *warn-threshold*is reached. The specified limit is enforced.

If you use the **maximum routes** *limit* **warning-only** command with the **snmp-server enable traps mpls rfc 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.

Note When both IPv4 and IPv6 address-family configurations exist, the MPLS-L3-VPN-STD-MIB displays the aggregate value of the maximum route settings (not to exceed the max int32 value). If the maximum route limit is configured for one address family and not for the other address family, the aggregate value is max int32 (4,294,967,295).

The notification types described are defined in the following MIB objects of the MPLS-L3-VPN-STD-MIB:

- mplsL3VpnVrfUp
- mplsL3VpnVrfDown
- mplsL3VpnVrfRouteMidThreshExceeded
- mplsL3VpnVrfNumVrfRouteMaxThreshExceeded
- mplsL3VpnNumVrfSecIllglLblThrshExcd
- mplsL3VpnNumVrfRouteMaxThreshCleared

Examples

In the following example, MPLS RFC 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 rfc vpn vrf-down vrf-up
```

Related Commands

Command	Description
clear ip route vrf	Removes routes from the VRF routing table.
maximum routes	Limits the maximum number of routes in a VRF to prevent a PE router from importing too many routes.
snmp-server host	Specifies the recipient of SNMP 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

up	(Optional) Enables only mplsTunnelUp notifications { mplsTeNotifyPrefix 1 }.
down	(Optional) Enables only mplsTunnelDown notifications { mplsTeNotifyPrefix 2}.
reroute	(Optional) Enables or disables only mplsTunnelRerouted notifications {mplsTeNotifyPrefix 3}.

Command Default

SNMP notifications are disabled.

When 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 enables or disables MPLS traffic engineering tunnel notifications. MPLS tunnel state-change 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 keyword in conjunction with this command, all three types of MPLS traffic engineering tunnel notifications are sent.

When the **up** keyword is used, 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.

When the **down** keyword is used, 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.

When the **reroute** keyword is used, mplsTunnelRerouted notifications are sent to the NMS under the following conditions:

- The signaling path of an existing MPLS traffic engineering tunnel fails and a new path option is signaled and placed into effect (that is, the tunnel is rerouted).
- 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 timer
  - The issuance of an **mpls traffic-eng reoptimize** command
  - A configuration change that requires the resignaling of a tunnel

The mplsTunnelReoptimized notification is not generated when an MPLS traffic engineering tunnel is reoptimized. However, an mplsTunnelReroute notification is generated. Thus, at the NMS, you cannot distinguish between a tunnel reoptimization and a tunnel reroute event.

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

Examples

The following example shows how to enable 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
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps mpls vpn

To enable the device 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

illegal-label	(Optional) Enables a notification for any illegal labels received on a VPN routing/forwarding instance (VRF) interface.
max-thresh-cleared	(Optional) Enables a notification when the number of routes attempts to exceed the maximum limit and then drops below the maximum number of routes.
max-threshold	(Optional) Enables a notification that a route creation attempt was unsuccessful because the maximum route limit was reached.
mid-threshold	(Optional) Enables a warning that the number of routes created has exceeded the warning threshold.
vrf-down	(Optional) Enables a notification for the removal of a VRF from an interface or the transition of an interface to the down state.
vrf-up	(Optional) Enables a notification for the assignment of a VRF to an interface that is operational or for the transition of a VRF interface to the operationally up state.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.

Release	Modification
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 max-thresh-cleared keyword.
12.2(28)SB2	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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

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

The **illegal-label** keyword enables a notification for 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.

When the **max-thresh-cleared** keyword is used and you attempt to create a route on a VRF that already contains the maximum number of routes, the mplsNumVrfRouteMaxThreshExceeded notification is sent (if enabled).

When you remove routes from the VRF so that the number of routes falls below the set limit, the cMplsNumVrfRouteMaxThreshCleared notification is sent. You can clear all routes from the VRF by using the **clear ip route vrf** command.

The **max-threshold** keyword 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 **maximum routes** command in VRF configuration mode.

The warning that the **mid-threshold** keyword enables is sent only at the time the warning threshold is exceeded.

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

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* **warning-only—**generates a warning message when the *warn-threshold* is reached. The specified limit is 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 *warn-threshold* value is reached. A max-threshold notification is generated when the *limit* value is reached.

The notification types described 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:

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

Related Commands

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

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* {**v1**| **v2c**| **v3** {**auth**| **noauth**| **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-number*| *acl-name*]]

no snmp-server group *group-name* {**v1**| **v2c**| **v3** {**auth**| **noauth**| **priv**}} [**context** *context-name*]

Syntax Description

group-name	Name of the group.
v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.
v2c	Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.
v3	Specifies that the group is using the SNMPv3 security model. SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
context-name	(Optional) Context name.
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.

read-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
write-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.
notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.
notify-view	(Optional) String of a maximum of 64 characters that is the name of the view. By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user). Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.
access	(Optional) Specifies a standard access control list (ACL) to associate with the group.
ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.
named-access-list	(Optional) Name of the IPv6 access list.
acl-number	(Optional) The *acl-number*argument is an integer from 1 to 99 that identifies a previously configured standard access list.

acl-name	(Optional) The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.

Command Default

No SNMP server groups are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.(3)T	This command was introduced.
12.0(23)S	The **context** *context-name* keyword and argument pair was added.
12.3(2)T	The **context** *context-name* keyword and argument pair was integrated into Cisco IOS Release 12.3(2)T, and support for standard named access lists (acl-name) was added.
12.0(27)S	The **ipv6** *named-access-list* keyword and argument pair was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	The **ipv6** *named-access-list* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Usage Guidelines

When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a Message Digest 5 (MD5) password, see the documentation of the **snmp-server user** command.

Configuring Notify Views

The notify-view option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.
- The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, you must either reconfigure the **snmp-server host** command, or specify the appropriate notify view.

Specifying a notify view when configuring an SNMP group is not recommended, for the following reasons:

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.
- Modifying the group's notify view will affect all users associated with that group.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in the order specified:

1. **snmp-server user** --Configures an SNMP user.
2. **snmp-server group** --Configures an SNMP group, without adding a notify view .
3. **snmp-server host** --Autogenerates the notify view by specifying the recipient of a trap operation.

SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

Use this command with the **context** *context-name* keyword and argument to associate a read, write, or notify SNMP view with an SNMP context.

Examples

Examples

The following example shows how to create the SNMP server group "public," allowing read-only access for all objects to members of the standard named access list "lmnop":

```
Router(config)# snmp-server group public v2c access lmnop
```

Examples

The following example shows how to remove the SNMP server group "public" from the configuration:

```
Router(config)# no snmp-server group public v2c
```

Examples

The following example shows SNMP context "A" associated with the views in SNMPv2c group "GROUP1":

```
Router(config)# snmp-server context A
Router(config)# snmp mib community commA
Router(config)# snmp mib community-map commA context A target-list commAVpn
Router(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

Related Commands

Command	Description
show snmp group	Displays the names of groups on the router and the security model, the status of the different views, and the storage type of each group.
snmp mib community-map	Associates a SNMP community with an SNMP context, engine ID, security name, or VPN target list.
snmp-server host	Specifies the recipient of a SNMP notification operation.
snmp-server user	Configures a new user to a SNMP group.

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*| **informs**| **traps**| **version** {**1**| **2c**| **3** [**auth**| **noauth**| **priv**]}] *community-string* [**udp-port** *port* [*notification-type*]| *notification-type*]

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

Command Syntax on Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches

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

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

Command Syntax on Cisco 7600 Series Router

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

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

Syntax Description

hostname	Name of the host. 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.
ip-address	IPv4 address or IPv6 address of the SNMP notification host.
vrf	(Optional) Specifies that a VPN routing and forwarding (VRF) instance should be used to send SNMP notifications. • In Cisco IOS Release 12.2(54)SE, the **vrf** keyword is required.

vrf-name	(Optional) VPN VRF instance used to send SNMP notifications. • In Cisco IOS Release 12.2(54)SE, the *vrf-name* argument is required.
informs	(Optional) Specifies that notifications should be sent as informs. • In Cisco IOS Release 12.2(54)SE, the **informs** keyword is required.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default. • In Cisco IOS Release 12.2(54)SE, the **traps** keyword is required.
version	(Optional) Specifies the version of the SNMP that is used to send the traps or informs. The default is 1. • In Cisco IOS Release 12.2(54)SE, the **version** keyword is required and the **priv** keyword is not supported. If you use the **version** keyword, one of the following keywords must be specified: • **1** --SNMPv1. • **2c** --SNMPv2C. • **3** --SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is **noauth**. One of the following three optional security level keywords can follow the **3** keyword: • • **auth** --Enables message digest algorithm 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. • **noauth** --Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. • **priv** --Enables Data Encryption Standard (DES) packet encryption (also called "privacy").

community-string	Password-like community string sent with the notification operation. **Note** You can set this string using the **snmp-server host** command by itself, but Cisco recommends that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command. **Note** The "at" sign (@) is used for delimiting the context information.
udp-port	(Optional) Specifies that SNMP traps or informs are to be sent to an network management system (NMS) host. • In Cisco IOS Release 12.2(54)SE, the **udp-port** keyword is not supported.
port	(Optional) User Datagram Protocol (UDP) port number of the NMS host. The default is 162. • In Cisco IOS Release 12.2(54)SE, the *port* argument is not supported.
notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. See the "Usage Guidelines" section for more information about the keywords available.

Command Default

This command behavior is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	This command was modified. • The **version 3** [**auth** | **noauth** | **priv**] syntax was added as part of the SNMPv3 Support feature. • The **hsrp** notification-type keyword was added. • The **voice** notification-type keyword was added.

Release	Modification
12.1(3)T	This command was modified. The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	This command was modified. • The **vrf** *vrf-name* keyword-argument pair was added. • The **ipmobile** notification-type keyword was added. • Support for the **vsimaster** notification-type keyword was added for the Cisco 7200 and Cisco 7500 series routers.
12.2(4)T	This command was modified. • The **pim** notification-type keyword was added. • The **ipsec** notification-type keyword was added.
12.2(8)T	This command was modified. • The **mpls-traffic-eng** notification-type keyword was added. • The **director** notification-type keyword was added.
12.2(13)T	This command was modified. • The **srp** notification-type keyword was added. • The **mpls-ldp** notification-type keyword was added.
12.3(2)T	This command was modified. • The **flash** notification-type keyword was added. • The **l2tun-session** notification-type keyword was added.
12.3(4)T	This command was modified. • The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added. • The **ospf notification-type** keyword was added.
12.3(8)T	This command was modified. The **iplocalpool notification-type** keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	This command was modified. The **vrrp** keyword was added.

Release	Modification
12.3(14)T	This command was modified. • 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 *hostname* argument. • The **eigrp** notification-type keyword was added.
12.4(20)T	This command was modified. The **license** notification-type keyword was added.
15.0(1)M	This command was modified. • The **nhrp** notification-type keyword was added. • The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, was changed. The **snmp-server community** command must be manually configured.
12.0(17)ST	This command was modified. The **mpls-traffic-eng** notification-type keyword was added.
12.0(21)ST	This command was modified. The **mpls-ldp notification-type** keyword was added.
12.0(22)S	This command was modified. • All features in Cisco IOS Release 12.0ST were integrated into Cisco IOS Release 12.0(22)S. • The **mpls-vpn** notification-type keyword was added.
12.0(23)S	This command was modified. The **l2tun-session** notification-type keyword was added.
12.0(26)S	This command was modified. The **memory** notification-type keyword was added.
12.0(27)S	This command was modified. • Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **vrf** *vrf-name* keyword and argument combination was added to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	This command was modified. The **l2tun-pseudowire-status** notification-type keyword was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.

Release	Modification
12.2(25)S	This command was modified. • The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added.
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.
12.2(31)SB2	The **cef** notification-type keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI5	This command was modified. • The **dhcp-snooping** notification-type keyword was added. • The **errdisable** notification-type keyword was added.
12.2(54)SE	This command was modified. See the snmp-server host, on page 250 for the command syntax for these switches.
12.2(33)SXJ	This command was integrated into Cisco IOS Release 12.2(33)SXJ. The **public storm-control** notification-type keyword was added.
15.0(1)S	This command was modified. The **flowmon notification-type** keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(1)S	This command was modified. The **p2mp-traffic-eng** notification-type keyword was added.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Usage Guidelines

If you enter this command with no optional keywords, the default is to send all notification-type traps 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 a 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** command will be the same as that 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. However, in Cisco IOS Release 12.2(33)SRE and later releases, you must manually configure the **snmp-server community** command. That is, the **snmp-server community** command will not be seen in the configuration.

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, an SNMP entity that receives an inform request acknowledges the message with an 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 than traps.

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 tried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **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 optional 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. 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.

The availability of notification-type options depends on the router type and the 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 VPN. The VRF defines a VPN membership of a user so that data is stored using the VPN.

In the case of the NMS sending the query having a correct SNMP community but not having a read or a write view, the SNMP agent returns the following error values:

- For a get or a getnext query, returns GEN_ERROR for SNMPv1 and AUTHORIZATION_ERROR for SNMPv2C.
- For a set query, returns NO_ACCESS_ERROR.

Notification-Type Keywords

The notification type can be one or more of the following keywords.

Note The available notification types differ based on the platform and Cisco IOS release. For a complete list of available notification types, use the question mark (?) online help function.

- **aaa server** --Sends SNMP authentication, authorization, and accounting (AAA) traps.
- **adslline** --Sends Asymmetric Digital Subscriber Line (ADSL) LINE-MIB traps.
- **atm** --Sends ATM notifications.
- **authenticate-fail** --Sends an SNMP 802.11 Authentication Fail trap.
- **auth-framework** --Sends SNMP CISCO-AUTH-FRAMEWORK-MIB notifications.
- **bgp** --Sends Border Gateway Protocol (BGP) state change notifications.
- **bridge** --Sends SNMP STP Bridge MIB notifications.
- **bstun** --Sends Block Serial Tunneling (BSTUN) event notifications.
- **bulkstat** --Sends Data-Collection-MIB notifications.
- **c6kxbar** --Sends SNMP crossbar notifications.
- **callhome** --Sends Call Home MIB notifications.
- **calltracker** -- Sends Call Tracker call-start/call-end notifications.
- **casa** --Sends Cisco Appliances Services Architecture (CASA) event notifications.
- **ccme** --Sends SNMP Cisco netManager Event (CCME) traps.
- **cef** --Sends notifications related to Cisco Express Forwarding.
- **chassis** --Sends SNMP chassis notifications.
- **cnpd** --Sends Cisco Network-based Application Recognition (NBAR) Protocol Discovery (CNPD) traps.
- **config** --Sends configuration change notifications.
- **config-copy** --Sends SNMP config-copy notifications.
- **config-ctid** --Sends SNMP config-ctid notifications.
- **cpu** --Sends CPU-related notifications.
- **csg** --Sends SNMP Content Services Gateway (CSG) notifications.
- **deauthenticate** --Sends an SNMP 802.11 Deauthentication trap.
- **dhcp-snooping** --Sends DHCP snooping MIB notifications.

- **director** --Sends notifications related to DistributedDirector.
- **disassociate** --Sends an SNMP 802.11 Disassociation trap.
- **dlsw** --Sends data-link switching (DLSW) notifications.
- **dnis** --Sends SNMP Dialed Number Identification Service (DNIS) traps.
- **dot1x** --Sends 802.1X notifications.
- **dot11-mibs** --Sends dot11 traps.
- **dot11-qos** --Sends SNMP 802.11 QoS Change trap.
- **ds1** --Sends SNMP digital signaling 1 (DS1) notifications.
- **ds1-loopback** --Sends ds1-loopback traps.
- **dspu** --Sends downstream physical unit (DSPU) notifications.
- **eigrp** --Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications.
- **energywise** --Sends SNMP energywise notifications.
- **entity** --Sends Entity MIB modification notifications.
- **entity-diag** --Sends SNMP entity diagnostic MIB notifications.
- **envmon** --Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
- **errdisable** --Sends error disable notifications.
- **ethernet-cfm** --Sends SNMP Ethernet Connectivity Fault Management (CFM) notifications.
- **event-manager** --Sends SNMP Embedded Event Manager notifications.
- **firewall** --Sends SNMP Firewall traps.
- **flash** --Sends flash media insertion and removal notifications.
- **flexlinks** --Sends FLEX links notifications.
- **flowmon** --Sends flow monitoring notifications.
- **frame-relay** --Sends Frame Relay notifications.
- **fru-ctrl** --Sends entity field-replaceable unit (FRU) control notifications.
- **hsrp** --Sends Hot Standby Routing Protocol (HSRP) notifications.
- **icsudsu** --Sends SNMP ICSUDSU traps.
- **iplocalpool** --Sends IP local pool notifications.
- **ipmobile** --Sends Mobile IP notifications.
- **ipmulticast** --Sends IP multicast notifications.
- **ipsec** --Sends IP Security (IPsec) notifications.
- **isakmp** --Sends SNMP ISAKMP notifications.
- **isdn** --Sends ISDN notifications.

- **l2tc** --Sends SNMP L2 tunnel configuration notifications.
- **l2tun-pseudowire-status** --Sends pseudowire state change notifications.
- **l2tun-session** --Sends Layer 2 tunneling session notifications.
- **license** --Sends licensing notifications as traps or informs.
- **llc2** --Sends Logical Link Control, type 2 (LLC2) notifications.
- **mac-notification** --Sends SNMP MAC notifications.
- **memory** --Sends memory pool and memory buffer pool notifications.
- **module** --Sends SNMP module notifications.
- **module-auto-shutdown** --Sends SNMP module autoshutdown MIB notifications.
- **mpls-fast-reroute** --Sends SNMP Multiprotocol Label Switching (MPLS) traffic engineering fast reroute notifications.
- **mpls-ldp** --Sends 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.
- **msdp** --Sends SNMP Multicast Source Discovery Protocol (MSDP) notifications.
- **mvpn** --Sends multicast VPN notifications.
- **nhrp** --Sends Next Hop Resolution Protocol (NHRP) notifications.
- **ospf** --Sends Open Shortest Path First (OSPF) sham-link notifications.
- **pim** --Sends Protocol Independent Multicast (PIM) notifications.
- **port-security** --Sends SNMP port-security notifications.
- **power-ethernet** --Sends SNMP power Ethernet notifications.
- **public storm-control** --Sends SNMP public storm-control notifications.
- **pw-vc** --Sends SNMP pseudowire virtual circuit (VC) notifications.
- **p2mp-traffic-eng**--Sends SNMP MPLS Point to Multi-Point MPLS-TE notifications.
- **repeater** --Sends standard repeater (hub) notifications.
- **resource-policy** --Sends CISCO-ERM-MIB notifications.
- **rf** --Sends SNMP RF MIB notifications.
- **rogue-ap** --Sends an SNMP 802.11 Rogue AP trap.
- **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.
- **slb** --Sends SNMP server load balancer (SLB) 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.

- **sonet** --Sends SNMP SONET notifications.
- **srp** --Sends Spatial Reuse Protocol (SRP) notifications.
- **stpx** --Sends SNMP STPX MIB notifications.
- **srst** --Sends SNMP Survivable Remote Site Telephony (SRST) traps.
- **stun** --Sends serial tunnel (STUN) notifications.
- **switch-over** --Sends an SNMP 802.11 Standby Switchover trap.
- **syslog** --Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **syslog** --Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **tty** --Sends Cisco enterprise-specific notifications when a TCP connection closes.
- **udp-port** --Sends the notification host's UDP port number.
- **vlan-mac-limit** --Sends SNMP L2 control VLAN MAC limit notifications.
- **vlancreate** --Sends SNMP VLAN created notifications.
- **vlandelete** --Sends SNMP VLAN deleted notifications.
- **voice** --Sends SNMP voice traps.
- **vrrp** --Sends Virtual Router Redundancy Protocol (VRRP) notifications.
- **vsimaster** --Sends Virtual Switch Interface (VSI) Master notifications.
- **vswitch** --Sends SNMP virtual switch notifications.
- **vtp** --Sends SNMP VLAN Trunking Protocol (VTP) notifications.
- **wlan-wep** --Sends an SNMP 802.11 Wireless LAN (WLAN) Wired Equivalent Privacy (WEP) trap.
- **x25** --Sends X.25 event notifications.
- **xgcp** --Sends External Media Gateway Control Protocol (XGCP) traps.

SNMP-Related Notification-Type Keywords

The *notification-type* argument 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-type* argument applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no embedded spaces). The corresponding parameter in the

snmp-server enable traps command is specified as **mpls traffic-eng** (containing an embedded space and a hyphen).

This syntax difference is necessary to ensure that the 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. The table below maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 83: snmp-server enable traps Commands and Corresponding Notification Keywords

snmp-server enable traps Command	snmp-server host Command Keyword
snmp-server enable traps l2tun session	**l2tun-session**
snmp-server enable traps mpls ldp	**mpls-ldp**
snmp-server enable traps mpls traffic-eng [1]	**mpls-traffic-eng**
snmp-server enable traps mpls vpn	**mpls-vpn**
snmp-server host *host-address community-string* **udp-port** *port* **p2mp-traffic-eng**	**snmp-server enable traps mpls p2mp-traffic-eng** [**down** | **up**]

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 10.0.0.0 comaccess
Router(config)# access-list 10 deny any
```

Note The "at" 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 specified host 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 10.0.0.0 using the community string public:

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

```
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 10.0.0.0 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 example.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host example.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
```

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 10.0.1.1 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 10.0.1.1 informs version 2c public cef
```

The following example shows how to enable all NHRP traps, and how to send all NHRP traps to the notification receiver with the IP address 10.0.0.0 using the community string public:

```
Router(config)# snmp-server enable traps nhrp
Router(config)# snmp-server host 10.0.0.0 traps version 2c public nhrp
```

The following example shows how to enable all P2MP MPLS-TE SNMP traps, and send them to the notification receiver with the IP address 172.20.2.160 using the community string "comp2mppublic":

```
Router(config)# snmp-server enable traps mpls p2mp-traffic-eng
Router(config)# snmp-server host 172.20.2.160 comp2mppublic udp-port 162 p2mp-traffic-eng
```

Related Commands

Command	Description
show snmp host	Displays recipient details configured for SNMP notifications.

Command	Description
snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server enable traps nhrp	Enables SNMP notifications (traps) for NHRP.
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP traps that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
test snmp trap storm-control event-rev1	Tests SNMP storm-control traps.

source template type pseudowire

To configure the name of a source template of type pseudowire, use the **source template type pseudowire** command in interface configuration mode. To remove a source template of type pseudowire, use the **no** form of this command.

source template type pseudowire *template-name*

no source template type pseudowire

Syntax Description

template-name	The name of source template of type pseudowire.

Command Default

A source template of type pseudowire is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command will replace the **pw-class** keyword in the **xconnect** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

The **source template type pseudowire** command applies a source template of type pseudowire that consists of configuration settings used by all pseudowires bound to the template.

Examples

The following example shows how to configure the source template of type pseudowire named ether-pw:

```
Device(config)# interface pseudowire 100
Device(config-if)# source template type pseudowire ether-pw
```

Related Commands

Command	Description
xconnect	Binds an attachment circuit to a pseudowire and configures an AToM static pseudowire.

spanning-tree mode

To switch between Per-VLAN Spanning Tree+ (PVST+), Rapid-PVST+, and Multiple Spanning Tree (MST) modes, use the **spanning-treemode** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mode [**pvst**| **mst**| **rapid-pvst**]

no spanning-tree mode

Syntax Description

pvst	(Optional) PVST+ mode.
mst	(Optional) MST mode.
rapid-pvst	(Optional) Rapid-PVST+ mode.

Command Default

pvst

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelin

Caution Be careful when using the **spanning-treemode** command to switch between PVST+, Rapid-PVST+, and MST modes. When you enter the command, all spanning-tree instances are stopped for the previous mode and are restarted in the new mode. Using this command may cause disruption of user traffic.

Examples

This example shows how to switch to MST mode:

```
Device(config)# spanning-tree mode mst
Device(config)#
```

This example shows how to return to the default mode (PVST+):

```
Device(config)# no spanning-tree mode
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst configuration

To enter MST-configuration submode, use the **spanning-treemstconfiguration** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax Description

This command has no arguments or keywords.

Command Default

The default value for the Multiple Spanning Tree (MST) configuration is the default value for all its parameters:

- No VLANs are mapped to any MST instance (all VLANs are mapped to the Common and Internal Spanning Tree [CIST] instance).
- The region name is an empty string.
- The revision number is 0.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

The MST configuration consists of three main parameters:

- Instance VLAN mapping--See the **instance** command
- Region name--See the **name(MSTconfigurationsubmode)** command
- Configuration revision number--See the **revision** command

The **abort** and **exit** commands allow you to exit MST configuration submode. The difference between the two commands depends on whether you want to save your changes or not.

The **exit** command commits all the changes before leaving MST configuration submode. If you do not map secondary VLANs to the same instance as the associated primary VLAN, when you exit MST-configuration

submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

The **abort** command leaves MST-configuration submode without committing any changes.

Changing an MST-configuration submode parameter can cause connectivity loss. To reduce service disruptions, when you enter MST-configuration submode, make changes to a copy of the current MST configuration. When you are done editing the configuration, you can apply all the changes at once by using the exit keyword, or you can exit the submode without committing any change to the configuration by using the abort keyword.

In the unlikely event that two users commit a new configuration at exactly at the same time, this warning message displays:

```
% MST CFG:Configuration change lost because of concurrent access
```

Examples

This example shows how to enter MST-configuration submode:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)#
```

This example shows how to reset the MST configuration to the default settings:

```
Device(config)# no spanning-tree mst configuration
Device(config)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST)	Sets the name of an MST region.
revision	Sets the revision number for the MST configuration.
show	Verifies the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.

status (pseudowire class)

To configure a device to send pseudowire status messages to a peer device, even when the attachment circuit is down, use the **status** command in the appropriate configuration mode. To remove the sending of pseudowire status messages, use the **no** form of this command.

status

no status

Syntax Description

This command has no arguments or keywords.

Command Default

The command is configured by default.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
Cisco IOS XE Release 3.7S	This command was modified as part of the MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in interface configuration and template configuration modes.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Both peer routers must support the ability to send and receive pseudowire status messages in label advertisement and label notification messages. If both peer devices do not support pseudowire status messages, we recommend that you disable the messages with the **no status** command.

Examples

The following example shows how to disable status messages to a peer device in pseudowirw class configuration mode:

```
Device(config)# pseudowire-class test1
Device(config-pw-class)# encapsulation mpls
Device(Config-pw-class)# no status
```

The following example shows how to disable status messages to a peer device in interface configuration mode:

```
Device(config)# interface pseudowire 1
Device(config-if)# encapsulation mpls
Device(Config-if)# status
```

The following example shows how to disable status messages to a peer device in template configuration mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# no status
```

Related Commands

Command	Description
debug l2vpn atom vc	Displays L2VPN AToM VCs.
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
show l2vpn atom vc	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 VPN packets on a device.
show mpls l2transport vc	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a device.

status control-plane route-watch

To enable listening for routing events to trigger redundancy status changes, use the **status control-plane route-watch** command in the appropriate configuration mode. To disable listening for routing events, use the **no** form of this command.

status control-plane route-watch

no status control-plane route-watch

Syntax Description

This command has no arguments or keywords.

Command Default

Listening for routing events is enabled.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was integrated into a release prior to Cisco IOS XE Release 3.7S. This command was modified as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command was made available in interface configuration and template configuration modes in Cisco IOS XE Release 3.7S.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Examples

The following example shows how to disable listening on the control plane for route watch events in pseudowire class configuration mode:

```
Device(config)# pseudowire-class mpls-dhd
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# no status control-plane route-watch
```

The following example shows how to disable listening on the control plane for route watch events in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# no status control-plane route-watch
```

The following example shows how to configure listening on the control plane for route watch events in template configuration mode:

```
Device(config)# template type pseudowire 1
Device(config-template)# encapsulation mpls
Device(config-template)# status control-plane route-watch
```

Related Commands

Command	Description
status (pseudowire class)	Enables a device to send pseudowire status messages to a peer device, even when the attachment circuit is down.

status protocol notification static

To enable the timers in the specified class name, use the **status protocol notification static** command in the appropriate configuration mode. To disable timers of the specified class, use the **no** form of this command.

status protocol notification static *class-name*

no status protocol notification static *class-name*

Syntax Description

class-name	Name of an Operation, Administration, and Maintenance (OAM) class that was created using the **pseudowire static-oam-class** or the **l2vpn pseudowire static-oam class** command.

Command Default

OAM classes are not specified.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated into Cisco IOS Release 15.1(3)S.
Cisco IOS XE Release 3.7S	This command was integrated into a release prior to Cisco IOS XE Release 3.7S. This command was made available in interface configuration and template configuration modes in Cisco IOS XE Release 3.7S as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. .
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Examples

The following example shows how to enable the timers in the class oam-class3:

```
Device(config)# pseudowire-class mpls-dhd
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# status protocol notification static oam-class3
```

The following example shows how to enable the timers in the class oam-class3 in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# status protocol notification static oam-class3
```

The following example shows how to enable the timers in the class oam-class3 in template configuration mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# status protocol notification static oam-class3
```

Related Commands

Command	Description
l2vpn pseudowire static-oam class	Creates an L2VPN OAM class and specifies the timeout intervals
pseudowire-static-oam class	Creates a class that defines the OAM parameters for the pseudowire.

status redundancy

To designate one pseudowire as the master to display status information for both active and backup pseudowires, use the **status redundancy** command in the appropriate configuration mode. To designate the pseudowire as slave, use the **no** form of this command.

status redundancy master

no status redundancy master

Syntax Description

master	Designates a pseudowire to work as the master.

Command Default

The pseudowire is in slave mode.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Release 2.3	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command was made available in interface configuration and template configuration modes.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

One pseudowire must be the master and the other must be the slave. You cannot configure both pseudowires as master or slave.

Examples

The following example shows how to designate the pseudowire as the master in pseudowire class configuration mode:

```
Device(config)# pseudowire-class mpls-dhd
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# status redundancy master
```

The following example shows how to designate the pseudowire as the master in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# status redundancy master
```

The following example shows how to designate the pseudowire as the master in template configuration mode:

```
Device(config)# template type pseudowire pw1
Device(config-template)# encapsulation mpls
Device(config-template)# status redundancy master
```

Related Commands

Command	Description
show l2vpn rib	Displays information about the L2VPN cross connect RIB.
show l2vpn service	Displays L2VPN service information.
show l2vpn vfi	Displays L2VPN VFI information.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

switching-point

To configure a switching point and specify a virtual circuit (VC) ID range, use the **switching-point** command in Layer 2 pseudowire routing configuration mode. To remove the switching point configuration, use the **no** form of this command.

switching-point vcid *minimum-vcid-value maximum-vcid-value*

switching-point vcid

Syntax Description

vcid	Configures a VC ID range for the switching point.
minimum-vcid-value	Minimum value or starting point for the VC ID range. Valid entries are 1 to 2147483647.
maximum-vcid-value	Maximum value or ending point for the VC ID range. Valid entries are 1 to 2147483647.

Command Default

If an Autonomous System Boundary Router (ASBR) has been configured as a switching point (accomplished by using the **no bgp default route-target filter** command), the default VC ID range is 1001 to 2147483647.

Command Modes

Layer 2 pseudowire routing (config-l2_pw_rtg)

Command History

Release	Modification
15.1(1)S	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

The **switching-point** command is used in Layer 2 pseudowire routing configuration mode. To enter Layer 2 pseudowire routing configuration mode, use the **l2 pseudowire routing** command.

Changing the VC ID Range on an ASBR

The **switching-point** command was introduced in the L2VPN VPLS Inter-AS Option B feature and is intended for use on an Autonomous System Boundary Router (ASBR). With the L2VPN VPLS Inter-AS Option B feature, VC IDs in the VC ID range of 1001 to 2147483647 are reserved for switching pseudowires. This command allows you to change this range if, for example, an existing xconnect VC is using one of the reserved VC IDs.

Examples

In the following example, the **switching-point** command has been used to specify a VCID range of 200 to 3500:

```
Router>
Router# enable
Router(config)# configure terminal
Router(config)# l2 pseudowire routing
Router(config-l2_pw_rtg)# switching-point vcid 200 3500
Router(config-l2_pw_rtg)# end
```

Related Commands

Command	Description
l2 pseudowire routing	Enables Layer 2 pseudowire routing and enters Layer 2 pseudowire routing configuration mode.
no bgp default route-target filter	Disables automatic BGP route-target community filtering or enables pseudowire switching in address family configuration mode.
show xconnect	Displays information about xconnect attachment circuits and pseudowires

switching tlv

To display the switching point type length value (TLV) in the label binding, use the **switching tlv** command in the appropriate configuration mode. To disable the display of the TLV, use the **no** form of this command.

switching tlv

no switching tlv

Syntax Description

This command has no arguments or keywords.

Command Default

Switching point TLV data is displayed to peers.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Release 2.3	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in interface configuration and template configuration modes.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

The pseudowire switching point TLV includes the following information:

- Pseudowire ID of the last pseudowire segment traversed.
- Pseudowire switching point description.
- Local IP address of the pseudowire switching point.
- Remote IP address of the last pseudowire switching point that was crossed or the terminating-Provider Edge (T-PE) device.

By default, switching point TLV data is advertised to peers.

Examples

The following example shows how to enable the display of the pseudowire switching TLV:

```
Device(config)# pseudowire-class atom
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# switching tlv
```

The following example shows how to enable the display of the pseudowire switching TLV in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# switching tlv
```

The following example shows how to enable the display of the pseudowire switching TLV in template configuration mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# switching tlv
```

Related Commands

Command	Description
show l2vpn atom binding	Displays L2VPN AToM label binding information.
show l2vpn atom vc	Displays information about L2VPN AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a router.
show mpls l2transport binding	Displays VC label binding information.
show mpls l2transport vc detail	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a router.