

show interface xtagatm

To display information about an extended Multiprotocol Label Switching (MPLS) ATM interface, use the **show interface xtagatm** command in user EXEC or privileged EXEC mode.

show interface xtagatm *if-number*

Syntax Description	<i>if-number</i>	Specifies the MPLS ATM interface number.
---------------------------	------------------	--

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

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.3T	Sample command output was added for when an interface is down.

Usage Guidelines	Extended MPLS ATM interfaces are virtual interfaces that are created on first reference like tunnel interfaces. Extended MPLS ATM interfaces are similar to ATM interfaces except that the former only supports LC-ATM encapsulation.
-------------------------	---

Examples The following is sample command output when an interface is down:

Router# **show interface xt92**

```
XTagATM92 is down, line protocol is down
Hardware is Tag-Controlled Switch Port
Interface is unnumbered. Using address of Loopback1 (15.15.15.15)
MTU 4470 bytes, BW 4240 Kbit, DLY 80 used,
reliability 186/255, txload 1/255, rxload 1/255
Encapsulation ATM, loopback not set
Keepalive set (10 sec) [00:00:08/4]
Encapsulation(s): AAL5
Control interface: not configured
0 terminating VCs
Switch port traffic:
  ? cells input, ? cells output
Last input 00:00:10, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
Terminating traffic:
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
138 packets input, 9193 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 i
00:05:46: %SYS-5-CONFIG_I: Configured from console by consolegnored, 0 abort
142 packets output, 19686 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

The following is sample command output when an interface is up:

Router# show interface xt92

```
XTagATM92 is up, line protocol is up
Hardware is Tag-Controlled Switch Port
Interface is unnumbered. Using address of Loopback1 (15.15.15.15)
MTU 4470 bytes, BW 4240 Kbit, DLY 80 used,
reliability 174/255, txload 1/255, rxload 1/255
Encapsulation ATM, loopback not set
Keepalive set (10 sec)
Encapsulation(s): AAL5
Control interface: ATM3/0, switch port: bpx 9.2
3 terminating VCs, 7 switch cross-connects
Switch port traffic:
275 cells input, 273 cells output
Last input 00:00:00, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
Terminating traffic:
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
127 packets input, 8537 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
131 packets output, 18350 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

Table 9 describes the significant fields shown in the displays.

Table 9 show interface xtagatm Field Descriptions

Field	Description
XTagATM0 is up XTagATM0 is down	Interface is currently active (up) or inactive (down).
line protocol is up line protocol is down	Displays the line protocol as up or down.
Hardware is Tag-Controlled Switch Port	Specifies the hardware type.
Interface is unnumbered	Specifies that this is an unnumbered interface.
MTU	Maximum transmission unit of the extended MPLS ATM interface.
BW	Bandwidth of the interface (in kBps).
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over 5 minutes.
Encapsulation ATM	Encapsulation method.
loopback not set	Indicates that loopback is not set.

Table 9 *show interface xtagatm Field Descriptions (continued)*

Field	Description
Keepalive set (10 sec) [00:00:08/4]	Indicates why the Xtag line is down. Valid values are: 1—Internal usage. 2—Administratively down. 3—Internal usage. 4—No extended port is configured. 5—Some cross-connects from an old session have been left operational. 6—No extended port or a wrong extended port was configured. 7—No control port was configured. 8—Internal usage. 9—Internal usage. 10—Internal usage. 11—Internal usage. 12—External port. The XTag is mapped to an invalid port on the switch. 13—External port. The XTag is mapped to a port that is down. 14—External port is mapped to the control panel on the switch. 15—OAM is being used to track the link state. The neighbor may be down or it is not responding to the OAM calls.
Encapsulation(s)	Identifies the ATM adaptation layer.
Control interface	Identifies the control port switch port with which the extended MPLS ATM interface has been associated through the extended-port interface configuration command.
<i>n</i> terminating VCs	Number of terminating VCs with an endpoint on this extended MPLS ATM interface. Packets are sent or received by the MPLS LSC on a terminating VC, or are forwarded between an LSC-controlled switch port and a router interface.
7 switch cross-connects	Number of switch cross-connects on the external switch with an endpoint on the switch port that corresponds to this interface. This includes cross-connects to terminating VCs that carry data to and from the LSC, and cross-connects that bypass the MPLS LSC and switch cells directly to other ports.
Switch port traffic	Number of cells received and sent on all cross-connects associated with this interface.
Terminating traffic	Indicates that counters below this line apply only to packets sent or received on terminating VCs.
5-minute input rate, 5-minute output rate	Average number of bits and packets sent per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.

Table 9 *show interface xtagatm Field Descriptions (continued)*

Field	Description
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet systems and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored and abort counts. Other input-related errors can also increment the count, so that this sum may not balance with other counts.
CRC	<p>Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received.</p> <p>On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus. A high number of CRCs is usually the result of traffic collisions or a station sending bad data.</p> <p>On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.</p>
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface. This usually indicates a clocking problem between the interface and the data-link equipment.
packets output	Total number of messages sent by the system.
bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
underruns	Number of times that the sender has been running faster than the router can handle data. This condition may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.

Table 9 *show interface xtagatm Field Descriptions (continued)*

Field	Description
collisions	Number of messages re-sent due to an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only one time in output packets.
interface resets	Number of times an interface has been completely reset. Resets occur if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.

Related Commands

Command	Description
interface xtagatm	Enters configuration mode for an extended MPLS ATM (XTagATM) interface.

show ip bgp labels

To display information about Multiprotocol Label Switching (MPLS) labels from the External Border Gateway Protocol (EBGP) route table, use the **show ip bgp labels** command in user EXEC or privileged EXEC mode.

show ip bgp labels

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to display EBGP labels associated with a carrier supporting carrier customer edge (CSC-CE) router.

This command displays labels for BGP routes in the default table only. To display labels in the VRF tables, use the **show ip bgp vpnv4 {all | vrf vrf-name}** command with the optional **labels** keyword.

Examples

The following example shows output for a CSC-CE router using BGP as a label distribution protocol:

```
Router# show ip bgp labels

Network          Next Hop          In Label/Out Label
3.3.0.0/16       0.0.0.0           imp-null/exp-null
15.15.15.15/32   15.15.15.15      18/exp-null
16.16.16.16/32   0.0.0.0           imp-null/exp-null
17.17.17.17/32   34.0.0.1         20/exp-null
18.18.18.18/32   43.0.0.1         24/31
18.18.18.18/32   38.0.0.1         24/33
19.19.19.19/32   43.0.0.1         25/32
19.19.19.19/32   38.0.0.1         25/34
20.20.20.20/32   43.0.0.1         21/30
20.20.20.20/32   38.0.0.1         21/32
33.0.0.0         15.15.15.15      19/exp-null
34.0.0.0         0.0.0.0           imp-null/exp-null
35.0.0.0         43.0.0.1         22/29
35.0.0.0         38.0.0.1         22/31
38.0.0.0         0.0.0.0           imp-null/exp-null
38.0.0.1/32      38.0.0.1         17/29
38.0.0.1/32      0.0.0.0           17/exp-null
40.0.0.0         38.0.0.1         26/35
40.0.0.0         43.0.0.1         26/34
42.0.0.0         43.0.0.1         23/28
```

```

42.0.0.0          38.0.0.1          23/30
43.0.0.0          0.0.0.0           imp-null/exp-null
43.0.0.1/32      0.0.0.0           16/exp-null

```

Table 10 describes the significant fields shown in the display.

Table 10 *show ip bgp labels Field Descriptions*

Field	Description
Network	Displays the network address from the EGBP table.
Next Hop	Specifies the EGBP next hop address.
In Label	Displays the label (if any) assigned by this router.
Out Label	Displays the label assigned by the BGP next hop router.

Related Commands

Command	Description
show ip bgp vpnv4	Displays VPN address information from the BGP table.

show ip bgp vpnv4

To display Virtual Private Network (VPN) address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** command in user EXEC or privileged EXEC mode.

```
show ip bgp vpnv4 { all | rd route-distinguisher | vrf vrf-name } [rib-failure] [ip-prefix/length
[longer-prefixes] [output-modifiers]] [network-address [mask] [longer-prefixes]
[output-modifiers]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list]
[flap-statistics] [inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp]
[regexp] [summary] [labels]
```

Syntax Description

all	Displays the complete VPNv4 database.
rd <i>route-distinguisher</i>	Displays Network Layer Reachability Information (NLRI) prefixes that have a matching route distinguisher.
vrf <i>vrf-name</i>	Displays NLRI prefixes associated with the named VPN routing and forwarding instance (VRF).
rib-failure	(Optional) Displays BGP routes that failed to install in the VRF table.
<i>ip-prefix/length</i>	(Optional) The IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
longer-prefixes	(Optional) Displays the entry, if any, that exactly matches the specified prefix parameter and all entries that match the prefix in a “longest-match” sense. That is, prefixes for which the specified prefix is an initial substring.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
<i>network-address</i>	(Optional) The IP address of a network in the BGP routing table.
<i>mask</i>	(Optional) The mask of the network address, in dotted decimal format.
cidr-only	(Optional) Displays only routes that have nonnatural net masks.
community	(Optional) Displays routes matching this community.
community-list	(Optional) Displays routes matching this community list.
dampened-paths	(Optional) Displays paths suppressed on account of dampening (BGP route from peer is up and down).
filter-list	(Optional) Displays routes conforming to the filter list.
flap-statistics	(Optional) Displays flap statistics of routes.
inconsistent-as	(Optional) Displays only routes that have inconsistent autonomous systems of origin.
neighbors	(Optional) Displays details about TCP and BGP neighbor connections.
paths	(Optional) Displays path information.
<i>line</i>	(Optional) A regular expression to match the BGP autonomous system paths.
peer-group	(Optional) Displays information about peer groups.
quote-regexp	(Optional) Displays routes matching the autonomous system path regular expression.

regex	(Optional) Displays routes matching the autonomous system path regular expression.
summary	(Optional) Displays BGP neighbor status.
labels	(Optional) Displays incoming and outgoing BGP labels for each NLRI prefix.

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

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.2(2)T	The output of the show ip bgp vpnv4 all ip-prefix command was enhanced to display attributes including multipaths and a best path to the specified network.
	12.0(21)ST	The tags keyword was replaced with the labels keyword to conform to the MPLS IETF guidelines. This command was integrated into Cisco IOS Release 12.0(21)ST.
	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.
	12.3	The rib-failure keyword was added for VRFs.

Usage Guidelines	Use this command to display VPNv4 information from the BGP database. The show ip bgp vpnv4 all command displays all available VPNv4 information. The show ip bgp vpnv4 summary command displays BGP neighbor status.
-------------------------	--

Examples	The following example shows output for all available VPNv4 information in a BGP routing table:
-----------------	--

```
Router# show ip bgp vpnv4 all

BGP table version is 18, local router ID is 14.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i6.6.6.6/32      223.0.0.21        11      100      0 ?
*> 7.7.7.7/32      150.150.0.2       11              32768 ?
*>i69.69.0.0/30    223.0.0.21        0        100      0 ?
*> 150.150.0.0/24  0.0.0.0           0              32768 ?
*> 222.0.0.1/32    150.150.0.2       11              32768 ?
*>i222.0.0.3/32    223.0.0.21        11      100      0 ?
*> 222.0.0.10/32   0.0.0.0           0              32768 ?
*>i222.0.0.30/32   223.0.0.21        0        100      0 ?
```

[Table 11](#) describes the significant fields shown in the display.

Table 11 show ip bgp vpnv4 Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows how to display a table of labels for NLRI prefixes that have a route distinguisher value of 100:1.

```
Router# show ip bgp vpnv4 rd 100:1 labels

Network          Next Hop          In label/Out label
Route Distinguisher: 100:1 (vrf1)
 2.0.0.0          10.20.0.60       34/nolabel
10.0.0.0          10.20.0.60       35/nolabel
12.0.0.0          10.20.0.60       26/nolabel
                  10.20.0.60       26/nolabel
13.0.0.0          10.15.0.15       nolabel/26
```

Table 12 describes the significant fields shown in the display.

Table 12 show ip bgp vpnv4 rd labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Specifies the BGP next hop address.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next hop router.

The following example shows VPNv4 routing entries for the VRF named vpn1:

```
Router# show ip bgp vpnv4 vrf vpn1

BGP table version is 18, local router ID is 14.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i6.6.6.6/32     223.0.0.21        11     100     0 ?
*> 7.7.7.7/32     150.150.0.2       11     32768 ?
*>i69.69.0.0/30   223.0.0.21        0      100     0 ?
*> 150.150.0.0/24 0.0.0.0           0      32768 ?
*> 222.0.0.1/32   150.150.0.2       11     32768 ?
*>i222.0.0.3/32   223.0.0.21        11     100     0 ?
```

Table 13 describes the significant fields shown in the display.

Table 13 *show ip bgp vpnv4 vrf Field Descriptions*

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows attributes for network 10.22.22.0 that includes multipaths and a best path:

```
Router# show ip bgp vpnv4 all 10.22.22.0

BGP routing table entry for 100:1:10.22.22.0/24, version 50
Paths:(6 available, best #1)
Multipath:iBGP
  Advertised to non peer-group peers:
    200.1.12.12
    22
      1.22.7.8 (metric 11) from 1.11.3.4 (100.0.0.8)
        Origin IGP, metric 0, localpref 100, valid, internal, multipath, best
        Extended Community:RT:100:1
        Originator:100.0.0.8, Cluster list:100.1.1.44
    22
      1.22.1.9 (metric 11) from 1.11.1.2 (100.0.0.9)
        Origin IGP, metric 0, localpref 100, valid, internal, multipath
        Extended Community:RT:100:1
        Originator:100.0.0.9, Cluster list:100.1.1.22
    22
      1.22.6.10 (metric 11) from 1.11.6.7 (100.0.0.10)
        Origin IGP, metric 0, localpref 100, valid, internal, multipath
        Extended Community:RT:100:1
        Originator:100.0.0.10, Cluster list:100.0.0.7
    22
      1.22.4.10 (metric 11) from 1.11.4.5 (100.0.0.10)
        Origin IGP, metric 0, localpref 100, valid, internal, multipath
        Extended Community:RT:100:1
        Originator:100.0.0.10, Cluster list:100.0.0.5
    22
      1.22.5.10 (metric 11) from 1.11.5.6 (100.0.0.10)
        Origin IGP, metric 0, localpref 100, valid, internal, multipath
        Extended Community:RT:100:1
        Originator:100.0.0.10, Cluster list:100.0.0.6
```

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

Table 14 *show ip bgp vpnv4 all 10.22.22.0 Field Descriptions*

Field	Description
BGP routing table ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths:	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.

Table 14 show ip bgp vpnv4 all 10.22.22.0 Field Descriptions (continued)

Field	Description
Multipath:	Indicates the maximum paths configured (iBGP or eBGP).
Advertised to non peer-group peers: 200.1.12.12 22	IP address of the BGP peers that the specified route is advertised to.
1.22.7.8 (metric 11) from 1.11.3.4 (100.0.0.8)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: IGP—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. incomplete—Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the redistribute router configuration command. EGP—Entry originated from an EGP.
metric	If shown, the value of the interautonomous system metric.
localpref	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is <i>internal</i> if the path is learned via iBGP. The field is <i>external</i> if the path is learned via eBGP.
multipath	One of multiple paths to the specified network.
best	If multiple paths exist, one of the multipaths is designated the best path and advertised the neighbors.
Extended Community:RT:100:1	Route Target value associated with the specified route.
Originator:	The router ID of the route originating router when route reflector is used.
Cluster list:	The router ID of all the route reflectors that the specified route has passed through.

The following example shows routes that BGP could not install in the VRF table:

```
Router# show ip bgp vpnv4 vrf foo rib-failure
```

```
Network          Next Hop          RIB-failure    RIB-NH Matches
Route Distinguisher: 2:2 (default for vrf bar)
10.1.1.2/32      100.100.100.100  Higher admin distance    No
111.111.111.112/32 9.9.9.9          Higher admin distance    Yes
```

Table 15 describes the significant fields shown in the display.

Table 15 show ip bgp Field Descriptions

Field	Description
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
RIB-failure	Cause of RIB failure. Higher admin distance means that a route with a better (lower) administrative distance such as a static route already exists in the IP routing table.
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and bgp suppress-inactive is configured for the address family being used. There are three choices: <ul style="list-style-type: none"> • Yes—Means that the route in the RIB has the same nexthop as the BGP route or nexthop recurses down to the same adjacency as the BGP nexthop. • No—Means that the nexthop in the RIB recurses down differently from the nexthop of the BGP route. • n/a—Means that bgp suppress-inactive is not configured for the address family being used.

Related Commands

Command	Description
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip explicit-paths

To display the configured IP explicit paths, use the **show ip explicit-paths** command in user EXEC or privileged EXEC mode.

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

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

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

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

Usage Guidelines An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

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

```
Router# show ip explicit-paths

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

Table 16 describes the significant fields shown in the display.

Table 16 show ip explicit-paths Field Descriptions

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

Related Commands	Command	Description
	append-after	Inserts a path entry after a specific index number. Commands might be renumbered as a result.
	index	Inserts or modifies a path entry at a specific index.

Command	Description
ip explicit-path	Enters the subcommand mode for IP explicit paths so that you can create or modify the named path.
list	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.

show ip ospf database opaque-area

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

show ip ospf database opaque-area

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

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

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

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

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

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

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

MPLS TE router ID: 24.8.8.8

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

Interface Address : 198.1.1.1
```

Table 17 describes the significant fields shown in the display.

Table 17 show ip ospf database opaque-area Field Descriptions

Field	Description
LS age	Link-state age.
Options	Type of service options.

Table 17 *show ip ospf database opaque-area Field Descriptions (continued)*

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

Related Commands

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

show ip ospf mpls ldp interface

To display information about interfaces belonging to an Open Shortest Path First (OSPF) process that are configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP), use the **show ip ospf mpls ldp interface** command in privileged EXEC mode.

show ip ospf [*process-id*] **mpls ldp interface** [*interface*]

Syntax Description		
<i>process-id</i>	(Optional) Process ID. If this argument is included, only information for the specified routing process is included.	
<i>interface</i>	(Optional) Defines the interface about which to display LDP-IGP Synchronization information.	

Defaults If no optional keyword or argument is specified in this command, information is displayed for each interface that has been configured for MPLS LDP-IGP Synchronization.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(30)S	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines This command shows MPLS LDP-IGP Synchronization information for specified interface or OSPF processes.

Examples The following shows sample output generated by the **show ip ospf mpls ldp interface** command:

```
Router# show ip ospf mpls ldp interface

Serial1/2.4
  Process ID 2, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holddown timer is disabled
  Interface is up
Serial1/2.11
  Process ID 6, VRF VFR1, Area 2
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holddown timer is disabled
  Interface is up
Ethernet2/0
  Process ID 1, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Required
  Holddown timer is configured : 1 msec
```

```

    Holddown timer is not running
    Interface is up
Loopback1
  Process ID 1, Area 0
  LDP is not configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holddown timer is disabled
  Interface is up
Serial1/2.1
  Process ID 1, Area 10.0.1.44
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Required
  Holddown timer is configured : 1 msec
  Holddown timer is not running
  Interface is up

```

Table 18 describes the significant fields shown in the display.

Table 18 *show ip ospf mpls ldp interface Field Descriptions*

Field	Description
Process ID	The number of the OSPF process to which the interface belongs.
Area	The OSPF area to which the interface belongs.
LDP is configured through	The means by which LDP was configured on the interface. LDP can be configured on the interface by the mpls ip or mpls ldp command.
LDP-IGP Synchronization	Indicates whether LDP-IGP Synchronization has been enabled on this interface.
Holddown timer	Indicates whether the holddown timer was specified for this interface.

Related Commands

Command	Description
debug mpls ldp igp sync	Displays events related to MPLS LDP-IGP Synchronization.
show mpls ldp igp sync	Displays information about interfaces enabled for MPLS LDP-IGP Synchronization.

show ip ospf mpls traffic-eng

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

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

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

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

Command History	Release	Modification
	Release 12.0S	This command was introduced.

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

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

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

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

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

```

Maximum bandwidth :1250000
Maximum reservable bandwidth :2500000
Number of Priority :8
Priority 0 :2500000      Priority 1 :2500000
Priority 2 :2500000      Priority 3 :2500000
Priority 4 :2500000      Priority 5 :2500000
Priority 6 :2500000      Priority 7 :2500000
Affinity Bit :0x0

```

Table 19 describes the significant fields shown in the display.

Table 19 show ip ospf mpls traffic-eng Field Descriptions

Field	Description
OSPF Router with ID	Router identification number.
Process ID	OSPF process identification.
Area instance	Number of times traffic engineering information or any link changed.
Link instance	Number of times any link changed.
Link ID	Link-state ID.
Interface Address	Local IP address on the link.
Neighbor Address	IP address that is on the remote end of the link.
Admin Metric	Traffic engineering link metric.
Maximum bandwidth	Bandwidth set by the bandwidth interface interface configuration command.
Maximum reservable bandwidth	Bandwidth available for traffic engineering on this link. This value is set in the ip rsvp interface configuration command.
Number of priority	Number of priorities that are supported.
Priority	Bandwidth (in bytes per second) that is available for traffic engineering at certain priorities.
Affinity Bit	Affinity bits (color) assigned to the link.

show ip protocols vrf

To display the routing protocol information associated with a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **show ip protocols vrf** command in user EXEC or privileged EXEC mode.

show ip protocols vrf *vrf-name*

Syntax Description

<i>vrf-name</i>	Name assigned to a VRF.
-----------------	-------------------------

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

Use this command to display routing information associated with a VRF.

Examples

The following example shows information about a VRF named vpn1:

```
Router# show ip protocols vrf vpn1

Routing Protocol is "bgp 100"
  Sending updates every 60 seconds, next due in 0 sec
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Redistributing:connected, static
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.13.13.13      200           02:20:54
    10.18.18.18      200           03:26:15
  Distance:external 20 internal 200 local 200
```

[Table 20](#) describes the significant fields shown in the display.

Table 20 *show ip protocols vrf Field Descriptions*

Field	Description
Gateway	Displays the IP address of the router identifier for all routers in the network.
Distance	Displays the metric used to access the destination route.
Last Update	Displays the last time the routing table was updated from the source.

Related Commands

Command	Description
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip route vrf

To display the IP routing table associated with a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **show ip route vrf** command in user EXEC or privileged EXEC mode.

```
show ip route vrf vrf-name [connected] [protocol [as-number] [tag] [output-modifiers]] [ip-prefix]
[list number [output-modifiers]] [profile] [static [output-modifiers]] [summary
[output-modifiers]] [supernets-only [output-modifiers]]
```

Syntax Description

<i>vrf-name</i>	Name assigned to the VRF.
connected	(Optional) Displays all connected routes in a VRF.
<i>protocol</i>	(Optional) To specify a routing protocol, use one of the following keywords: bgp , egp , eigrp , hello , igrp , isis , ospf , or rip .
<i>as-number</i>	(Optional) Autonomous system number.
<i>tag</i>	(Optional) Cisco IOS routing area label.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
<i>ip-prefix</i>	(Optional) Specifies a network to display.
list number	(Optional) Specifies the IP access list to display.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
supernets-only	(Optional) Displays supernet entries only.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	The <i>ip-prefix</i> argument was added. The output from the show ip route vrf vrf-name ip-prefix command was enhanced to display information on the multipaths to the specified network.

Usage Guidelines

This command displays specified information from the IP routing table of a VRF.

Examples

This example shows the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o - ODR
T - traffic engineered route

```

Gateway of last resort is not set

```

B   51.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C   50.0.0.0/8 is directly connected, Ethernet1/3
B   11.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B   12.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20

```

This example shows BGP entries in the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1 bgp
```

```

B   51.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B   11.0.0.0/8 [20/0] via 51.0.0.1, 03:44:12
B   12.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14

```

This example shows the IP routing table associated with a VRF named PATH and network 10.22.22.0:

```
Router# show ip route vrf PATH 10.22.22.0
```

```

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.22.5.10 00:01:07 ago
  Routing Descriptor Blocks:
  * 1.22.7.8 (Default-IP-Routing-Table), from 1.11.3.4, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  1.22.1.9 (Default-IP-Routing-Table), from 1.11.1.2, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  1.22.6.10 (Default-IP-Routing-Table), from 1.11.6.7, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  1.22.4.10 (Default-IP-Routing-Table), from 1.11.4.5, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  1.22.5.10 (Default-IP-Routing-Table), from 1.11.5.6, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1

```

[Table 21](#) describes the significant fields shown when using the `show ip route vrf vrf-name ip-prefix` command.

Table 21 *show ip route vrf Field Descriptions*

Field	Description
Routing entry for 10.22.22.0/24	Network number.
Known via ...	Indicates how the route was derived.
distance	Administrative distance of the information source.
metric	The metric to reach the destination network.
Tag	Integer that is used to implement the route.
type	Indicates that the route is a L1 type or L2 type route.

Table 21 *show ip route vrf Field Descriptions (continued)*

Field	Description
Last update from 10.22.5.10	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
<i>hh:mm:ss</i> ago	Specifies the last time the route was updated (in hours:minutes:seconds).
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
<i>ip-address</i> , from <i>ip-address</i> , <i>hh:mm:ss</i> ago	Indicates the next hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received (in hours:minutes:seconds).
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.
AS Hops	Number of hops to the destination or to the router where the route first enters iBGP.

Related Commands

Command	Description
show ip cache	Displays the CEF forwarding table associated with a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip rsvp fast bw-protect

To display information about whether backup bandwidth protection is enabled and the status of backup tunnels that may be used to provide that protection, use the **show ip rsvp fast bw-protect** command in EXEC mode.

show ip rsvp fast bw-protect

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	12.0(29)S	This command was introduced.

Examples The following is sample output from the **show ip rsvp fast bw-protect** command:

```
Router# show ip rsvp fast bw-protect
```

Primary Tunnel	Protect I/F	BW BPS:Type	Backup Tunnel:Label	State	BW-P	Type
PRAB-72-5_t500	PO2/0	500K:S	Tu501:19	Ready	ON	Nhop
PRAB-72-5_t601	PO2/0	103K:S	Tu501:20	Ready	OFF	Nhop
PRAB-72-5_t602	PO2/0	70K:S	Tu501:21	Ready	ON	Nhop
PRAB-72-5_t603	PO2/0	99K:S	Tu501:22	Ready	ON	Nhop
PRAB-72-5_t604	PO2/0	100K:S	Tu501:23	Ready	OFF	Nhop
PRAB-72-5_t605	PO2/0	101K:S	Tu501:24	Ready	OFF	Nhop

[Table 22](#) describes the significant fields shown in the display.

Table 22 *show ip rsvp fast bw-protect* Field Descriptions

Field	Description
Primary Tunnel	Identification of the tunnel being protected.
Protect I/F	Interface name.
BW BPS:Type	Bandwidth, in bits per second, and type of bandwidth. Possible values are: <ul style="list-style-type: none"> S—Sub-pool G—Global-pool
Backup Tunnel:Label	Identification of the backup tunnel.

Table 22 *show ip rsvp fast bw-protect Field Descriptions (continued)*

Field	Description
State	Status of backup tunnel. Valid values are: <ul style="list-style-type: none"> • Ready—Data is passing through the primary tunnel, but the backup tunnel is ready to take over if the primary tunnel goes down. • Active—The primary tunnel is down, so the backup tunnel is used for traffic. • None—There is no backup tunnel.
BW-P	Status of backup bandwidth protection. Possible values are ON and OFF.
Type	Type of backup tunnel. Possible values are: <ul style="list-style-type: none"> • NHOP—Next hop • NNHOP—Next-next hop

Related Commands

Command	Description
tunnel mpls traffic-eng fast-reroute bw-protect	Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.

show ip rsvp fast detail

To display specific information for Resource Reservation Protocol (RSVP) categories, use the **show ip rsvp fast detail** command in EXEC mode.

show ip rsvp fast detail

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	12.0(24)S	This command was introduced
	12.0(29)S	Bandwidth Prot desired was added in the Flag field of the command output.

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

```
Router# show ip rsvp fast detail

PATH:
Tun Dest: 15.0.0.7 Tun ID: 500 Ext Tun ID: 15.0.0.5
Tun Sender: 15.0.0.5 LSP ID: 8
Path refreshes:
  sent: to NHOP 50.5.6.6 on POS2/0
Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
  Session Name: PRAB-72-5_t500
ERO: (incoming)
  15.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
  50.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
  50.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  15.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
ERO: (outgoing)
  50.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
  50.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  15.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
Fast-Reroute Backup info:
  Inbound FRR: Not active
  Outbound FRR: Ready -- backup tunnel selected
  Backup Tunnel: Tu501 (label 19)
  Bkup Sender Template:
    Tun Sender: 51.5.6.5 LSP ID: 8
  Bkup FilerSpec:
    Tun Sender: 51.5.6.5, LSP ID: 8
Path ID handle: 04000405.
```

```
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxied
Output on POS2/0. Policy status: Forwarding. Handle: 02000406
```

Table 23 describes the significant fields shown in the display.

Table 23 show ip rsvp fast detail Field Descriptions

Field	Description
Tunnel Dest	IP address of the receiver.
Tunnel ID	Tunnel identification number.
Ext Tun ID	Extended tunnel identification number.
Tun Sender	IP address of the sender.
LSP ID	Label-switched path identification number.
Setup Prio	Setup priority.
Holding Prio	Holding priority.
Flags	Backup bandwidth protection has been configured for the LSP.
Session Name	Name of the session.
ERO (incoming)	EXPLICIT_ROUTE object of incoming Path messages.
ERO (outgoing)	EXPLICIT_ROUTE object of outgoing Path messages.
Traffic params Rate	Average rate, in bits per second.
Max burst	Maximum burst size, in bytes.
Min Policed Units	Minimum policed units, in bytes.
Max Pkt Size	Maximum packet size, in bytes.
Inbound FRR	Status of inbound Fast ReRoute (FRR) backup tunnel. If this node is downstream from a rerouted LSP (for example, at a merge point for this LSP), the state is Active.
Outbound FRR	Status of outbound FRR backup tunnel. If this node is a PLR for an LSP, there are three possible states: <ul style="list-style-type: none"> Active—This LSP is actively using its backup tunnel, presumably because there has been a downstream failure. No Backup—This LSP does not have local (Fast ReRoute) protection. No backup tunnel has been selected for it to use in case of a failure. Ready—This LSP is ready to use a backup tunnel in case of a downstream link or node failure. A backup tunnel has been selected for it to use.
Backup Tunnel	If the Outbound FRR state is Ready or Active, this field indicates the following: <ul style="list-style-type: none"> Which backup tunnel has been selected for this LSP to use in case of a failure. The inbound label that will be prepended to the LSP's data packets for acceptance at the backup tunnel tail (the merge point).

Table 23 show ip rsvp fast detail Field Descriptions (continued)

Field	Description
Bkup Sender Template	If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if/when the LSP starts actively using the backup tunnel. They differ from the original (pre-failure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, Path and PathTear messages will contain the new SENDER_TEMPLATE. Resv and ResvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes.
Bkup FilerSpec	If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if/when the LSP starts actively using the backup tunnel. They differ from the original (pre-failure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, Path and PathTear messages will contain the new SENDER_TEMPLATE. Resv and ResvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes.
Path ID handle	PSB identifier.
Incoming policy	Policy decision of the LSP. If RSVP policy was not granted for the incoming Path message for the tunnel, the LSP does not come up. Accepted is displayed.
Policy source(s)	For FRR LSPs, this value always is MPLS/TE for the policy source.
Status	For FRR LSPs, valid values are: <ul style="list-style-type: none"> • Proxied—Headend routers • Proxied Terminated—Tailend routers For midpoint routers, the field always is blank.

Related Commands

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

show ip rsvp host

To display Resource Reservation Protocol (RSVP) terminal point information for receivers or senders, use the **show ip rsvp host** command in user EXEC or privileged EXEC mode.

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

Syntax Description		
senders		Displays information for senders.
receivers		Displays information for receivers.
<i>hostname</i>		(Optional) Restricts the display to sessions with <i>hostname</i> as their destination.
<i>A.B.C.D</i>		(Optional) Restricts the display to sessions with the specified IP address as their destination.

Command Modes	
	User EXEC Privileged EXEC

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

Examples

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

```
Router# show ip rsvp host receivers
```

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

[Table 24](#) describes the significant fields shown in the display.

Table 24 show ip rsvp host Field Descriptions

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

Table 24 *show ip rsvp host Field Descriptions (continued)*

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

Related Commands

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

show ip vrf

To display the set of defined Virtual Private Network (VPN) routing/forwarding instances (VRFs) and associated interfaces, use the **show ip vrf** command in privileged EXEC mode.

```
show ip vrf [brief | detail | interfaces | id] [vrf-name] [output-modifiers]
```

Syntax Description		
brief	(Optional)	Displays concise information on the VRFs and associated interfaces.
detail	(Optional)	Displays detailed information on the VRFs and associated interfaces.
interfaces	(Optional)	Displays detailed information about all interfaces bound to a particular VRF or any VRF.
id	(Optional)	Displays the VPN IDs that are configured in a PE router for different VPNs.
<i>vrf-name</i>	(Optional)	Name assigned to a VRF.
<i>output-modifiers</i>	(Optional)	For a list of associated keywords and arguments, use context-sensitive help.

Defaults When no keywords or arguments are specified, the command shows concise information about all configured VRFs.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.0(17)ST	This command was modified to include the id keyword, and VPN ID information was added to the output of the show ip vrf detail command.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
	12.3(6)	This command was integrated into Cisco IOS Release 12.3(6). The command shows the downstream VRF for each associated VAI.

Usage Guidelines Use this command to display information about VRFs. Two levels of detail are available:

- The **brief** keyword (or no keyword) displays concise information.
- The **detail** keyword displays all information.

To display information about all interfaces bound to a particular VRF, or to any VRF, use the **interfaces** keyword. To display information about VPN IDs assigned to a PE router, use the **id** keyword.

Examples

The following example displays information about all the VRFs configured on the router, including the downstream VRF for each associated VAI. The lines that are highlighted (for documentation purposes only) indicate the downstream VRF.

```
Router# show ip vrf

Name      Default RD   Interface
D         2:0          Loopback2
           Virtual-Access3 [D]
           Virtual-Access4 [D]

U         2:1          Virtual-Access3
           Virtual-Access4
```

Table 25 describes the significant fields shown in the display.

Table 25 show ip vrf Field Descriptions

Field	Description
Name	Specifies the VRF name.
Default RD	Specifies the default route distinguisher.
Interfaces	Specifies the network interfaces.

The following example displays detailed information about all of the VRFs configured on the router, including all of the VAIs associated with each VRF:

```
Router# show ip vrf detail

VRF D; default RD 2:0; default VPNID <not set>
  Interfaces:
    Loopback2          Virtual-Access3 [D]  Virtual-Access4 [D]
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:2:0
  Import VPN route-target communities
    RT:2:1
  No import route-map
  No export route-map
VRF U; default RD 2:1; default VPNID <not set>
  Interfaces:
    Virtual-Access3          Virtual-Access4
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  Import VPN route-target communities
    RT:2:1
  No import route-map
  No export route-map
```

Table 26 describes the significant fields shown in the display.

Table 26 show ip vrf detail Field Descriptions

Field	Description
VPNID	Specifies the VPN ID assigned to the VRF.
Interfaces	Specifies the network interfaces.
Virtual-Access n [D]	Specifies the downstream VRF.

Table 26 *show ip vrf detail Field Descriptions (continued)*

Export	Specifies VPN route-target export communities.
Import	Specifies VPN route-target import communities.

The following example shows the interfaces bound to a particular VRF:

```
Router# show ip vrf interfaces

Interface      IP-Address      VRF              Protocol
Ethernet2      130.22.0.33     blue_vrf         up
Ethernet4      130.77.0.33     hub              up
Router#
```

Table 27 describes the significant fields shown in the display.

Table 27 *show ip vrf interfaces Field Descriptions*

Field	Description
Interface	Specifies the network interfaces for a VRF.
IP-Address	Specifies the IP address of a VRF interface.
VRF	Specifies the VRF name.
Protocol	Displays the state of the protocol (up or down) for each VRF interface.

The following is sample output that shows all the VPN IDs that are configured in the router and their associated VRF names and VRF route distinguishers (RDs):

```
Router# show ip vrf id
VPN Id      Name          RD
2:3         vpn2          <not set>
A1:3F6C     vpn1          100:1
```

Table 28 describes the significant fields shown in the display.

Table 28 *show ip vrf id Field Descriptions*

Field	Description
VPN ID	Specifies the VPN ID assigned to the VRF.
Name	Specifies the VRF name.
RD	Specifies the route distinguisher.

Related Commands

Command	Description
import map	Configures an import route map for a VRF.
ip vrf	Configures a VRF routing table.
ip vrf forwarding (interface configuration)	Associates a VRF with an interface or subinterface.
rd	Creates routing and forwarding tables for a VRF.
route-target	Creates a route-target extended community for a VRF.
vpn id	Assigns a VPN ID to a VRF.

show isis database verbose

To display additional information about the IS-IS database, use the **show isis database verbose** command in user EXEC or privileged EXEC mode.

show isis database verbose

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.

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

```
Router# show isis database verbose

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

[Table 29](#) describes the significant fields shown in the display.

Table 29 show isis database verbose Field Descriptions

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

Table 29 *show isis database verbose Field Descriptions (continued)*

Field	Description
Reservable BW	Amount of reservable bandwidth on this link.
BW Unreserved	Amount of bandwidth that is available for reservation.

The following example includes a route tag:

Router# **show isis database verbose**

```
IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num   LSP Checksum   LSP Holdtime   ATT/P/OL
dasher.00-00   0x000000F8    0xE57B         518             1/0/0
  Area Address: 49.0002
  NSPID:        0xCC
  Hostname: dasher
  IP Address: 10.3.0.1
  Metric: 10    IP 172.19.170.0/24
  Metric: 10    IP 4.1.1.0/24
  Metric: 10    IP 10.3.0.0/30
  Metric: 10    IS-Extended dasher.02172.19.170.0/24
  Metric: 20    IP-Interarea 1.1.1.1/32
    Route Admin Tag: 60
  Metric: 20    IP-Interarea 205.171.0.6/32
    Route Admin Tag: 50
```

Related Commands

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

show isis mpls traffic-eng adjacency-log

To display a log of 20 entries of Multiprotocol Label Switching (MPLS) traffic engineering Intermediate System-to-Intermediate System (IS-IS) adjacency changes, use the **show isis mpls traffic-eng adjacency-log** command in user EXEC or privileged EXEC mode.

show isis mpls traffic-eng adjacency-log

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.

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

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

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

[Table 30](#) describes the significant fields shown in the display.

Table 30 *show isis mpls traffic-eng adjacency-log Field Descriptions*

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

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

show isis mpls traffic-eng advertisements

To display the last flooded record from Multiprotocol Label Switching (MPLS) traffic engineering, use the **show isis mpls traffic-eng advertisements** command in user EXEC or privileged EXEC mode.

show isis mpls traffic-eng 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.

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

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

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

[Table 31](#) describes the significant fields shown in the display.

Table 31 *show isis mpls traffic-eng advertisements Field Descriptions*

Field	Description
System ID	Identification value for the local system in the area.
Router ID	MPLS traffic engineering router ID.
Link Count	Number of links that MPLS traffic engineering advertised.
Neighbor System ID	Identification value for the remote system in an area.
Interface IP address	IPv4 address of the interface.
Neighbor IP Address	IPv4 address of the neighbor.

Table 31 *show isis mpls traffic-eng advertisements Field Descriptions (continued)*

Field	Description
Admin. Weight	Administrative weight associated with this link.
Physical BW	Link bandwidth capacity (in bits per second).
Reservable BW	Amount of reservable bandwidth on this link.
BW unreserved	Amount of bandwidth that is available for reservation.
Affinity Bits	Link attribute flags being flooded.

Related Commands

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

show isis mpls traffic-eng tunnel

To display information about tunnels considered in the Intermediate System-to-Intermediate System (IS-IS) next hop calculation, use the **show isis mpls traffic-eng tunnel** command in privileged EXEC mode.

show isis mpls traffic-eng tunnel

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

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

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

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

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

[Table 32](#) describes the significant fields shown in the display.

Table 32 *show isis mpls traffic-eng tunnel Field Descriptions*

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

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

