Cisco IOS Multiprotocol Label Switching Command Reference

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

A through D

address-family

To enter the address family submode for configuring routing protocols such as Border Gateway Protocol (BGP), Routing Information Protocol (RIP), and static routing, use the **address-family** command in address family configuration submode. To disable the address family submode for configuring routing protocols, use the **no** form of this command.

VPN-IPv4 Unicast
address-family vpnv4 [**unicast**]
no address-family vpnv4 [**unicast**]

IPv4 Unicast
address-family ipv4 [**unicast**]
no address-family ipv4 [**unicast**]

IPv4 Unicast with CE router
address-family ipv4 [**unicast**] **vrf** *vrf-name*
no address-family ipv4 [**unicast**] **vrf** *vrf-name*

Syntax Description

vpnv4	Configures sessions that carry customer Virtual Private Network (VPN)-IPv4 prefixes, each of which has been made globally unique by adding an 8-byte route distinguisher.
ipv4	Configures sessions that carry standard IPv4 address prefixes.
unicast	(Optional) Specifies unicast prefixes.
vrf *vrf-name*	Specifies the name of a VPN routing/forwarding instance (VRF) to associate with submode commands.

Command Default

Routing information for address family IPv4 is advertised by default when you configure a BGP session using the **neighbor remote-as** command unless you execute the **no bgp default ipv4-activate** command.

Command Modes

Address family configuration

Command History

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

Using the **address-family** command puts the router in address family configuration submode (prompt: (config-router-af)#). Within this submode, you can configure address-family specific parameters for routing protocols, such as BGP, that can accommodate multiple Layer 3 address families.

To leave address family configuration submode and return to router configuration mode, enter the **exit-address-family** or the **exit** command.

Examples

The **address-family** command in the following example puts the router into address family configuration submode for the VPNv4 address family. Within the submode, you can configure advertisement of Network Layer Reachability Information (NLRI) for the VPNv4 address family using **neighbor activate** and other related commands:

```
router bgp 100
address-family vpnv4
```

The **address-family** command in the following example puts the router into address family configuration submode for the IPv4 address family. Use this form of the command, which specifies a VRF, only to configure routing exchanges between provider edge (PE) and customer edge (CE) devices. This **address-family** command causes subsequent commands entered in the submode to be executed in the context of VRF vrf2. Within the submode, you can use **neighbor activate** and other related commands to accomplish the following:

- Configure advertisement of IPv4 NLRI between the PE and CE routers.
- Configure translation of the IPv4 NLRI (that is, translate IPv4 into VPNv4 for NLRI received from the CE, and translate VPNv4 into IPv4 for NLRI to be sent from the PE to the CE).
- Enter the routing parameters that apply to this VRF.

The following example shows how to enter the address family submode:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 unicast vrf vrf2
```

Related Commands

Command	Description
default	Exits from address family submode.
neighbor activate	Enables the exchange of information with a neighboring router.

address-family l2vpn

To enter address family configuration mode to configure a routing session using Layer 2 Virtual Private Network (L2VPN) endpoint provisioning address information, use the **address-family l2vpn** command in router configuration mode. To remove the L2VPN address family configuration from the running configuration, use the **no** form of this command.

address-family l2vpn [**evpn | vpls**]
no address-family l2vpn [**evpn | vpls**]

Syntax Description

evpn	(Optional) Specifies L2VPN Ethernet Virtual Private Network (EVPN) endpoint provisioning address information.
vpls	(Optional) Specifies L2VPN Virtual Private LAN Service (VPLS) endpoint provisioning address information.

Command Default

No L2VPN endpoint provisioning support is enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
Cisco IOS XE Release 3.11S	This command was modified. The **evpn** keyword was added.

Usage Guidelines

The **address-family l2vpn** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that support L2VPN endpoint provisioning.

BGP support for the L2VPN address family introduces a BGP-based autodiscovery mechanism to distribute L2VPN endpoint provisioning information. BGP uses a separate L2VPN routing information base (RIB) to store endpoint provisioning information, which is updated each time any Layer 2 (L2) virtual forwarding instance (VFI) is configured. Prefix and path information is stored in the L2VPN database, allowing BGP to make best-path decisions. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to set up a pseudowire mesh to support L2VPN-based services.

The BGP autodiscovery mechanism facilitates the setting up of L2VPN services, which are an integral part of the Cisco IOS Virtual Private LAN Service (VPLS) feature. VPLS enables flexibility in deploying services by connecting geographically dispersed sites as a large LAN over high-speed Ethernet in a robust and scalable IP MPLS network.

The multiprotocol capability for address family L2VPN EVPN is advertised when the Address Family Identifier (AFI) is enabled under the internal BGP (iBGP) and external BGP (eBGP) neighbors for both IPv4 and IPv6 neighbors.

Note Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Examples

In this example, two provider edge (PE) routers are configured with VPLS endpoint provisioning information that includes L2 VFI, VPN, and VPLS IDs. BGP neighbors are configured and activated under L2VPN address family to ensure that the VPLS endpoint provisioning information is saved to a separate L2VPN RIB and then distributed to other BGP peers in BGP update messages. When the endpoint information is received by the BGP peers, a pseudowire mesh is set up to support L2VPN-based services.

Router A

```
enable
configure terminal
l2 vfi customerA autodiscovery
 vpn id 100
 vpls-id 45000:100
 exit
l2 vfi customerB autodiscovery
 vpn id 200
 vpls-id 45000:200
 exit
router bgp 45000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 172.16.1.2 remote-as 45000
 neighbor 172.21.1.2 remote-as 45000
 address-family l2vpn vpls
 neighbor 172.16.1.2 activate
 neighbor 172.16.1.2 send-community extended
 neighbor 172.21.1.2 activate
 neighbor 172.21.1.2 send-community extended
 end
```

Router B

```
enable
configure terminal
l2 vfi customerA autodiscovery
 vpn id 100
 vpls-id 45000:100
 exit
l2 vfi customerB autodiscovery
 vpn id 200
 vpls-id 45000:200
 exit
router bgp 45000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 172.16.1.1 remote-as 45000
 neighbor 172.22.1.1 remote-as 45000
```

```
address-family l2vpn vpls
neighbor 172.16.1.1 activate
neighbor 172.16.1.1 send-community extended
neighbor 172.22.1.1 activate
neighbor 172.22.1.1 send-community extended
end
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
show ip bgp l2vpn	Displays L2VPN address family information.

affinity

To specify attribute flags for links of a label switched path (LSP) in an LSP attribute list, use the **affinity** command in LSP Attributes configuration mode. To remove the specified attribute flags, use the **no** form of this command.

affinity *value* [**mask** *value*]
no affinity

Syntax Description

value	Attribute flag value required for links that make up an LSP. Values of the bits are either 0 or 1.
mask *value*	(Optional) Indicates which attribute values should be checked. If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of that link and the required affinity of the tunnel for that bit must match.

Command Default

Attribute values are not checked.

Command Modes

LSP Attributes configuration (config-lsp-attr)

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.

Usage Guidelines

Use this command to set the affinity and affinity mask values for an LSP in an LSP attribute list.

The affinity value determines the attribute flags for links that make up the LSP, either 0 or 1. The attribute mask determines which attribute value the router should check. If a bit in the mask is 0, an attribute value of a link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of a link and the required affinity of the LSP for that bit must match.

An LSP can use a link if the link affinity equals the attribute flag value and the affinity mask value.

Any value set to 1 in the affinity should also be set to 1 in the mask.

To associate the LSP affinity attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example sets the affinity values for a path option in an LSP attribute list:

```
configure terminal
!
mpls traffic-eng lsp attributes 1
```

```
 affinity 0 mask 0
 exit
end
```

Related Commands

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

allocate

To configure local label allocation filters for learned routes for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), use the **allocate** command in MPLS LDP label configuration mode. To remove the specific MPLS LDP local label allocation filter without resetting the LDP session, use the **no** form of this command.

allocate global {**prefix-list** {*list-namelist-number*} | **host-routes**}
no allocate global {**prefix-list** {*list-namelist-number*} | **host-routes**}

Syntax Description

global	Specifies the global routing table.
prefix-list	Specifies a prefix list to be used as a filter for MPLS LDP local label allocation.
list-name	Name that identifies the prefix list.
list-number	Number that identifies the prefix list.
host-routes	Specifies that host routes be used as a filter for MPLS LDP local label allocation.

Command Default

Prefix filters are not configured for MPLS LDP local label allocation.

Command Modes

MPLS LDP label configuration (config-ldp-lbl)

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

LDP allocates local labels for all learned routes or prefixes. Use the **allocate** command to specify a prefix list or a host route to control local label allocation filtering.

If you configure the **allocate** command with a prefix list as the filter and the prefix list does not exist, a prefix list is created that initially permits all prefixes.

You can configure only one prefix list for the global routing table. Configuring a different prefix list overrides the existing configuration.

If you configure the **allocate** command with host routes as the filter, then LDP allocates local labels for host routes only.

The **no** form in a specific **allocate** command removes that particular local label allocation configuration from the global table.

Examples

The following example shows how to configure a prefix list named List1 found in the global routing table as a filter for MPLS LDP local label allocation:

```
configure terminal
!
```

```
mpls ldp label
 allocate global prefix-list List1
 end
```

LDP allocates local labels only for prefixes that match the configured prefix list.

The following example shows how to remove a local label allocation filter:

```
configure terminal
!
mpls ldp label
 no allocate global prefix-list List1
 end
```

The following example shows how to configure host routes as the filter for the MPLS LDP local label allocation:

```
configure terminal
!
mpls ldp label
 allocate global host-routes
 end
```

LDP allocates local labels only for host routes found in the global routing table.

Related Commands

Command	Description
mpls ldp label	Enters MPLS LDP label configuration mode to specify how MPLS LDP handles local label allocation.
show mpls ldp label bindings	Displays the contents of the LIB.

append-after

To insert a path entry after a specified index number, use the **append-after** command in IP explicit path configuration mode.

append-after *index command*

Syntax Description

index	Previous index number. Valid values are from 0 to 65534.
command	An IP explicit path configuration command that creates a path entry. (Use the **next-address** command to specify the next IP address in the explicit path.)

Command Default

No path entry is inserted after a specified index number.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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

In the following example, the **next-address** command is inserted after index 5:

```
Router(config-ip-expl-path)# append-after 5 next-address 10.3.27.3
```

Related Commands

Command	Description
index	Inserts or modifies a path entry at a specific index.
interface fastethernet	Enters the command mode for IP explicit paths and creates or modifies the specified path.
list	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

auto-bw (LSP Attributes)

To specify automatic bandwidth configuration for a label switched path (LSP) in an LSP attribute list, use the **auto-bw** command in LSP Attributes configuration mode. To remove automatic bandwidth configuration, use the **no** form of this command.

auto-bw [**frequency** *secs*] [**max-bw** *kbps*] [**min-bw** *kbps*] [**collect-bw**]
no auto-bw

Syntax Description

frequency *secs*	(Optional) Interval between bandwidth adjustments. The specified interval can be from 300 to 604800 seconds.
max-bw *kbps*	(Optional) Maximum automatic bandwidth for the path option. The value can be from 0 to 4294967295 kilobits per second (kbps).
min-bw *kbps*	(Optional) Minimum automatic bandwidth for the path option. The value is from 0 to 4294967295 kilobits per second (kbps).
collect-bw	(Optional) Collects output rate information for the path option, but does not adjust its bandwidth.

Command Default

If the command is entered with no optional keywords, automatic bandwidth adjustment for the LSP is enabled, with adjustments made every 24 hours and with no constraints on the bandwidth adjustments made. If the **collect-bw** keyword is entered, the bandwidth is sampled but not adjusted, and the other options, if any, are ignored. If the **collect-bw** keyword is not entered and some, but not all of the other keywords are entered, the defaults for the keywords not entered are: **frequency**, every 24 hours; **min-bw**, unconstrained (0); **max-bw**, unconstrained.

Command Modes

LSP Attributes configuration (config-lsp-attr)

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 Everest 16.6.1	This command was introduced.

Usage Guidelines

Use this command to set an automatic bandwidth configuration in an LSP attributes list.

To sample the bandwidth used by an LSP without automatically adjusting it, specify the **collect-bw** keyword in the **auto-bw** command in an LSP attribute list.

If you enter the **auto-bw** command without the **collect-bw** keyword, the bandwidth of the LSP is adjusted to the largest average output rate sampled for the LSP since the last bandwidth adjustment for the LSP was made.

To constrain the bandwidth adjustment that can be made to an LSP in an LSP attribute list, use the **max-bw** or the **min-bw** keyword and specify the permitted maximum allowable bandwidth or minimum allowable bandwidth, respectively.

The **no auto-bw** command disables bandwidth adjustment for the tunnel and restores the configured bandwidth for the LSP where configured bandwidth is determined as follows:

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

To associate the LSP automatic bandwidth adjustment attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example sets automatic bandwidth configuration for an LSP in an LSP attribute list:

```
configure terminal
!
mpls traffic-eng lsp attributes 1
 auto-bw
 exit
end
```

Related Commands

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

auto-route-target

To enable the automatic generation of a route target, use the **auto-route-target** command in L2 VFI configuration or VFI autodiscovery configuration mode. To remove the automatically generated route targets, use the **no** form of this command.

auto-route-target
no auto-route-target

Syntax Description

This command has no arguments or keywords.

Command Default

A route target is automatically enabled.

Command Modes

L2 VFI configuration (config-vfi)

VFI autodiscovery configuration (config-vfi-autodiscovery)

Command History

Release	Modification
12.2(33)SRB	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 VFI autodiscovery configuration mode.

Usage Guidelines

Use this command with the **l2 vfi autodiscovery** or the **autodiscovery (MPLS)** command, which automatically creates route targets. The **no** form of this command allows you to remove the automatically generated route targets. You cannot enter this command if route targets have not been automatically created yet.

Examples

The following example shows how to generate route targets for Border Gateway Protocol (BGP) autodiscovered pseudowire members with Label Discovery Protocol (LDP) signaling:

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 100
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi-autodiscovery)# auto-route-target
```

The following example shows how to remove automatically generated route targets in VFI configuration mode:

```
Device(config-vfi)# no auto-route-target
```

Related Commands

Command	Description
autodiscovery (MPLS)	Designates a VFI as having BGP autodiscovered pseudowire members.
l2 vfi autodiscovery	Enables the VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.
route-target (VPLS)	Specifies a route target for a VPLS VFI.

autodiscovery (MPLS)

To designate a Layer 2 virtual forwarding interface (VFI) as having Border Gateway Protocol (BGP) or Label Distribution Protocol (LDP) autodiscovered pseudowire members, use the **autodiscovery** command in L2 VFI configuration mode. To disable autodiscovery, use the **no** form of this command.

autodiscovery bgp signaling {**bgp** | **ldp**}[{**template** *template-name*}]
no autodiscovery bgp signaling {**bgp** | **ldp**}[{**template** *template-name*}]

Syntax Description

bgp	Specifies that BGP should be used for signaling and autodiscovery.
ldp	Specifies that LDP should be used for signaling.
template *template-name*	Specifies the template to be used for autodiscovered pseudowires.

Command Default

Layer 2 VFI autodiscovery is disabled.

Command Modes

L2 VFI configuration (config-vfi)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support.. This command will replace the **l2 vfi autodiscovery** command in future releases.
Cisco IOS XE Release 3.8S	This command was modified. The **bgp** keyword was added.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **l2 vfi autodiscovery** command in future releases.

Layer 2 VFI autodiscovery enables each VPLS PE router to discover other PE routers that are part of the same VPLS domain. VPLS autodiscovery also automatically detects when PE routers are added to or removed from the VPLS domain

The **bgp** keyword specifies that BGP should be used for signaling and autodiscovery, accordance with RFC 4761.

The **ldp** keyword specifies that LDP should be used for signaling. BGP will be used for autodiscovery.

Use of the **autodiscovery** command places the device into L2VPN VFI autodiscovery configuration mode (config-vfi-autodiscovery).

Examples

The following example shows how to enable Layer 2 VFI as having BGP autodiscovered pseudowire members and specify that LDP signaling should be used for autodiscovery:

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 100
```

```
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi-autodiscovery)#
```

Related Commands

Command	Description
l2 vfi autodiscovery	Enables the VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.
vpn id	Sets or updates a VPN ID on a VPLS instance.

backup delay (L2VPN local switching)

To specify how long a backup pseudowire virtual circuit (VC) should wait before resuming operation after the primary pseudowire VC goes down, use the **backup delay** command in interface configuration mode or xconnect configuration mode.

backup delay *enable-delay* {*disable-delay* | **never**}

Syntax Description

enable-delay	Number of seconds that elapse after the primary pseudowire VC goes down before the Cisco IOS software activates the secondary pseudowire VC. The range is from 0 to 180. The default is 0.
disable-delay	Number of seconds that elapse after the primary pseudowire VC comes up before the Cisco IOS software deactivates the secondary pseudowire VC. The range is from 0 to 180. The default is 0.
never	Specifies that the secondary pseudowire VC will not fall back to the primary pseudowire VC if the primary pseudowire VC becomes available again unless the secondary pseudowire VC fails.

Command Default

If a failover occurs, the xconnect redundancy algorithm will immediately switch over or fall back to the backup or primary member in the redundancy group.

Command Modes

Interface configuration (config-if)
Xconnect configuration (config-if-xconn)

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 integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.

Examples

The following example shows a Multiprotocol Label Switching (MPLS) xconnect with one redundant peer. Once a switchover to the secondary VC occurs, there will be no fallback to the primary VC unless the secondary VC fails.

```
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config)# connect frpw1 serial0/1 50 l2transport
```

```
Router(config-if)# xconnect 10.0.0.1 50 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 50
Router(config-if-xconn)# backup delay 0 never
```

The following example shows an MPLS xconnect with one redundant peer. The switchover will not begin unless the Layer 2 Tunnel Protocol (L2TP) pseudowire has been down for 3 seconds. After a switchover to the secondary VC occurs, there will be no fallback to the primary until the primary VC has been reestablished and is up for 10 seconds.

```
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config)# connect frpw1 serial0/1 50 l2transport
Router(config-if)# xconnect 10.0.0.1 50 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 50
Router(config-if-xconn)# backup delay 3 10
```

Cisco CMTS Routers: Example

The following example sets a 2-second delay before resuming operation after the primary pseudowire VC goes down.

```
cable l2vpn 0011.0011.0011
 service instance 1 ethernet
  encapsulation default
  xconnect  10.2.2.2 22 encapsulation mpls
  backup delay 1 2
```

Related Commands

Command	Description
backup peer	Configures a redundant peer for a pseudowire VC.

backup peer

To specify a redundant peer for a pseudowire virtual circuit (VC), use the **backup peer** command in interface configuration mode or xconnect configuration mode. To remove the redundant peer, use the **no** form of this command.

backup peer *peer-router-ip-addr vcid* [**pw-class** *pw-class-name*] [**priority** *value*]
no backup peer *peer-router-ip-addr vcid*

Syntax Description

peer-router-ip-addr	IP address of the remote peer.
vcid	32-bit identifier of the VC between the routers at each end of the layer control channel.
pw-class	(Optional) Specifies the pseudowire type. If not specified, the pseudowire type is inherited from the parent xconnect.
pw-class-name	(Optional) Name of the pseudowire you created when you established the pseudowire class.
priority *value*	(Optional) Specifies the priority of the backup pseudowire in instances where multiple backup pseudowires exist. The default is 1. The range is from 1 to 10.

Command Default

No redundant peer is established.

Command Modes

Interface configuration (config-if)
Xconnect configuration (config-if-xconn)

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 integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.4	This command was modified. The ability to add up to three backup pseudowires was added. The **priority** keyword was added to assign priority to the backup pseudowires.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The combination of the *peer-router-ip-addr* and *vcid* arguments must be unique on the router.

In Cisco IOS XE Release 2.3, only one backup pseudowire is supported. In Cisco IOS XE Release 2.4 and later releases, up to three backup pseudowires are supported.

The Cisco IOS Release 12.2(33)SCF supports up to three backup pseudowires for a primary pseudowire. The priority keyword is optional when only one backup pseudowire is configured. This keyword is a required choice when multiple backup pseudowires are configured.

Examples

The following example shows how to configure a Multiprotocol Label Switching (MPLS) xconnect with one redundant peer:

```
Device(config)# pseudowire-class mpls
Device(config-pw-class)# encapsulation mpls
RoDeviceuter(config)# interface serial0/0
Device(config-if)# xconnect 10.0.0.1 100 pw-class mpls
Device(config-if-xconn)# backup peer 10.0.0.2 200
```

The following example shows how to configure a local-switched connection between ATM and frame relay using Ethernet interworking. The frame relay circuit is backed up by an MPLS pseudowire.

```
Device(config)# pseudowire-class mpls
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# interworking ethernet
Device(config)# connect atm-fr atm1/0 100/100 s2/0 100 interworking ethernet
Device(config-if)# backup peer 10.0.0.2 100 pw-class mpls
```

The following example shows how to configure a pseudowire with two backup pseudowires:

```
interface ATM4/0.1 point-to-point
 pvc 0/100 l2transport
  encapsulation aal5snap
  xconnect 10.1.1.1 100 pw-class mpls
   backup peer 10.1.1.1 101
   backup peer 10.10.1.1 110 priority 2
   backup peer 10.20.1.1 111 priority 9
```

Cisco CMTS Routers: Example

The following example shows how to set a redundant peer for a pseudowire.

```
cable l2vpn 0011.0011.0011
 service instance 1 ethernet
  encapsulation default
  xconnect  10.2.2.2 22 encapsulation mpls
    backup peer 10.3.3.3 33
```

Related Commands

Command	Description
backup delay	Specifies how long the backup pseudowire VC should wait before resuming operation after the primary pseudowire VC goes down.

bandwidth (LSP Attributes)

To configure label switched path (LSP) bandwidth in an LSP attribute list, use the **bandwidth** command in LSP Attributes configuration mode. To remove the configured bandwidth from the LSP attribute list, use the **no** form of this command.

bandwidth [{**sub-pool** | **global**}] *kbps*
no bandwidth

Syntax Description

sub-pool	(Optional) Indicates a subpool path option.
global	(Optional) Indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the **sub-pool** keyword.
kbps	Number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.

Command Default

The default bandwidth is 0.

Command Modes

LSP Attributes configuration (config-lsp-attr)

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.

Usage Guidelines

Use this command to configure LSP bandwidth in the LSP attribute list. The bandwidth configured can be associated with both dynamic and explicit path options.

To associate the LSP bandwidth and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

The bandwidth configured in the LSP attribute list will override the bandwidth configured on the tunnel.

Examples

The following example shows how to set the LSP bandwidth to 5000 kbps in the LSP attribute list identified with the numeral 2:

```
configure terminal
!
mpls traffic-eng lsp attributes 2
 bandwidth 5000

exit
end
```

Related Commands

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

bgp default ipv4-unicast

To set the IP version 4 (IPv4) unicast address family as default for BGP peering session establishment, use the **bgp default ipv4-unicast** command in router configuration mode. To disable default IPv4 unicast address family for peering session establishment, use the **no** form of this command.

bgp default ipv4-unicast
no bgp default ipv4-unicast

Syntax Description

This command has no arguments or keywords.

Command Default

IPv4 address family routing information is advertised by default for each BGP routing session configured with the **neighbor remote-as** command, unless you first configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(5)T	This command was introduced.
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 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **bgp default ipv4-unicast** command is used to enable the automatic exchange of IPv4 address family prefixes. The **neighbor activate** address family configuration command must be entered in each IPv4 address family session before prefix exchange will occur.

Examples

In the following example, the automatic exchange of IP version 4 unicast address family routing information is disabled:

```
Device(config)# router bgp 50000
Device(config-router)# no bgp default ipv4-unicast
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a neighboring router.

bgp default route-target filter

To enable automatic Border Gateway Protocol (BGP) default route-target community filtering, use the **bgp default route-target filter** command in router configuration mode. To disable automatic BGP route-target community filtering or to enable pseudowire switching in address family configuration mode, use the **no** form of this command.

bgp default route-target filter
no bgp default route-target filter

Syntax Description

This command has no arguments or keywords.

Command Default

Automatic BGP default route-target community filtering is enabled.

Command Modes

Router configuration (config-router)
Address family configuration (config-router-af)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.0(16)ST	This command was integrated into Cisco IOS Release 12.0(16)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
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.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S and the functionality of the **no** form of the command was modified. When this command is used in address family configuration mode, the **no bgp default route-target filter** command enables pseudowire switching on an Autonomous System Boundary Router (ASBR).
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **bgp default route-target filter** command to control the distribution of VPN routing information through the list of VPN route-target communities.

When you use the **no** form of this command, all received VPN-IPv4 routes are accepted by the configured router. Accepting VPN-IPv4 routes is the desired behavior for a router configured as an ASBR or as a customer edge (CE) BGP border edge router.

If you configure the router for BGP route-target community filtering, all received exterior BGP (EBGP) VPN-IPv4 routes are discarded when those routes do not contain a route-target community value that matches the import list of any configured VPN routing and forwarding (VRF) instances. This is the desired behavior for a router configured as a provider edge (PE) router.

Note This command is automatically disabled if a PE router is configured as a client of a common VPN-IPv4 route reflector in the autonomous system.

Enabling Pseudowire Switching at the ASBR

In Cisco IOS Release 15.1(1)S, the functionality of the **no bgp default route-target filter** command has been modified to support Virtual Private LAN Switching (VPLS) on an ASBR.

In router family configuration mode (router-config-af), which is entered by using the **address-family l2vpn** command, the **no bgp default route-target filter**command enables pseudowire switching.

Examples

In the following example, BGP route-target filtering is disabled for autonomous system 120:

```
router bgp 120
 no bgp default route-target filter
```

Pseudowire Switching Enabled at the ASBR

In the following example, pseudowire switching is enabled at the ASBR:

```
Router# enable
Router# configure terminal
Router(config)# router bgp 1
Router(config-router)# address-family l2vpn
Router(config-router-af)# no bgp default route-target filter
```

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning address information.

bgp log-neighbor-changes

To enable logging of BGP neighbor resets, use the **bgp log-neighbor-changes** command in router configuration mode. To disable the logging of changes in BGP neighbor adjacencies, use the **no** form of this command.

bgp log-neighbor-changes
no bgp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Logging of BGP neighbor resets is not enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0	This command was integrated into Cisco IOS release 12.0.
12.0(7)T	Address family configuration mode support was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
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.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **bgp log-neighbor-changes** command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

Using the **bgp log-neighbor-changes** command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging. If the UNIX syslog facility is enabled, messages are sent to the UNIX host running the syslog daemon so that the messages can be stored and archived. If the UNIX syslog facility is not enabled, the status change messages are retained in the internal buffer of the router, and are not stored to disk. You can set the size of this buffer, which is dependent upon the available RAM, using the **logging buffered** command.

The neighbor status change messages are not tracked if the **bgp log-neighbor-changes** command is not enabled, except for the reset reason, which is always available as output of the **show ip bgp neighbors** and **show bgp ipv6 neighbors** commands.

The **eigrp log-neighbor-changes** command enables logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, but messages for BGP neighbors are logged only if they are specifically enabled with the **bgp log-neighbor-changes** command.

Use the **show logging** command to display the log for the BGP neighbor changes.

Examples

The following example logs neighbor changes for BGP in router configuration mode:

```
Device(config)# bgp router 40000
Device(config-router)# bgp log-neighbor-changes
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
eigrp log-neighbor-changes	Enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.
logging buffered	Logs messages to an internal buffer.
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.
show ip bgp neighbors	Displays information about BGP neighbors.
show logging	Displays the state of logging (syslog).

bgp next-hop

To configure a loopback interface as the next hop for routes associated with a VPN routing and forwarding instance (VRF), use the **bgp next-hop** command in VRF configuration or in VRF address family configuration mode. To return the router to default operation, use the **no** form of this command.

bgp next-hop {**ipv4** | **ipv6**} **loopback** *number*
no bgp next-hop

Syntax Description

ipv4	Specifies the IPv4 address of the loopback (see the "Usage Guidelines" section).
ipv6	Specifies the IPv6 address of the loopback (see the "Usage Guidelines" section).
loopback *number*	Specifies the number of the loopback interface. The *number* argument is a number from 1 to 2147483647.

Command Default

The IP address of the source interface, from which the route was advertised is set as the next hop when this command is not enabled.

Command Modes

VRF configuration (config-vrf)
VRF address family configuration (config-vrf-af)

Command History

Release	Modification
12.2(13)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.3(1)S	This command was modified. The **ipv4** and **ipv6** keywords were added.

Usage Guidelines

The **bgp next-hop** command is used in Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) and Tunnel Engineering (TE) configurations. This command allows you to configure a loopback interface as the next hop for routes that are associated with the specified VRF. This command can be used, for example, to configure VPN traffic to use a specific Label Switched Path (LSP) through an MPLS core network.

The **ipv4** and **ipv6** keywords are available under the VRF definition for the IPv6 address family in the VRF address family configuration mode. See the "Examples" section.

Examples

In the following example, loopback interface 0 is configured as the next hop for VPN traffic associated with VRF RED:

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 40000:1
Router(config-vrf)# route-target import 40000:2
Router(config-vrf)# route-target export 40000:2
Router(config-vrf)# bgp next-hop loopback 0
```

The following example for an IPv6 address family defined under the **vrf definition** command shows how to configure loopback interface 0 as the next hop for VPN traffic associated with VRF vrf1:

```
Router(config)# vrf definition vfr1
Router(config-vrf)# rd 40000:1
Router(config-vrf)# address-family ipv6
Router(config-vrf-af)# route-target import 40000:2
Router(config-vrf-af)# route-target export 40000:2
Router(config-vrf-af)# bgp next-hop ipv6 loopback 0
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
ip vrf	Configures a VRF routing table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

bgp scan-time

To configure scanning intervals of Border Gateway Protocol (BGP) routers for next hop validation or to decrease import processing time of Virtual Private Network version 4 (VPNv4) routing information, use the **bgp scan-time** command in address family or router configuration mode. To return the scanning interval of a router to its default scanning interval of 60 seconds, use the **no** form of this command.

bgp scan-time [**import**] *scanner-interval*
no bgp scan-time [**import**] *scanner-interval*

Syntax Description

import	(Optional) Configures import processing of VPNv4 unicast routing information from BGP routers into routing tables.
scanner-interval	The scanning interval of BGP routing information. • Valid values are from 15 to 60 seconds. The default is 60 seconds.

Command Default

The default scanning interval is 60 seconds.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(7)T	This command was introduced.
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.
15.0(1)M	This command was modified. The **import** keyword was removed. It is not available in Cisco IOS Release 15.0(1)M and later Cisco IOS Release 15.0M releases.
12.2(33)SRE	This command was modified. The **import** keyword was removed. It is not available in Cisco IOS Release 12.2(33)SRE and later Cisco IOS Release 12.2SR releases.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(2)T	This command was modified. The minimum scan time is increased from 5 seconds to 15 seconds.
15.0(1)S	This command was modified. The minimum scan time is increased from 5 seconds to 15 seconds.
Cisco IOS XE 3.1S	This command was modified. The minimum scan time is increased from 5 seconds to 15 seconds.

Usage Guidelines

Entering the **no** form of this command does not disable scanning, but removes it from the output of the **show running-config** command.

The **import** keyword is supported in address family VPNv4 unicast mode only.

The BGP Event Based VPN Import feature introduced a modification to the existing BGP path import process using new commands and the **import** keyword was removed from the **bgp scan-time** command in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases.

While **bgp next-hop** address tracking (NHT) is enabled for an address family, the **bgp scan-time** command will not be accepted in that address family and will remain at the default value of 60 seconds. NHT must be disabled before the **bgp scan-time** command will be accepted in either router mode or address family mode.

Examples

In the following router configuration example, the scanning interval for next hop validation of IPv4 unicast routes for BGP routing tables is set to 20 seconds:

```
router bgp 100
 no synchronization
 bgp scan-time 20
```

In the following address family configuration example, the scanning interval for next hop validation of address family VPNv4 unicast routes for BGP routing tables is set to 45 seconds:

```
router bgp 150
 address-family vpn4 unicast
  bgp scan-time 45
```

In the following address family configuration example, the scanning interval for importing address family VPNv4 routes into IP routing tables is set to 30 seconds:

```
router bgp 150
 address-family vpnv4 unicast
  bgp scan-time import 30
```

Related Commands

Command	Description
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
bgp next-hop	Configures BGP next-hop address tracking.

cell-packing

To enable ATM over Multiprotocol Label Switching (MPLS) or Layer 2 Tunneling Protocol Version 3 (L2TPv3) to pack multiple ATM cells into each MPLS or L2TPv3 packet, use the **cell-packing** command in the appropriate configuration mode. To disable cell packing, use the **no** form of this command.

cell-packing *cells* **mcpt-timer** *timer*
no cell-packing

Syntax Description

cells	The number of cells to be packed into an MPLS or L2TPv3 packet. The range is from 2 to the maximum transmission unit (MTU) of the interface divided by 52. The default number of ATM cells to be packed is the MTU of the interface divided by 52. If the number of cells packed by the peer provider edge router exceeds this limit, the packet is dropped.
mcpt-timer *timer*	Specifies which timer to use for maximum cell-packing timeout (MCPT). Valid values are 1, 2, or 3. The default value is 1.

Command Default

Cell packing is disabled.

Command Modes

Interface configuration
L2transport PVC configuration--for ATM PVC
L2transport PVP configuration--for ATM PVP
VC class configuration

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.0(29)S	Support for L2TPv3 sessions was added.
12.0(30)S	This command was updated to enable cell packing as part of a virtual circuit (VC) class.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
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 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.
12.2(1)SRE	This command was modified. Support for static pseudowires was added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Release	Modification
Cisco IOS XE Release 3.1S.	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **cell-packing** command is available only if you configure the ATM VC or virtual path (VP) with ATM adaptation layer 0 (AAL0) encapsulation. If you specify ATM adaptation layer 5 (AAL5) encapsulation, the command is not valid.

Only cells from the same VC or VP can be packed into one MPLS or L2TPv3 packet. Cells from different connections cannot be concatenated into the same packet.

When you change, enable, or disable the cell-packing attributes, the ATM VC or VP and the MPLS or L2TPv3 emulated VC are reestablished.

If a provider edge (PE) router does not support cell packing, the PE router sends only one cell per MPLS or L2TPv3 packet.

The number of packed cells need not match between the PE routers. The two PE routers agree on the lower of the two values. For example, if PE1 is allowed to pack 10 cells per MPLS or L2TPv3 packet and PE2 is allowed to pack 20 cells per MPLS or L2TPv3 packet, the two PE routers would agree to send no more than 10 cells per packet.

If the number of cells packed by the peer PE router exceeds the limit, the packet is dropped.

If you issue the **cell-packing** command without first specifying the **atm mcpt-timers** command, you get the following error:

```
Please set mcpt values first
```

In order to support cell packing for static pseudowires, both PEs must run Cisco IOS Release 12.2(1)SRE, and the maximum number of cells that can be packed must be set to the same value on each.

Examples

The following example shows cell packing enabled on an interface set up for VP mode. The **cell-packing** command specifies that ten ATM cells be packed into each MPLS packet. The command also specifies that the second maximum cell-packing timeout (MCPT) timer be used.

```
Router> enable
Router# configure terminal
Router(config)# interface atm1/0
Router(config-if)# atm mcpt-timers 1000 800 500
Router(config-if)# atm pvp 100 l2transport
Router(config-if-atm-l2trans-pvp)# xconnect 10.0.0.1 234 encapsulation mpls
Router(config-if-atm-l2trans-pvp)# cell-packing 10 mcpt-timer 2
```

The following example shows how to configure ATM cell relay over MPLS with cell packing in VC class configuration mode. The VC class is then applied to an interface.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm cellpacking
Router(config-vc-class)# encapsulation aal0
Router(config-vc-class)# cell-packing 10 mcpt-timer 1
Router(config-vc-class)# exit
Router(config)# interface atm1/0
Router(config-if)# atm mcpt-timers 100 200 250
Router(config-if)# class-int cellpacking
```

```
Router(config-if)# pvc ½00 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

The following example shows how to configure ATM AAL5 over L2TPv3 in VC class configuration mode. The VC class is then applied to an interface.

```
Router(config)# vc-class atm aal5class
Router(config-vc-class)# encapsulation aal5
!
Router(config)# interface atm1/0
Router(config-if)# class-int aal5class
Router(config-if)# pvc ½00 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation l2tpv3
```

Related Commands

Command	Description
atm mcpt-timers	Creates cell-packing timers, which specify how long the PE router can wait for cells to be packed into an MPLS or L2TPv3 packet.
debug atm cell-packing	Displays ATM cell relay cell packing debugging information.
show atm cell-packing	Displays information about the VCs and VPs that have ATM cell packing enabled.

class

To associate a map class with a specified data-link connection identifier (DLCI), use the **class** command in Frame Relay DLCI configuration mode or Frame Relay VC-bundle-member configuration mode. To remove the association between the DLCI and the map class, use the **no** form of this command.

class *name*
no class *name*

Syntax Description

name	Name of the map class to associate with the specified DLCI.

Command Default

No map class is defined.

Command Modes

Frame Relay DLCI configuration
Frame Relay VC-bundle-member configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	This command was made available in Frame Relay VC-bundle-member configuration mode.
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)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use this command with DLCIs that were created using the **frame-relay interface-dlci** command and with DLCIs that were created as permanent virtual circuit (PVC) bundle members within a specified Frame Relay PVC bundle. The PVC bundle is created using the **frame-relay vc-bundle** command. The Frame Relay PVC bundle member DLCIs are then created by using the **pvc** command in Frame Relay VC-bundle configuration mode.

A map class applied to the interface is applied to all PVC members in a PVC bundle. A class applied to an individual PVC bundle member supersedes the class applied at the interface level.

The map class is created by using the **map-class frame-relay** command in global configuration mode.

Examples

The following example shows how to define a map class named slow-vcs and apply it to DLCI 100:

```
interface serial 0.1 point-to-point
 frame-relay interface-dlci 100
  class slow-vcs
```

```
map-class frame-relay slow-vcs
 frame-relay cir out 9600
```

The following example shows how to apply a map class to a DLCI for which a **frame-relay map** statement exists. The **frame-relay interface-dlci** command must also be used.

```
interface serial 0.2 point-to-multipoint
 frame-relay map ip 172.16.13.2 100
 frame-relay interface-dlci 100
 class slow-vcs
map-class frame-relay slow_vcs
 frame-relay traffic-rate 56000 128000
 frame-relay idle-timer 30
```

The following example creates a Frame Relay map class named class1 and shows how to assign it to PVC 300 in a Frame Relay PVC bundle named MP-3-static:

```
map-class frame-relay class1
interface serial 1/4
 frame-relay map ip 10.2.2.2 vc-bundle MP-3-static
 frame-relay vc-bundle MP-3-static
 pvc 300
 class HI
```

Example of the class Command for Defining Traffic Classes Inside a 802.1p Domain in Cisco IOS Release 12.2(33)SCF

The following example shows how to define traffic classes for the 8021.p domain with packet CoS values:

```
enable
configure terminal
 policy-map cos7
  class cos2
  set cos 2
  end
```

Example of the class Command for Defining Traffic Classes Inside an MPLS Domain in Cisco IOS Release 12.2(33)SCF

The following example shows how to define traffic classes for the MPLS domain with packet EXP values:

```
enable
configure terminal
 policy-map exp7
  class exp7
  set mpls experimental topmost 2
  end
```

Related Commands

Command	Description
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.

Command	Description
frame-relay map	Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.
frame-relay vc-bundle	Creates a Frame Relay PVC bundle and enters Frame Relay VC-bundle configuration mode.
map-class frame-relay	Creates a map class for which unique QoS values can be assigned.
pvc (frame-relay vc-bundle)	Creates a PVC and PVC bundle member and enters Frame Relay VC-bundle-member configuration mode.

class (MPLS)

To configure a defined Multiprotocol Label Switching (MPLS) class of service (CoS) map that specifies how classes map to label switched controlled virtual circuits (LVCs) when combined with a prefix map, use the **class** command in CoS map submode. To remove the defined MPLS CoS map, use the **no** form of this command.

class *class* [{**available** | **standard** | **premium** | **control**}]
no class *class* [{**available** | **standard** | **premium** | **control**}]

Syntax Description

class	The precedence of identified traffic to classify traffic.
available	(Optional) Means low precedence (In/Out plus lower two bits = 0,4).
standard	(Optional) Means next precedence (In/Out plus lower two bits = 1,5).
premium	(Optional) Means high precedence (In/Out plus lower two bits = 2,6).
control	(Optional) Means highest precedence pair (In/Out plus lower two bits = 3,7). These bits are reserved for control traffic.

Command Default

This command is disabled.

Command Modes

CoS map submode

Command History

Release	Modification
12.0(5)T	This command was introduced.
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 example shows how to configure a CoS map:

```
Router(config)# mpls cos-map 55
Router(config-mpls-cos-map)# class 1 premium
Router(config-mpls-cos-map)# exit
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
mpls cos-map	Creates a class map that specifies how classes map to LVCs when combined with a prefix map.

Command	Description
mpls prefix-map	Configures a router to use a specified quality of service (QoS) map when a label definition prefix matches the specified access list.
show mpls cos-map	Displays the CoS map used to assign quantity of LVCs and associated CoS of those LVCs.

class-map

To create a class map to be used for matching packets to a specified class and to enter QoS class-map configuration mode, use the **class-map** command in global configuration mode. To remove an existing class map from a device, use the **no** form of this command.

Cisco 2600, 3660, 3845, 6500, 7200, 7401, and 7500 Series Routers
class-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-class*}] [{**match-all** | **match-any**}] *class-map-name*
no class-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-class*}] [{**match-all** | **match-any**}] *class-map-name*

Cisco 7600 Series Routers
class-map *class-map-name* [{**match-all** | **match-any**}]
no class-map *class-map-name* [{**match-all** | **match-any**}]

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE
class-map *class-map-name*
no class-map *class-map-name*

Syntax Description

type	(Optional) Specifies the class-map type.
stack	(Optional) Enables the flexible packet matching (FPM) functionality to determine the protocol stack to examine. When you use the **load protocol** command to load protocol header description files (PHDFs) on the device, a stack of protocol headers can be defined so that the filter can determine which headers are present and in what order.
access-control	(Optional) Determines the pattern to look for in the configured protocol stack. **Note** You must specify a stack class map (by using the **type stack** keywords) before specifying an access-control class map (by using the **type access-control** keywords).
port-filter	(Optional) Creates a port-filter class map that enables the TCP or UDP port policing of control plane packets. When this keyword is enabled, the command filters the traffic that is destined to specific ports on the control-plane host subinterface.
queue-threshold	(Optional) Enables queue thresholding, which limits the total number of packets for a specified protocol allowed in the control plane IP input queue. The queue-thresholding applies only to the control-plane host subinterface.
logging *log-class*	(Optional) Enables the logging of packet traffic on the control plane. The value for the *log-class* argument is the name of the log class.
match-all	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical AND function. A packet must match all statements to be accepted. If you do not specify the **match-all** or **match-any** keyword, the default keyword used is **match-all**.

match-any	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical OR function. A packet must match any of the match statements to be accepted. If you do not specify the **match-any** or **match-all** keyword, the default keyword is used **match-all**.
class-map-name	Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map. **Note** You can enter the value for the *class-map-name* argument within quotation marks. The software does not accept spaces in a class map name entered without quotation marks.

Command Default

A class map is not configured.

Command Modes

Global configuration (config)

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.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and implemented on Cisco 7600 series routers.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB and implemented on Cisco 7600 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)T	This command was modified. The **stack** and **access-control** keywords were added to support FPM. The **port-filter** and **queue-threshold** keywords were added to support control-plane protection.
12.4(6)T	This command was modified. The **logging** *log-class* keyword and argument pair was added to support control-plane packet logging.
12.2(18)ZY	This command was modified. The **stack** and **access-control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on Catalyst 6500 series switches equipped with the programmable intelligent services accelerator (PISA).
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor with the *class-map-name* argument as the only syntax element available.

Release	Modification
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor with the *class-map-name* argument.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
15.2(3)T	This command was modified. The software does not accept spaces in a class map name entered without quotation marks.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

Only the *class-map-name* argument is available.

Cisco 2600, 3660, 3845, 6500, 7200, 7401, 7500, and ASR 1000 Series Routers

Use the **class-map** command to specify the class that you will create or modify to meet the class-map match criteria. This command enters QoS class-map configuration mode in which you can enter one or more **match** commands to configure the match criteria for this class. Packets that arrive at either the input interface or the output interface (determined by how the **service-policy** command is configured) are checked against the match criteria that are configured for a class map to determine if packets belong to that class.

When configuring a class map, you can use one or more **match** commands to specify the match criteria. For example, you can use the **match access-group** command, the **match protocol** command, or the **match input-interface** command. The **match** commands vary according to the Cisco software release. For more information about match criteria and **match** commands, see the "Modular Quality of Service Command-Line Interface (CLI) (MQC)" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Cisco 7600 Series Routers

Apply the **class-map** command and commands available in QoS class-map configuration mode on a per-interface basis to define packet classification, marking, aggregating, and flow policing as part of a globally named service policy.

You can attach a service policy to an EtherChannel. Do not attach a service policy to a port that is a member of an EtherChannel.

When a device is in QoS class-map configuration mode, the following configuration commands are available:

- **description**—Specifies the description for a class-map configuration.
- **exit**—Exits from QoS class-map configuration mode.
- **match**—Configures classification criteria.
- **no**—Removes a match statement from a class map.

The following commands appear in the CLI help but are not supported on LAN interfaces or WAN interfaces on Optical Service Modules (OSMs):

- **destination-address mac** *mac-address*
- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}

- **protocol** *link-type*
- **source-address mac** *mac-address*

OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Policy Feature Card (PFC) QoS does not support the following commands:

- **destination-address mac** *mac-address*
- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **qos-group** *group-value*
- **source-address mac** *mac-address*

If you enter these commands, PFC QoS does not detect unsupported keywords until you attach a policy map to an interface. When you try to attach the policy map to an interface, an error message is generated. For additional information, see the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide* and Cisco IOS command references.

After configuring the class-map name and the device you can enter the **match access-group** and **match ip dscp** commands in QoS class-map configuration mode. The syntax for these commands is as follows:

match [**access-group** {*acl-index* | *acl-name*} | **ip dscp** | **precedence**} *value*]

See the table below for a description of **match** command keywords.

Table 1: match command Syntax Description

Optional command	Description
access-group *acl-index* | *acl-name*	(Optional) Specifies the access list index or access list names. Valid access list index values are from 1 to 2699.
access-group *acl-name*	(Optional) Specifies the named access list.
ip dscp *value1 value2 ... value8*	(Optional) Specifies IP differentiated services code point (DSCP) values to match. Valid values are from 0 to 63. You can enter up to eight DSCP values separated by spaces.
ip precedence *value1 value2 ... value8*	(Optional) Specifies the IP precedence values to match. Valid values are from 0 to 7. You can enter up to eight precedence values separated by spaces.

Examples

The following example shows how to specify class101 as the name of a class and define a class map for this class. The class named class101 specifies policy for the traffic that matches ACL 101.

```
Device(config)# class-map class101
Device(config-cmap)# match access-group 101
Device(config-cmap)# end
```

The following example shows how to define FPM traffic classes for slammer and UDP packets. The match criteria defined within class maps are for slammer and UDP packets with an IP length that

does not exceed 404 (0x194) bytes, UDP port 1434 (0x59A), and pattern 0x4011010 at 224 bytes from the start of the IP header.

```
Device(config)# load protocol disk2:ip.phdf
Device(config)# load protocol disk2:udp.phdf
Device(config)# class-map type stack match-all ip-udp
Device(config-cmap)# description "match UDP over IP packets"
Device(config-cmap)# match field ip protocol eq 0x11 next udp
Device(config-cmap)#exit
Device(config)# class-map type access-control match-all slammer
Device(config-cmap)# description "match on slammer packets"
Device(config-cmap)# match field udp dest-port eq 0x59A
Device(config-cmap)# match field ip length eq 0x194
Device(config-cmap)# match start 13-start offset 224 size 4 eq 0x 4011010
Device(config-cmap)# end
```

The following example shows how to configure a port-filter policy to drop all traffic that is destined to closed or "nonlistened" ports except Simple Network Management Protocol (SNMP):

```
Device(config)# class-map type port-filter pf-class
Device(config-cmap)# match not port udp 123
Device(config-cmap)# match closed-ports
Device(config-cmap)# exit
Device(config)# policy-map type port-filter pf-policy
Device(config-pmap)# class pf-class
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

The following example shows how to configure a class map named ipp5 and enter a match statement for IP precedence 5:

```
Device(config)# class-map ipp5
Device(config-cmap)# match ip precedence 5
```

Setting Up a Class Map Inside an 802.1p Domain

The following example shows how to set up a class map and match traffic classes for the 802.1p domain with packet class of service (CoS) values:

```
Device> enable
Device# configure terminal
Device(config)# class-map cos1
Device(config-cmap)# match cos 0
Device(config-pmap-c)# end
```

Setting Up a Class Map Inside an MPLS Domain

The following example shows how to set up a class map and match traffic classes for the Multiprotocol Label Switching (MPLS) domain with packet experimental (EXP) values:

```
Device> enable
Device# configure terminal
Device(config)# class-map exp7
Device(config-cmap)# match mpls experimental topmost 2
Device(config-pmap-c)# end
```

Related Commands

Command	Description
description	Specifies the description for a class map or policy map configuration.
drop	Configures the traffic class to discard packets belonging to a specific class map.
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class before you configure its policy.
load protocol	Loads a PHDF onto a router.
match (**class-map**)	Configures the match criteria for a class map on the basis of port filter or protocol queue policies.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match ip dscp	Identifies one or more DSCP, AF, and CS value as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
protocol	Configures a timer and authentication method for a control interface.
qos-group	Associates a QoS group value for a class map.
service-policy	Attaches a policy map to an input interface or VC or to an output interface or VC to be used as the service policy for that interface or VC.
show class-map	Displays class map information.
show policy-map interface	Displays statistics and configurations of input and output policies that are attached to an interface.
source-address	Configures the source-address control on a port.

clear ip route vrf

To remove routes from the Virtual Private Network (VPN) routing and forwarding(VRF) table, use the **clear ip route vrf** command in user EXEC or privileged EXEC mode.

clear ip route vrf *vrf-name* {***** | *network* [*mask*]}

Syntax Description

vrf-name	Name of the VRF for the static route.
*****	Indicates all routes for a given VRF.
network	Destination to be removed, in dotted decimal format.
mask	(Optional) Mask for the specified network destination, in dotted decimal format.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
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

Use this command to clear routes from the routing table. Use the asterisk (*) to delete all routes from the forwarding table for a specified VRF, or enter the address and mask of a particular network to delete the route to that network.

Examples

The following command shows how to remove the route to the network 10.13.0.0 in the vpn1 routing table:

```
Router# clear ip route vrf vpn1 10.13.0.0
```

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.

clear ip rsvp hello bfd

To globally reset to zero the number of times that the Bidirectional Forwarding Detection (BFD) protocol was dropped on an interface or the number of times that a link was down, use the **clear ip rsvp hello bfd** command in user EXEC or privileged EXEC mode. To disable the resetting of those counters, use the **no** form of this command.

clear ip rsvp hello bfd {**lost-cnt** | **nbr-lost**}
no clear ip rsvp hello bfd {**lost-cnt** | **nbr-lost**}

Syntax Description

lost-cnt	Resets to zero the number of times that the BFD session was lost (dropped) on an interface.
nbr-lost	Resets to zero the number of times the BFD protocol detected that a link was down.

Command Default

The counters are not reset to zero.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

When you unconfigure BFD-triggered Fast Reroute, the BFD session is not torn down. Enter the **clear ip rsvp hello bfd** command to clear **show** command output for Multiprotocol Label Switching (MPLS) traffic engineering (TE) features that use the BFD protocol.

The **clear ip rsvp hello bfd** command globally resets to zero the LostCnt field in the **show ip rsvp hello bfd nbr summary** command and the **show ip rsvp hello bfd nbr** command. Those fields show the number of times that the BFD session was lost (dropped) on an interface.

The **clear ip rsvp hello bfd** command also resets to zero the Communication with neighbor lost field in the **show ip rsvp hello bfd nbr detail** command. That field shows the number of times the BFD protocol detected that a link was down.

Examples

The following example resets to zero the Communication with neighbor lost field in the **show ip rsvp hello bfd nbr detail** command that shows the number of times the BFD protocol detected that a link was down:

```
Router# clear ip rsvp hello bfd nbr-lost
```

Related Commands

Command	Description
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

clear ip rsvp hello instance counters

To clear (refresh) the values for hello instance counters, use the **cleariprsvphelloinstancecounters**command in privileged EXEC mode.

clear ip rsvp hello instance counters

Syntax Description

This command has no arguments or keywords.

Command Modes

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.
12.2(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(31)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

Following is sample output from the**showiprsvphelloinstancedetail** command and then the **cleariprsvphelloinstancecounters** command. Notice that the “Statistics” fields have been cleared to zero.

```
Router# show ip rsvp hello instance detail
Neighbor 10.0.0.2  Source  10.0.0.1
 State: UP      (for 2d18h)
 Type: PASSIVE  (responding to requests)
 I/F: Et1/1
 LSPs protecting: 0
 Refresh Interval (msec) (used when ACTIVE)
  Configured: 100
  Statistics: (from 2398195 samples)
   Min:      100
   Max:      132
   Average:  100
   Waverage: 100 (Weight = 0.8)
   Current:  100
 Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
 Counters:
 Communication with neighbor lost:
  Num times: 0
  Reasons:
   Missed acks:             0
   Bad Src_Inst received:   0
   Bad Dst_Inst received:   0
   I/F went down:           0
   Neighbor disabled Hello: 0
```

```
  Msgs Received:   2398194
   Sent:       2398195
   Suppressed: 0
Router# clear ip rsvp hello instance counters
Neighbor 10.0.0.2  Source  10.0.0.1
 State: UP      (for 2d18h)
 Type: PASSIVE  (responding to requests)
 I/F: Et1/1
 LSPs protecting: 0
 Refresh Interval (msec) (used when ACTIVE)
  Configured: 100
  Statistics:
   Min:        0
   Max:        0
   Average:    0
   Waverage:   0
   Current:    0
 Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
 Counters:
  Communication with neighbor lost:
  Num times: 0
  Reasons:
   Missed acks:             0
   Bad Src_Inst received:   0
   Bad Dst_Inst received:   0
   I/F went down:           0
   Neighbor disabled Hello: 0
  Msgs Received:   2398194
   Sent:       2398195
   Suppressed: 0
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables hello globally on a router.
ip rsvp signalling hello (interface)	Enables hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Enables hello statistics on a router.
show ip rsvp hello statistics	Displays how long hello packets have been in the hello input queue.

clear ip rsvp hello instance statistics

To clear hello statistics for an instance, use the **cleariprsvphelloinstancestatistics**command in privileged EXEC mode.

clear ip rsvp hello instance statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Hello statistics are not cleared for an instance.

Command Modes

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.
12.2(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(31)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

This example shows sample output from the **showiprsvphellostatistics** command and the values in those fields after you enter the **cleariprsvphelloinstancestatistics** command.

```
Router# show ip rsvp hello statistics
 Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
   Weighted Average:0 (weight = 0.8)
   Max:4
  Current length: 0 (max:500)
 Number of samples taken: 2398525

Router# clear ip rsvp hello instance statistics
Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
   Weighted Average:0 (weight = 0.8)
   Max:0
  Current length: 0 (max:500)
 Number of samples taken: 0
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables hello globally on a router.
ip rsvp signalling hello (interface)	Enables hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Enables hello statistics on a router.
show ip rsvp hello statistics	Displays how long hello packets have been in the hello input queue.

clear ip rsvp hello statistics

To clear hello statistics globally, use the **cleariprsvphellostatistics**command in privileged EXEC mode.

clear ip rsvp hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Hello statistics are not globally cleared.

Command Modes

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.
12.2(31)SB2s	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(31)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to remove all information about how long hello packets have been in the hello input queue.

Examples

Following is sample output from the **showiprsvphellostatistics** command and the **cleariprsvphellostatistics** command. Notice that the values in the "Packet arrival queue" fields have been cleared.

```
Router# show ip rsvp hello statistics
Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
   Weighted Average:0 (weight = 0.8)
   Max:4
  Current length: 0 (max:500)
Number of samples taken: 2398525
Router# clear ip rsvp hello statistics
Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
   Weighted Average:0 (weight = 0.8)
   Max:0
  Current length: 0 (max:500)
 Number of samples taken: 16
```

Related Commands

Command	Description
ip rsvp signalling hello statistics	Enables hello statistics on a router.
show ip rsvp hello statistics	Displays how long hello packets have been in the hello input queue.

clear ip rsvp msg-pacing

Note Effective with Cisco IOS Release 12.4(20)T, the **cleariprsvpmsg-pacing**command is not available in Cisco IOS software. This command was replaced by the**cleariprsvpsignallingrate-limit** command.

To clear the Resource Reservation Protocol (RSVP) message pacing output from the **showiprsvpneighbor** command, use the **cleariprsvpmsg-pacing** command in privileged EXEC mode.

clear ip rsvp msg-pacing

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)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.
12.2(13)T	This command was replaced by the**cleariprsvpsignallingrate-limit** command.
12.4(20)T	This command was removed.

Examples

The following example clears the RSVP message pacing output:

```
Router# clear ip rsvp msg-pacing
```

Related Commands

Command	Description
show ip rsvp counters	Displays the number of RSVP messages that were sent and received.
show ip rsvp neighbor	Displays the current RSVP neighbors and indicates whether the neighbor is using IP or UDP encapsulation for a specified interface or for all interfaces.

clear l2vpn atom fsm

To clear Layer 2 VPN (L2VPN) Any Transport over MPLS (AToM) finite state machine (FSM) counters, use the **clear l2vpn atom fsm** command in privileged EXEC mode.

clear l2vpn atom fsm {**event** | **state transition**}[{**dynamic** | **llrrp** | **static** | **status**}]

Syntax Description

event	Clears L2VPN AToM FSM event counters.
state transition	Clears L2VPN AToM FSM state transition counters.
dynamic	(Optional) Clears L2VPN AToM dynamic FSM counters.
llrrp	(Optional) Clears L2VPN AToM High Availability (HA) Liberal Label Retention (LLR) counters.
static	(Optional) Clears L2VPN AToM FSM static label counters.
status	(Optional) Clears L2VPN AToM FSM status counters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **clear mpls l2transport fsm** 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 clear L2VPN AToM FSM event counters.

```
Device# clear l2vpn atom fsm event

Device# show l2vpn atom fsm event
Event State event occurred in

        Idl  Prd  Lsb  Ldp  Lrd  Rrd  Riv  Eng  Avt  Est
        ================================================
Prov    6    -    -    -    -    -    -    -    -    -
Unprov  -    -    -    -    -    5    -    -    -    -
LocReady-    1    -    -    -    5    -    -    -    -
LocPres -    -    -    -    -    -    -    -    -    -
LocNRdy -    6    -    -    -    5    -    -    -    5
RemRdy  -    5    -    -    1    -    -    -    -    -
RemNRdy -    -    -    -    -    -    -    -    -    -
RemVld  -    -    -    -    -    -    -    6    -    -
RemInvld-    -    -    -    -    -    -    -    -    -
RemRls  -    -    -    -    -    -    -    -    -    -
LdpUp   -    -    1    -    -    5    -    -    -    -
LdpDown -    -    -    -    -    -    -    -    -    -
```

```
LdpEqUp -    -    -    -    -    -    -    -    -    -
LdpEqDn -    -    -    -    -    -    -    -    -    -
RemUpTmr-    -    -    -    -    -    -    -    -    -
DpDnTmr -    -    -    -    -    -    -    -    -    -
DpUp    -    -    -    -    -    -    -    -    6    12
DpNotRdy-    -    -    -    -    -    -    -    -    -
DpDown  -    -    -    -    -    -    -    -    -    -
DpReact -    -    -    -    -    -    -    -    -    -
DpActvte-    -    -    -    -    -    -    6    -    -
DpDeact -    -    -    -    -    -    -    -    -    -
LdpGrDn -    -    -    -    -    -    -    -    -    -
LdpGrDl -    -    -    -    -    -    -    -    -    -
NeedCpt -    -    -    -    -    -    -    -    -    -
RcvdCpt -    -    -    -    -    -    -    -    -    -
RRPtoRP -    -    -    -    -    -    -    -    -    -
FsmJump -    -    -    -    -    -    -    -    -    -
ActNRdy -    -    -    -    -    -    -    -    -    -
MacWdrw -    -    -    -    -    -    -    -    -    -
RLT     -    -    -    -    -    -    -    -    -    -
```

Related Commands

Command	Description
clear mpls l2transport fsm	Clears MPLS Layer 2 transport FSM counters.

clear l2vpn service

To clear Layer 2 VPN (L2VPN) service configurations, use the **clear l2vpn service** command in privileged EXEC mode.

clear l2vpn service [{**vfi** | **xconnect**}] {**all** | **interface** *interface-type-number* | **name** *service-name* | **peer** *ip-address* {**all** | **vcid** *vc-id*}}

Syntax Description

vfi	(Optional) Clears all Virtual Private LAN Services (VPLS)
xconnect	(Optional) Clears all Virtual Private Wired Services (VPWS).
all	Clears all L2VPN services.
interface *interface-type-number*	Clears L2VPN services on the specified interface.
name *service-name*	Clears a specific L2VPN service.
peer *ip-address* {**all** | **vcid** *vc-id*}	Clears L2VPN services associated with the specified peer IP address. • **all**—Clears all L2VPN services associated with the specified peer IP address. • **vcid** *vc-id*—Clears L2VPN services associated with the specified peer IP address and the specified virtual circuit (VC) ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **clear xconnect** 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 clear all L2VPN services:

```
Device# clear l2vpn service all
Reprovision all xconnects? [confirm]

Device# show l2vpn service all
Legend: St=State    XC St=State in the L2VPN Service      Prio=Priority
        UP=Up       DN=Down             AD=Admin Down     IA=Inactive
        SB=Standby  HS=Hot Standby      RV=Recovering     NH=No Hardware
        m=manually selected

  Interface          Group       Encapsulation                  Prio  St  XC St
  ---------          -----       -------------                  ----  --  -----
VPWS name: Gi1/1/1-1001, State: UP
```

```
  Gi1/1/1            left        Gi1/1/1:1001(Gi VLAN)          0     UP  UP
  pw100001           right       2.1.1.2:1234000(MPLS)           0     UP  UP

Device# show logging
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes, 0 overruns,
 xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging:  level debugging, 277 messages logged, xml disabled, filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
Trap logging: level informational, 90 message lines logged
Logging Source-Interface:       VRF Name:

Log Buffer (1000000 bytes):

*Aug 10 18:53:36.042: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state ADMIN
 DOWN
*Aug 10 18:53:36.042: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state DOWN

*Aug 10 18:53:36.043: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state DOWN,
 PW Err
*Aug 10 18:53:36.044: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state ADMIN
 DOWN
*Aug 10 18:53:36.044: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state DOWN

*Aug 10 18:53:36.047: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state UP
```

The following example shows how to clear all L2VPN services associated with peer router 10.1.1.2:

```
Device# clear l2vpn service peer 10.1.1.2 all

Device# show logging
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes, 0 overruns,
 xml disabled, filtering disabled)

No Active Message Discriminator.
No Inactive Message Discriminator.

Console logging: disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging:  level debugging, 289 messages logged, xml disabled, filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
Trap logging: level informational, 102 message lines logged
Logging Source-Interface:       VRF Name:

Log Buffer (1000000 bytes):

*Aug 10 18:56:40.803: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state ADMIN
 DOWN
*Aug 10 18:56:40.803: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state DOWN

*Aug 10 18:56:40.804: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state DOWN,
 PW Err
*Aug 10 18:56:40.804: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state ADMIN
```

```
 DOWN
*Aug 10 18:56:40.805: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state DOWN

*Aug 10 18:56:40.806: %XCONNECT-5-PW_STATUS: MPLS peer 2.1.1.2 vcid 1234000, VC state UP
```

The following example shows how to clear the L2VPN services associated with peer router 10.1.1.2 and VC ID 1234001:

```
Device# clear l2vpn service peer 10.1.1.2 vcid 1234001

Device# show logging
02:14:23: Xconnect[ac:Gi1/1/1(Gi VLAN)]: provisioning fwder with fwd_type=1, sss_role=1
02:14:23: Xconnect[mpls:10.1.1.2:1234001]: provisioning fwder with fwd_type=2, sss_role=2
02:14:23: MPLS peer 10.1.1.2 vcid 1234001, VC DOWN, VC state DOWN
02:14:23: XC AUTH [Gi1/1/1, 1002]: Event: start xconnect authorization, state changed from
 IDLE to AUTHORIZING
02:14:23: XC AUTH [Gi1/1/1, 1002]: Event: found xconnect authorization, state changed from
 AUTHORIZING to DONE
02:14:23: XC AUTH [Gi1/1/1, 1002]: Event: free xconnect authorization request, state changed
 from DONE to END
02:14:23: MPLS peer 10.1.1.2 vcid 1234001, VC UP, VC state UP
```

The following example shows how to clear the L2VPN services associated with Gigabit Ethernet interface 1/0/0:

```
Device# clear l2vpn service interface gigabitethernet 1/1/1

Device# show logging
02:14:48: Xconnect[ac:Gi1/1/1(Gi VLAN)]: provisioning fwder with fwd_type=1, sss_role=2
02:14:48: Xconnect[mpls:10.1.1.2:1234000]: provisioning fwder with fwd_type=2, sss_role=1
02:14:48: MPLS peer 10.1.1.2 vcid 1234000, VC DOWN, VC state DOWN
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: start xconnect authorization, state changed
from IDLE to AUTHORIZING
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: found xconnect authorization, state changed
from AUTHORIZING to DONE
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: free xconnect authorization request, state
changed from DONE to END
02:14:48: MPLS peer 10.1.1.2 vcid 1234000, VC UP, VC state UP
```

Related Commands

Command	Description
clear xconnect	Clears xconnect attachment circuits and pseudowires.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

clear mpls counters

To clear the Multiprotocol Label Switching (MPLS) forwarding table disposition counters, the Any Transport over MPLS (AToM) imposition and disposition virtual circuit (VC) counters, and the MAC address withdrawal counters, use the **clear mpls counters** command in privileged EXEC mode.

clear mpls counters

Syntax Description

This command has no arguments or keywords.

Command Default

Checkpoint information resides on the active and standby Route Processor.

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. This command was updated to clear AToM VC counters.
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)SRE	This command was modified. This command now clears the MAC address withdrawal counters.
Cisco IOS XE Release 2.5	This command was modified. This command now clears the MAC address withdrawal counters.

Examples

In the following example, the first **show mpls forwarding-table** command shows that 590 label-switched bytes exist in the forwarding table. The **clear mpls counters** command clears the counters. The second **show mpls forwarding-table** command shows that the number of label-switched bytes is 0.

```
Router# show mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
20     30            10.10.17.17      590           Et3/0      172.16.0.2
Router# clear mpls counters
Clear "show mpls forwarding-table" counters [confirm]
mpls forward counters cleared
Router# show mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
20     30            10.10.17.17      0             Et3/0       172.16.0.2
```

In the following example, the first **show mpls l2transport vc detail** command shows that one MAC address withdrawal message was sent (and none were received), 15 packets were received and sent,

1656 bytes were received, and 1986 bytes were sent. The **clear mpls counters** command clears the counters. The second **show mpls l2transport vc detail** command shows that no MAC address withdrawal messages, bytes, or packets were received or sent. (If there are no MAC address withdrawal messages received or sent, the MAC Withdraw field is absent.)

```
Router# show mpls l2transport vc detail

Local interface: Et1/0 up, line protocol up, Ethernet up
  Destination address: 12.1.1.1, VC ID: 99, VC status: up
    Output interface: Se2/0, imposed label stack {21 16}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:00:32, last status change time: 00:00:14
  Signaling protocol: LDP, peer 12.1.1.1:0 up
    Targeted Hello: 11.1.1.1(LDP Id) -> 12.1.1.1
    Status TLV support (local/remote)   : enabled/supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: no fault
    MPLS VC labels: local 23, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
    MAC Withdraw: sent:1, received:0 <---- MAC address withdrawal totals
  Sequencing: receive disabled, send disabled
  SSO Descriptor: 12.1.1.1/99, local label: 23
    SSM segment/switch IDs: 16387/8193 (used), PWID: 8193
  VC statistics:
    packet totals: receive 15, send 15 <---- packet totals
    byte totals:   receive 1656, send 1986 <---- byte totals
    packet drops:  receive 0, seq error 0, send 0
Router# clear mpls counters

Clear "show mpls forwarding-table" counters [confirm]
mpls forward counters cleared

Router# show mpls l2transport vc detail
Local interface: Et1/0 up, line protocol up, Ethernet up
  Destination address: 12.1.1.1, VC ID: 99, VC status: up
    Output interface: Se2/0, imposed label stack {21 16}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:00:32, last status change time: 00:00:14
  Signaling protocol: LDP, peer 12.1.1.1:0 up
    Targeted Hello: 11.1.1.1(LDP Id) -> 12.1.1.1
    Status TLV support (local/remote)   : enabled/supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: no fault
    MPLS VC labels: local 23, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
```

```
SSO Descriptor: 12.1.1.1/99, local label: 23
  SSM segment/switch IDs: 16387/8193 (used), PWID: 8193
VC statistics:
  packet totals: receive 0, send 0 <---- packet totals
  byte totals:   receive 0, send 0 <---- byte totals
  packet drops:  receive 0, seq error 0, send 0
```

Related Commands

Command	Description
show mpls forwarding-table	Displays the contents of the MPLS FIB.
show mpls l2transport vc detail	Displays detailed information related to a VC.

clear mpls ip iprm counters

To clear the IP Rewrite Manager (IPRM) counters, use the **clear mpls ip iprm counters** command in privileged EXEC mode.

clear mpls ip iprm counters

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command sets IPRM counters to zero.

Examples

The command in the following example clears the IPRM counters:

```
Router# clear mpls ip iprm counters
Clear iprm counters [confirm]
```

Related Commands

Command	Description
show mpls ip iprm counters	Displays the IPRM counters.

clear mpls ldp checkpoint

To clear the checkpoint information from the Label Information Base (LIB) entries on the active Route Processor (RP) or PRE and to clear the LIB entries created by checkpointing on the standby RP or PRE, use the **clear mpls ldp checkpoint** command in privileged EXEC mode.

clear mpls ldp checkpoint [**vrf** *vpn-name*] {**network** {*masklength*} [**longer-prefixes**] | *****} [**incomplete**]

Cisco 10000 Series Routers
clear mpls ldp checkpoint {**network** {*masklength*} [**longer-prefixes**] | *****} [**incomplete**]

Syntax Description

vrf *vpn-name*	(Optional) Clears the checkpoint information for the specified VPN routing and forwarding (VRF) instance (vpn-name). **Note** Applies to the Cisco 7000 series routers only.
network	Clears the checkpoint information for the specified destination address.
mask	Specifies the network mask, written as A.B.C.D.
length	Specifies the mask length.
longer-prefixes	(Optional) Clears the checkpoint information for any prefix that matches *mask* with the *length* specified.
*****	(Optional) Clears the checkpoint information for all destinations.
incomplete	(Optional) Clears any incomplete checkpoint information from the LIB.

Command Default

Checkpoint information resides on the active and standby RP.

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.

Usage Guidelines

Use this command only when Cisco support personnel recommend it as a means of rectifying a problem.

On the active RP or PRE, this command does the following:

- Clears the checkpoint state information from the specified LIB entries.
- Triggers a checkpoint attempt for those entries.

On the standby RP or PRE, this command deletes all of the LIB entries created by checkpointing.

Examples

The command in the following example clears the checkpointing information for prefix 10.1.10.1:

```
Router(config)# clear mpls ldp checkpoint 10.1.10.1 32
Clear LDP bindings checkpoint state [confirm]
00:20:29: %LDP-5-CLEAR_CHKPT: Clear LDP bindings checkpoint state (*) by console
```

Related Commands

Command	Description
show mpls ldp checkpoint	Displays information about the LDP checkpoint system on the active RP.

clear mpls ldp neighbor

To forcibly reset a label distribution protocol (LDP) session, use the **clear mpls ldp neighbor** command in privileged EXEC mode.

clear mpls ldp neighbor [**vrf** *vpn-name*] {*nbr-address* | *****}

Syntax Description

vrf *vpn-name*	(Optional) Specifies the VPN routing and forwarding instance (*vpn-name*) for resetting an LDP session.
nbr-address	Specifies the address of the LDP neighbor whose session will be reset. The neighbor address is treated as <nbr-address>:0, which means it pertains to the LDP session for the LSR's platform-wide label space.
*****	Designates that all LDP sessions will be reset.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **clear mpls ldp neighbor** command terminates the specified LDP sessions. The LDP sessions should be reestablished if the LDP configuration remains unchanged.

You can clear an LDP session for an interface-specific label space of an LSR by issuing the no mpls ip command and then the mpls ip command on the interface associated with the LDP session.

Examples

The following example resets an LDP session:

```
Router# clear mpls ldp neighbor 10.12.12.12
```

To verify the results of the **clear mpls ldp neighbor** command, enter the **show mpls ldp neighbor** command. Notice the value in the "Up time" field.

```
Router# show mpls ldp neighbor 10.12.12.12

 Peer LDP Ident: 10.12.12.12:0; Local LDP Ident 10.13.13.13:0
   TCP connection: 10.12.12.12.646 - 10.13.13.13.15093
```

```
   State: Oper; Msgs sent/rcvd: 142/138; Downstream
   Up time: 02:16:28
   LDP discovery sources:
    Serial1/0, Src IP addr: 10.0.0.2
   Addresses bound to peer LDP Ident:
    10.0.0.129       10.12.12.12     10.0.0.2        10.1.0.5
    10.7.0.1
```

Then enter the following **clear mpls ldp neighbor 12.12.12.12** command. With mpls ldp logging configured, the easiest way to verify the **clear mpls ldp neighbor** command is to monitor the LDP log messages.

```
Router# clear mpls ldp neighbor 10.12.12.12
1w1d: %LDP-5-CLEAR_NBRS: Clear LDP neighbors (10.12.12.12) by console
1w1d: %LDP-5-NBRCHG: LDP Neighbor 10.12.12.12:0 is DOWN
1w1d: %LDP-5-NBRCHG: LDP Neighbor 10.12.12.12:0 is UP
```

Reenter the **show mpls ldp neighbor 10.12.12.12** command. Notice that the "Up time" value has been reset.

```
Router# show mpls ldp neighbor 10.12.12.12
  Peer LDP Ident: 10.12.12.12:0; Local LDP Ident 10.13.13.13:0
    TCP connection: 10.12.12.12.646 - 10.13.13.13.15095
    State: Oper; Msgs sent/rcvd: 125/121; Downstream
    Up time: 00:00:05
    LDP discovery sources:
     Serial1/0, Src IP addr: 10.0.0.2
    Addresses bound to peer LDP Ident:
     10.0.0.129       10.12.12.12     10.0.0.2        10.1.0.5
     10.7.0.1
```

The following example resets all LDP sessions:

```
Router# clear mpls ldp neighbor *
```

Related Commands

Command	Description
show mpls ldp neighbor	Displays the status of the LDP sessions.

clear mpls traffic-eng auto-bw timers

To reinitialize the automatic bandwidth adjustment feature on a platform, use the **clear mpls traffic-eng auto-bw timers** command in user EXEC mode.

clear mpls traffic-eng auto-bw timers

Syntax Description

This command has no arguments or keywords.

Command Default

There are no defaults for this command.

Command Modes

User EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)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.

Usage Guidelines

For each tunnel for which automatic bandwidth adjustment is enabled, the platform maintains information about sampled output rates and the time remaining until the next bandwidth adjustment. The **clear mpls traffic-eng auto-bw timers** command clears this information for all such tunnels. The effect is as if automatic bandwidth adjustment had just been enabled for the tunnels.

Examples

The following example shows how to clear information about sampled output rates and the time remaining until the next bandwidth adjustment:

```
Router# clear mpls traffic-eng auto-bw timers

Clear mpls traffic engineering auto-bw timers [confirm]
```

Related Commands

Command	Description
mpls traffic-eng auto-bw timers	Enables automatic bandwidth adjustment on a platform for tunnels configured for bandwidth adjustment.
tunnel mpls traffic-eng auto-bw timers	Enables automatic bandwidth adjustment for a tunnel, specifies the frequency with which tunnel bandwidth can be automatically adjusted, and designates the allowable range of bandwidth adjustments.

clear mpls traffic-eng auto-tunnel mesh tunnel

To remove an autotunnel mesh interface and then re-create it, use the **clear mpls traffic-eng auto-tunnel mesh tunnel** command in privileged EXEC mode.

clear mpls traffic-eng auto-tunnel mesh tunnel *tunnel-interface-number*

Syntax Description

tunnel-interface-number	Tunnel interface to be removed. The range is 0 to 65535.

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.
15.2(2)S	This command was modified. For details, see the "Usage Guidelines" section.
Cisco IOS XE Release 3.6S	This command was modified. For details, see the "Usage Guidelines" section.

Usage Guidelines

The software no longer supports using the **clear mpls traffic-eng auto-tunnel mesh** command to remove all autotunnel mesh interfaces. Use the **no mpls traffic-eng auto-tunnel mesh** global configuration command to remove all autotunnel mesh interfaces, or use the **clear mpls traffic-eng auto-tunnel mesh tunnel** *tunnel-interface-number* command to remove and re-create a particular tunnel interface.

Examples

The following example shows how to remove an autotunnel mesh interface and then re-create it:

```
Router# clear mpls traffic-eng auto-tunnel mesh tunnel 2000
```

Related Commands

Command	Description
interface auto-template	Creates the template interface.
no mpls traffic-eng auto-tunnel mesh	Enables autotunnel mesh groups globally.

clear mpls traffic-eng auto-tunnel backup tunnel

To remove an autotunnel backup interface and then re-create it, use the **clear mpls traffic-eng auto-tunnel backup tunnel** command in privileged EXEC mode.

clear mpls traffic-eng auto-tunnel backup tunnel *tunnel-interface-number*

Syntax Description

tunnel-interface-number	Tunnel interface to be removed. The range is 0 to 65535.

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.
15.2(2)S	This command was modified. For details, see the "Usage Guidelines" section.
Cisco IOS XE Release 3.6S	This command was modified. For details, see the "Usage Guidelines" section.

Usage Guidelines

The software no longer supports using the **clear mpls traffic-eng auto-tunnel backup** command to remove all autotunnel backup interfaces. Use the **no mpls traffic-eng auto-tunnel backup** global configuration command to remove all autotunnel backup interfaces, or use the **clear mpls traffic-eng auto-tunnel backup tunnel** *tunnel-interface-number* command to remove and re-create a particular tunnel interface.

Examples

The following example shows how to remove an autotunnel backup interface and then re-create it:

```
Router# clear mpls traffic-eng auto-tunnel backup tunnel 2000
```

Related Commands

Command	Description
no mpls traffic-eng auto-tunnel backup	Automatically builds next-hop (NHOP) and next-next hop (NNHOP) backup tunnels.
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

clear mpls traffic-eng auto-tunnel primary tunnel

To remove an autotunnel primary one-hop interface and then re-create it, use the **clear mpls traffic-eng auto-tunnel primary tunnel** command in privileged EXEC mode.

clear mpls traffic-eng auto-tunnel primary tunnel *tunnel-interface-number*

Syntax Description

tunnel-interface-number	Tunnel interface to be removed. The range is 0 to 65535.

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.
15.2(2)S	This command was modified. For details, see the "Usage Guidelines" section.
Cisco IOS XE Release 3.6S	This command was modified. For details, see the "Usage Guidelines" section.

Usage Guidelines

The software no longer supports using the **clear mpls traffic-eng auto-tunnel primary** command to remove all autotunnel primary interfaces. Use the **no mpls traffic-eng auto-tunnel primary onehop** global configuration command to remove all autotunnel primary interfaces, or use the **clear mpls traffic-eng auto-tunnel primary tunnel** *tunnel-interface-number* command to remove and re-create a particular tunnel interface.

Examples

The following example shows how to remove an autotunnel primary one-hop interface and then re-create it:

```
Router# clear mpls traffic-eng auto-tunnel primary tunnel 2000
```

Related Commands

Command	Description
no mpls traffic-eng auto-tunnel primary onehop	Automatically creates primary tunnels to all next hops.
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

clear mpls traffic-eng tunnel counters

To clear the counters for all Multiprotocol Label Switching (MPLS) traffic engineering tunnels, use the **clear mpls traffic-eng tunnel counters** command in privileged EXEC mode.

clear mpls traffic-eng tunnel counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)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.

Usage Guidelines

This command allows you to set the MPLS traffic engineering tunnel counters to zero so that you can see changes to the counters easily.

Examples

In the following example, the counters for all MPLS traffic engineering tunnels are cleared and a request is made for confirmation that the specified action occurred:

```
Router# clear mpls traffic-eng tunnel counters

Clear traffic engineering tunnel counters [confirm]
```

Related Commands

Command	Description
show mpls traffic-eng tunnels statistics	Displays event counters for one or more MPLS traffic engineering tunnels.

clear pw-udp vc

To clear pseudowire User Datagram Protocol (UDP) virtual circuit (VC) counter values, use the **clear pw-udp vc** command in privileged EXEC mode.

clear pw-udp vc {*min-vc max-vc* | **destination** *address* **vcid** *min-vc max-vc* | **vcid** *min-vc max-vc*} **counters**

Syntax Description

min-vc	Minimum VC ID. The range is 1 to 4294967295.
max-vc	Maximum VC ID. The range is 1 to 4294967295.
destination *address*	Specifies the destination hostname or the IP address of the VC.
vcid	Specifies the VC ID range.
counters	Specifies forwarding counters of pseudowire over UDP.

Command Default

The pseudowire UDP VC counter values are not cleared.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to clear the pseudowire UDP VC counter values:

```
Router# clear pw-udp vc destination 10.1.1.1 counters
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
show pw-udp vc	Displays information about pseudowire UDP VCs.
udp port	Configures the UDP port information on the xconnect class.

clear xconnect

To remove xconnect attachment circuits and pseudowires, use the **clear xconnect** command in privileged EXEC mode.

clear xconnect {**all** | **interface** *interface* | **peer** *ip-address* {**all** | **vcid** *vc-id*}}

Syntax Description

all	Removes all xconnect attachment circuits and pseudowires.
interface *interface*	Removes xconnect attachment circuits and pseudowires on the specified interface.
peer *ip-address* {**all** | **vcid** *vc-id*}	For Virtual Private Wire Service (VPWS), the keyword resets pseudowires associated with the specified peer IP address. For Virtual Private LAN Service (VPLS), the keyword resets all pseudowires in each virtual forwarding instance (VFI) that have a pseudowire to the specified peer IP address. • **all** --Removes all xconnects associated with the specified peer IP address. • **vcid** *vc-id*--Removes xconnects associated with the specified peer IP address and the specified VCID. **Note** In a VPLS scenario, resetting pseudowires causes route flapping on all pseudowires in each VFI that have a pseudowire to the specified peer IP address.

Command Default

xconnect attachment circuits and pseudowires are not removed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **clear xconnect** command is intended to be used with caution in a critical situation when one or more virtual circuits (VCs) are disabled and there are no other methods for recovering them. Using this command may impact xconnect services such as VPWS, VPLS, and local switching.

Note Using the **clear xconnect** command does not guarantee that any VC recovers.

Examples

The following example shows how to remove all xconnect attachment circuits and pseudowires:

```
Router# clear xconnect all
02:13:56: Xconnect[ac:Et1/0.1(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=1
02:13:56: Xconnect[mpls:10.1.1.2:1234000]: provisioning fwder with fwd_type=2, sss_role=2
02:13:56: Xconnect[ac:Et1/0.2(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=2
02:13:56: Xconnect[mpls:10.1.1.2:1234001]: provisioning fwder with fwd_type=2, sss_role=1
02:13:56: Xconnect[ac:Et1/0.3(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=1
02:13:56: Xconnect[mpls:10.1.2.2:1234002]: provisioning fwder with fwd_type=2, sss_role=2
02:13:56: Xconnect[ac:Et1/0.4(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=2
02:13:56: Xconnect[mpls:10.1.2.2:1234003]: provisioning fwder with fwd_type=2, sss_role=1
02:13:56: MPLS peer 10.1.1.2 vcid 1234000, VC DOWN, VC state DOWN
02:13:56: MPLS peer 10.1.1.2 vcid 1234001, VC DOWN, VC state DOWN
02:13:56: MPLS peer 10.1.2.2 vcid 1234002, VC DOWN, VC state DOWN
02:13:56: MPLS peer 10.1.2.2 vcid 1234003, VC DOWN, VC state DOWN
02:13:56: XC AUTH [Et1/0.1, 1001]: Event: start xconnect authorization, state changed from
 IDLE to AUTHORIZING
02:13:56: XC AUTH [Et1/0.1, 1001]: Event: found xconnect authorization, state changed from
 AUTHORIZING to DONE
02:13:56: XC AUTH [Et1/0.3, 1003]: Event: start xconnect authorization, state changed from
 IDLE to AUTHORIZING
02:13:56: XC AUTH [Et1/0.3, 1003]: Event: found xconnect authorization, state changed from
 AUTHORIZING to DONE
02:13:56: XC AUTH [10.1.1.2, 1234001]: Event: start xconnect authorization, state changed
from IDLE to AUTHORIZING
02:13:56: XC AUTH [10.1.1.2, 1234001]: Event: found xconnect authorization, state changed
from AUTHORIZING to DONE
02:13:56: XC AUTH [10.1.2.2, 1234003]: Event: start xconnect authorization, state changed
from IDLE to AUTHORIZING
02:13:56: XC AUTH [10.1.2.2, 1234003]: Event: found xconnect authorization, state changed
from AUTHORIZING to DONE
02:13:56: XC AUTH [Et1/0.1, 1001]: Event: free xconnect authorization request, state changed
 from DONE to END
02:13:56: XC AUTH [Et1/0.3, 1003]: Event: free xconnect authorization request, state changed
 from DONE to END
02:13:56: XC AUTH [10.1.1.2, 1234001]: Event: free xconnect authorization request, state
changed from DONE to END
02:13:56: XC AUTH [10.1.2.2, 1234003]: Event: free xconnect authorization request, state
changed from DONE to END
02:13:56: MPLS peer 10.1.1.2 vcid 1234001, VC UP, VC state UP
02:13:56: MPLS peer 10.1.2.2 vcid 1234003, VC UP, VC state UP
02:13:56: MPLS peer 10.1.1.2 vcid 1234000, VC UP, VC state UP
02:13:56: MPLS peer 10.1.2.2 vcid 1234002, VC UP, VC state UP
```

The following example shows how to remove all the xconnects associated with peer router 10.1.1.2:

```
Router# clear xconnect peer 10.1.1.2 all
02:14:08: Xconnect[ac:Et1/0.1(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=1
02:14:08: Xconnect[mpls:10.1.1.2:1234000]: provisioning fwder with fwd_type=2, sss_role=2
02:14:08: Xconnect[ac:Et1/0.2(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=2
02:14:08: Xconnect[mpls:10.1.1.2:1234001]: provisioning fwder with fwd_type=2, sss_role=1
02:14:08: MPLS peer 10.1.1.2 vcid 1234000, VC DOWN, VC state DOWN
02:14:08: MPLS peer 10.1.1.2 vcid 1234001, VC DOWN, VC state DOWN
02:14:08: XC AUTH [Et1/0.1, 1001]: Event: start xconnect authorization, state changed from
 IDLE to AUTHORIZING
02:14:08: XC AUTH [Et1/0.1, 1001]: Event: found xconnect authorization, state changed from
 AUTHORIZING to DONE
02:14:08: XC AUTH [10.1.1.2, 1234001]: Event: start xconnect authorization, state changed
from IDLE to AUTHORIZING
02:14:08: XC AUTH [10.1.1.2, 1234001]: Event: found xconnect authorization, state changed
from AUTHORIZING to DONE
02:14:08: XC AUTH [Et1/0.1, 1001]: Event: free xconnect authorization request, state changed
 from DONE to END
02:14:08: XC AUTH [10.1.1.2, 1234001]: Event: free xconnect authorization request, state
changed from DONE to END
```

```
02:14:08: MPLS peer 10.1.1.2 vcid 1234001, VC UP, VC state UP
02:14:08: MPLS peer 10.1.1.2 vcid 1234000, VC UP, VC state UP
```

The following example shows how to remove the xconnects associated with peer router 10.1.1.2 and VC ID 1234001:

```
Router# clear xconnect peer 10.1.1.2 vcid 1234001
02:14:23: Xconnect[ac:Et1/0.2(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=1
02:14:23: Xconnect[mpls:10.1.1.2:1234001]: provisioning fwder with fwd_type=2, sss_role=2
02:14:23: MPLS peer 10.1.1.2 vcid 1234001, VC DOWN, VC state DOWN
02:14:23: XC AUTH [Et1/0.2, 1002]: Event: start xconnect authorization, state changed from
 IDLE to AUTHORIZING
02:14:23: XC AUTH [Et1/0.2, 1002]: Event: found xconnect authorization, state changed from
 AUTHORIZING to DONE
02:14:23: XC AUTH [Et1/0.2, 1002]: Event: free xconnect authorization request, state changed
 from DONE to END
02:14:23: MPLS peer 10.1.1.2 vcid 1234001, VC UP, VC state UP
```

The following example shows how to remove the xconnects associated with Ethernet interface 1/0.1:

```
Router# clear xconnect interface eth1/0.1

02:14:48: Xconnect[ac:Et1/0.1(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=2
02:14:48: Xconnect[mpls:10.1.1.2:1234000]: provisioning fwder with fwd_type=2, sss_role=1
02:14:48: MPLS peer 10.1.1.2 vcid 1234000, VC DOWN, VC state DOWN
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: start xconnect authorization, state changed
from IDLE to AUTHORIZING
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: found xconnect authorization, state changed
from AUTHORIZING to DONE
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: free xconnect authorization request, state
changed from DONE to END
02:14:48: MPLS peer 10.1.1.2 vcid 1234000, VC UP, VC state UP
```

Related Commands

Command	Description
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

connect (Frame Relay)

To define connections between Frame Relay permanent virtual circuits (PVCs), use the **connect** command in global configuration mode. To remove connections, use the **no** form of this command.

connect *connection-name interface dlci* {*I* **interface dlci** | **l2transport**}
no connect *connection-name interface dlci* {**interface dlci** | **l2transport**}

Syntax Description

connection-name	A name for this connection.
interface	Interface on which a PVC connection will be defined.
dlci	Data-link connection identifier (DLCI) number of the PVC that will be connected.
l2transport	Specifies that the PVC will not be a locally switched PVC, but will be tunneled over the backbone network.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.0(23)S	The l2transport keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
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

When Frame Relay switching is enabled, the **connect** command creates switched PVCs in Frame Relay networks.

Examples

The following example shows how to define a connection called *frompls1* with DLCI 100 on serial interface 5/0.

```
connect frompls1 Serial5/0 100 l2transport
```

The following example shows how to enable Frame Relay switching and define a connection called *one* between DLCI 16 on serial interface 0 and DLCI 100 on serial interface 1.

```
frame-relay switching
connect one serial0 16 serial1 100
```

Related Commands

Command	Description
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.
mpls l2transport route	Enables routing of Frame Relay packets over a specified VC.

connect (L2VPN local switching)

To create Layer 2 data connections between two ports on the same router, use the **connect** command in global configuration mode. To remove such connections, use the **no** form of this command.

Syntax for 12.0S, 12.2S and 12.4T Releases
connect *connection-name type number circuit-id* [{*dlcipvcpvp*}] *type number circuit-id* [{*dlcipvcpvp*}] [{**interworking ip** | **ethernet**}]
no connect *connection-name type number circuit-id* [{*dlcipvcpvp*}] *type number circuit-id* [{*dlcipvcpvp*}] [{**interworking ip** | **ethernet**}]

Syntax for Cisco IOS XE Release 2.5 and Later Releases
connect *connection-name type number type number*
no connect *connection-name type number type number*

Syntax Description

connection-name	A name for this local switching connection.
type	String that identifies the type of interface used to create a local switching connection; for example, serial or Gigabit Ethernet.
number	Integer that identifies the number of the interface; for example, 0/0/0.1 for a Gigabit Ethernet interface.
circuit-id	CEM group ID. This option is used for CEM circuits only.
dlci	(Optional) The data-link connection identifier (DLCI) assigned to the interface.
pvc	(Optional) The permanent virtual circuit (PVC) assigned to the interface, expressed by its vpi/vci (virtual path and virtual channel identifiers).
pvp	(Optional) The permanent virtual path (PVP) assigned to the interface.
interworking ip	(Optional) Specifies that this local connection enables different transport types to be switched locally and causes IP packets to be extracted from the attachment circuit and sent over the pseudowire. Attachment circuit frames that do not contain IPv4 packets are dropped. **Note** This keyword is not necessary for configurations that locally switch the same transport type, such as ATM to ATM, or Frame Relay to Frame Relay.
ethernet	(Optional) Specifies that this local connection enables different transport types to be switched locally and causes Ethernet frames to be extracted from the attachment circuit and sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that do not contain Ethernet frames are dropped. In the case of VLAN, the VLAN tag is removed, leaving a pure Ethernet frame. **Note** This keyword is not necessary for configurations that locally switch the same transport type, such as ATM to ATM, or Frame Relay to Frame Relay.

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(27)S	This command was introduced for local switching.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
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 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.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(1)S	This command was modified. The *circuit-id* argument was added.

Examples

The following example shows an Ethernet interface configured for Ethernet, plus an ATM interface configured for AAL5 Subnetwork Access Protocol (SNAP) encapsulation. The **connect** command allows local switching between these two interfaces and specifies the interworking type as IP mode.

```
Router(config)# interface atm 0/0/0
Router(config-if)# pvc 0/100 l2transport
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal5snap
Router(config)# interface fastethernet 6/0/0.1
Router(config-subif)# encapsulation dot1q 100
Router(config)# connect atm-eth-con atm 0/0/0 0/100 fastethernet 6/0/0.1 interworking ip
```

Related Commands

Command	Description
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.

context

Note Effective with Cisco IOS Release 15.0(1)M, the **context** command is replaced by the **snmp context** command. See the **snmp context** command for more information.

To associate a Simple Network Management Protocol (SNMP) context with a particular VPN routing and forwarding (VRF) instance, use the **context** command in VRF configuration mode. To disassociate an SNMP context from a VPN, use the **no** form of this command.

context *context-name*
no context

Syntax Description

context-name	Name of the SNMP VPN context. The name can be up to 32 alphanumeric characters.

Command Default

No SNMP contexts are associated with VPNs.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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)SRB	This command was modified. Support for IPv6 was added.
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)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.0(1)M	This command was replaced by the **snmp context** command.

Usage Guidelines

Before you use the **context** command to associate an SNMP context with a VPN, you must do the following:

- Issue the **snmp-server context** command to create an SNMP context.
- Associate a VPN with a context so that the specific MIB data for that VPN exists in the context.
- Associate a VPN group with the context of the VPN using the **context** *context-name* keyword argument pair of the **snmp-server group** command.

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, MIB data for that VPN exists in that context. Associating a VPN with a context helps 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 other VPN users on the same networking device.

A route distinguisher (RD) is required to configure an SNMP context. An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of an IPv4 prefix to make it globally unique. An RD is either an autonomous system number (ASN) relative, which means that it is composed of an autonomous system number and an arbitrary number, or an IP address relative and is composed of an IP address and an arbitrary number.

Examples

The following example shows how to create an SNMP context named context1 and associate the context with the VRF named vrf1:

```
Router(config)# snmp-server context context1
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:120
Router(config-vrf)# context context1
```

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode for the configuration of a VRF.
snmp mib community-map	Associates an SNMP community with an SNMP context, engine ID, or security name.
snmp mib target list	Creates a list of target VRFs and hosts to associate with an SNMP v1 or v2c community.
snmp-server context	Creates an SNMP context.
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.
snmp-server trap authentication vrf	Controls VRF-specific SNMP authentication failure notifications.
snmp-server user	Configures a new user to an SNMP group.

control-word

To enable the Multiprotocol Label Switching (MPLS) control word in an Any Transport over MPLS (AToM) dynamic pseudowire connection, use the **control-word** command in pseudowire class configuration mode. To set the control word to autosense mode, use the **default control-word** command. To disable the control word, use the **no** form of this command.

control-word
default control-word
no control-word

Syntax Description

This command has no arguments or keywords.

Command Default

The control word is set to autosense mode.

Command Modes

Pseudowire class configuration (config-pw-class)

Command History

Release	Modification
12.2(33SRE	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

If the MPLS control word is enabled for a static pseudowire and you disable it at the xconnect level, any option set by the pseudowire class is disabled.

Examples

The following example shows how to enable the control word in an AToM dynamic pseudowire connection:

```
Device(config)# pseudowire-class cw-enable
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# control-word
Device(config-pw-class)# exit
```

The following example shows how to enable the control word in an AToM dynamic pseudowire connection and set it to autosense mode:

```
Device(config)# pseudowire-class cw-enable
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# default control-word
Device(config-pw-class)# exit
```

Related Commands

Command	Description
mpls control-word	Enables the MPLS control word in an AToM static pseudowire connection.
show mpls l2transport binding	Displays VC label binding information.

Command	Description
show mpls l2transport vc	Displays information about AToM VCs and AToM static pseudowires that have been enabled to route Layer 2 packets on a router.
xconnect	Binds an attachment circuit to a pseudowire, and configures an AToM static pseudowire.

control-word (MPLS)

To enable the Multiprotocol Label Switching (MPLS) control word in an Any Transport over MPLS (AToM) dynamic pseudowire connection, use the **control-word** command in interface configuration or template configuration mode. To set the control word to autosense mode, use the **default control-word** command. To disable the control word, use the **no** form of this command.

control-word {**include** | **exclude**}
default control-word
no control-word

Syntax Description

include	Specifies that the control word should be included in the pseudowire packets.
exclude	Specifies that the control word should be excluded from the pseudowire packets.

Command Default

The control word is set to autosense mode.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. .
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

If the MPLS control word is enabled for a static pseudowire and you disable it at the cross connect level, any option set by the pseudowire class is disabled.

Examples

The following example shows how to enable the control word in an AToM dynamic pseudowire connection in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# control-word include
```

The following example shows how to enable the control word in an AToM dynamic pseudowire connection and set it to autosense mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# default control-word
Device(config-template)# exit
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
show l2vpn atom binding	Displays VC label binding information.

Command	Description
show l2vpn atom vc	Displays information about AToM VCs and AToM static pseudowires that have been enabled to route Layer 2 packets on a router.

description (l2 vfi)

To provide a description of the switching provider edge (PE) router for an L2VPN multisegment pseudowire, use the **description** command in L2 VFI configuration mode. To remove the description, use the **no** form of this command.

description *string*
no description *string*

Syntax Description

string	Switchng PE router description. The string must be 80 characters or fewer.

Command Default

The switching PE router does not have a description.

Command Modes

L2 VFI (config-vfi)

Command History

Release	Modification
Cisco IOS XE Release 2.3	This command was introduced.

Usage Guidelines

This description is useful for tracking the status of each switching PE router.

Examples

This example adds a description for switching PE router 2:

```
Router(config)# l2 vfi domain_a point-to-point
Router(config-vfi)# description s-pe2
```

Related Commands

Command	Description
show mpls l2transport vc detail	Displays the status information about the pseudowire, including the switching PE router.

description (L2VPN)

To provide a description of the cross connect in a Layer 2 VPN (L2VPN) multisegment pseudowire, use the **description** command in xconnect configuration mode. To remove the description, use the **no** form of this command.

description *string*
no description *string*

Syntax Description

string	Switching PE device description. The string cannot be more than 80 characters.

Command Default

Description for the cross connect is not specified.

Command Modes

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 L2VPN command modifications for cross-OS support. This command will replace the **description (L2VFI)** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

This description is useful for tracking the status of each switching PE device.

Examples

The following example shows how to add a description for the cross connect named xconnect1:

```
Device(config)# l2vpn xconnect context xconnect1
Device(config-xconnect)# description s-pe2
```

Related Commands

Command	Description
description (L2VFI)	Provides a description of the switching PE device for an L2VPN multisegment pseudowire.
show l2vpn atom vc	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a device.

E through L

echo

To customize the default behavior of echo packets, use the **echo** command in MPLS OAM configuration mode. To set the echo packet's behavior to its default value, use the **no** form of this command.

echo {**jitter** *jitter-value* | **permit vrf all** | **revision** {**3** | **4**} | **vendor-extension**}
no echo {**jitter** *jitter-value* | **permit vrf all** | **revision** {**3** | **4**} | **vendor-extension**}

Syntax Description

jitter *jitter-value*	Configures the jitter value, in milliseconds, that is used in the jitter type, length, values (TLVs) and sent as part of the echo request packets. The range is from 1 to 2147483647. The default is 200.
permit	Specifies VRF instances from which to permit echo packets from.
vrf	Specifies the VRF instance where echo packet are permitted.
all	Permits echo packets on all VRF instances.
revision	Specifies the revision number of the echo packet's default values. Valid values are: • **3**—draft-ietf-mpls-lsp-ping-03 (Revision 2) • **4**—RFC 4379 compliant (default)
vendor-extension	Sends Cisco-specific extension TLVs with the echo packets.

Command Default

Cisco-specific extension TLVs are sent with the echo packet. Revision 4 is the router's default.

Command Modes

MPLS OAM configuration

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)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.3(3)S	This command was modified. The **jitter** keyword was added.

Usage Guidelines

Before you can use the **echo** command, you must first enter the **mpls oam** command to enter MPLS OAM configuration mode.

The **jitter** keyword specifies the jitter TLV that is encoded in the echo request to instruct the responder to delay responding by a random time between zero and the jitter value. This allows the echo replies to be spread out uniformly over the jitter duration. The configured jitter value is also used by the responder node. If the configured jitter value is smaller than the received jitter TLV, then the reply is generated after a random time between one and the configured jitter value. If the configured jitter value is larger than the received jitter TLV, then the reply is generated after a random time between one and the received jitter TLV.

Specify the **revision** keyword if one of the following conditions exists:

- You want to change the revision number from the default value of **4** to **3**.
- You previously entered the **mpls oam** command and changed the revision number to **3** and you want to change it back to **4**.

To prevent failures reported by the replying device due to TLV version issues, you can use the **echo revision** command to configure all devices in the core for the same version of the IEFT label-switched path (LSP) ping draft. For example, if the network is running draft RFC 4379 implementations, but one device is capable of only Version 3 (Cisco Revision 3), configure all devices in the network to operate in Revision 3 mode. Revision 3 mode is used only with Multiprotocol Label Switching (MPLS) LSP ping or traceroute. Revision 3 mode does not support MPLS multipath LSP traceroute.

The **vendor-extension** keyword is enabled by default in the device. If your network includes devices that are not Cisco devices, you may want to disable Cisco-extended TLVs. To disable Cisco-extended TLVs, specify the **no echo vendor-extension** command in MPLS OAM configuration mode. To enable Cisco-extended TLVs again, enter the **echo vendor-extension** command.

Examples

The following example configures the jitter value to 100 and permits echo packets on all VRFs:

```
Device(config)# mpls oam
Device(config-mpls)# echo jitter 100
Device(config-mpls)# echo permit vrf all
Device(config-mpls)# exit
```

The following example specifies revision 3 for the echo packet's default values and sends the vendor’s extension TLV with the echo packet:

```
Device(config)# mpls oam
Device(config-mpls)# echo revision 3
Device(config-mpls)# echo vendor-extension
Device(config-mpls)# exit
```

Related Commands

Command	Description
mpls oam	Enters MPLS OAM configuration mode for customizing the default behavior of echo packets.

encapsulation (Any Transport over MPLS)

To configure the ATM adaptation layer (AAL) encapsulation for an Any Transport over MPLS (AToM), use the **encapsulation** command in the appropriate configuration mode. To remove the ATM encapsulation, use the **no** form of this command.

encapsulation *layer-type*
no encapsulation *layer-type*

Syntax Description

layer-type	The adaptation layer type, which is one of the following: • **aal5** --ATM adaptation layer 5 • **aal0** --ATM adaptation layer 0

Command Default

The default encapsulation is AAL5.

Command Modes

L2transport PVC configuration--for ATM PVCs
VC class configuration--for VC class

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(30)S	This command was updated to enable ATM encapsulations as part of a virtual circuit (VC) class.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)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.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

In L2transport VC configuration mode, the **pvc** command and the **encapsulation** command work together. Use the commands for AToM differently than for all other applications. The table below shows the differences in how the commands are used.

Table 2: AToM-Specific Variations of the pvc and encapsulation Commands

Other Applications	AToM
`Router(config-if)# pvc 1/100` `Router(config-if-atm-vc)# encapsulation aal5snap`	`Router(config-if)# pvc 1/100 l2transport` `Router(config-if-atm-l2trans-pvc)# encapsulation aal5`

The following list highlights the differences:

- **pvc** command: For most applications, you create a permanent virtual circuit (PVC) by using the **pvc** *vpi/vci* command. For AToM, you must add the **l2transport** keyword to the **pvc** command. The **l2transport** keyword enables the PVC to transport Layer 2 packets.
- **encapsulation** command: The **encapsulation** command for AToM has only two keyword values: **aal5** or **aal0**. You cannot specify an encapsulation type, such as **aal5snap**. In contrast, the **encapsulation aal5** command you use for most other applications requires you to specify the encapsulation type, such as **aal5snap**.
- You cannot create switched virtual circuits or VC bundles to transport Layer 2 packets.

When you use the **aal5** keyword, incoming cells (except Operation, Administration, and Maintenance [OAM] cells) on that PVC are treated as AAL5 encapsulated packets. The router reassembles the packet from the incoming cells. The router does not check the contents of the packet, so it does not need to know the encapsulation type (such as **aal5snap** and **aal5mux**). After imposing the Multiprotocol Label Switching (MPLS) label stack, the router sends the reassembled packet over the MPLS core network.

When you use the **aal0** keyword, the router strips the header error control (HEC) byte from the cell header and adds the MPLS label stack. The router sends the cell over the MPLS core network.

Examples

The following example shows how to configure a PVC to transport ATM cell relay packets for AToM:

```
Router> enable
Router# configure terminal
Router(config)# interface atm1/0
Router(config-if)# pvc 1/100 l2transport
Router(config-if-atm-l2trans-pvc)# encapsulation aal0
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

The following example shows how to configure ATM AAL5 over MPLS in VC class configuration mode. The VC class is applied to a PVC.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm aal5class
Router(config-vc-class)# encapsulation aal5
Router(config)# interface atm1/0
Router(config-if)# pvc ½00 l2transport
Router(config-if-atm-l2trans-pvc)# class-vc aal5class
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

Related Commands

Command	Description
pvc	Creates or assigns a name to an ATM PVC.

encapsulation (Layer 2 local switching)

To configure the ATM adaptation layer (AAL) for a Layer 2 local switching ATM permanent virtual circuit (PVC), use the **encapsulation** command in ATM PVC L2transport configuration mode. To remove an encapsulation from a PVC, use the **no** form of this command.

encapsulation *layer-type*
no encapsulation *layer-type*

Syntax Description

layer-type	Adaptation layer type. The values are: • **aal5** • **aal0** • **aal5snap** • **aal5mux** • **aal5nlpid** (not available on Cisco 12000 series)

Command Default

If you do not create a PVC, one is created for you. The default encapsulation types for autoprovisioned PVCs are as follows:

- For ATM-to-ATM local switching, the default encapsulation type for the PVC is AAL0.
- For ATM-to-Ethernet or ATM-to-Frame Relay local switching, the default encapsulation type for the PVC is AAL5 SNAP.

Command Modes

ATM PVC L2transport configuration

Command History

Release	Modification
12.0(27)S	This command was introduced for Layer 2 local switching.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
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 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.

Usage Guidelines

The pvc command and the encapsulation command work together. The use of these commands with Layer 2 local switching is slightly different from the use of these commands with other applications. The following list highlights the differences:

- For Layer 2 local switching, you must add the **l2transport** keyword to the **pvc** command. The **l2transport** keyword enables the PVC to transport Layer 2 packets.
- The Layer 2 local switching **encapsulation** command works only with the **pvc** command. You cannot create switched virtual circuits or VC bundles to transport Layer 2 packets. You can use only PVCs to transport Layer 2 packets.

The table below shows the encapsulation types supported for each transport type:

Table 3: Supported Encapsulation Types

Interworking Type	Encapsulation Type
ATM to ATM	AAL0, AAL5
ATM to Ethernet with IP interworking	AAL5SNAP, AAL5MUX
ATM to Ethernet with Ethernet interworking	AAL5SNAP
ATM to Frame-Relay	AAL5SNAP, AAL5NLPID

Examples

The following example shows how to configure a PVC to transport AAL0 packets for Layer 2 local switching:

```
pvc 1/100 l2transport
 encapsulation aal0
```

Related Commands

Command	Description
pvc	Creates or assigns a name to an ATM PVC.

encapsulation dot1q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN, use the **encapsulationdot1q** command in interface range configuration mode or subinterface configuration mode. To disable IEEE 802.1Q encapsulation, use the **no** form of this command.

Interface Range Configuration Mode
encapsulation dot1q *vlan-id* **second-dot1q** {**any***vlan-id*} [**native**]
no encapsulation dot1q

Subinterface Configuration Mode
encapsulation dot1q *vlan-id* **second-dot1q** {**from-bd** | **any***vlan-idvlan-id-vlan-id* | [{,*vlan-id-vlan-id*}]}
no encapsulation dot1q *vlan-id* **second-dot1q** {**from-bd** | **any***vlan-idvlan-id-vlan-id* | [{,*vlan-id-vlan-id*}]}

Syntax Description

vlan-id	Virtual LAN identifier. The allowed range is from 1 to 4094. For the IEEE 802.1Q-in-Q VLAN Tag Termination feature, the first instance of this argument defines the outer VLAN ID, and the second and subsequent instances define the inner VLAN ID.
native	(Optional) Sets the VLAN ID value of the port to the value specified by the *vlan-id* argument. **Note** This keyword is not supported by the IEEE 802.1Q-in-Q VLAN Tag Termination feature.
second-dot1q	Supports the IEEE 802.1Q-in-Q VLAN Tag Termination feature by allowing an inner VLAN ID to be configured.
from-bd	Configures trunk EFP with encapsulation from bridge domain (BD). In this case all the BDs configured on the switch will be part of the VLAN list of the trunk EFP configured with this command.
any	Sets the inner VLAN ID value to a number that is not configured on any other subinterface. **Note** The **any** keyword in the **second-dot1q**command is not supported on a subinterface configured for IP over Q-in-Q (IPoQ-in-Q) because IP routing is not supported on ambiguous subinterfaces.
-	Separates the inner and outer VLAN ID values in the range to be defined. The hyphen is required.
,	Separates each VLAN ID range from the next range. The comma is required. Do not insert spaces between the values.

Command Default

IEEE 802.1Q encapsulation is disabled.

Command Modes

Interface range configuration (config-int-range) Subinterface configuration (config-ifsub)

Command History

Release	Modification
12.0(1)T	This command was introduced.

Release	Modification
12.1(3)T	The **native** keyword was added.
12.2(2)DD	Support was added for this command in interface range configuration mode.
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(7)T	The **second-dot1q** keyword was added to support the IEEE 802.1Q-in-Q VLAN Tag Termination feature.
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI and implemented on the Cisco 10000 series routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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 integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.
Cisco IOS XE Everest Release 16.7.1	The **from-bd** keyword is added to configure trunk EFP with encapsulation from bridge domain (BD).

Usage Guidelines

Interface Range Configuration Mode

IEEE 802.1Q encapsulation is configurable on Fast Ethernet interfaces. IEEE 802.1Q is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

Use the **encapsulationdot1q**command in interface range configuration mode to apply a VLAN ID to each subinterface within the range specified by the**interfacerange** command. The VLAN ID specified by the *vlan-id* argument is applied to the first subinterface in the range. Each subsequent interface is assigned a VLAN ID, which is the specified *vlan-id* value plus the subinterface number minus the first subinterface number (VLAN ID + subinterface number - first subinterface number).

Note The Cisco 10000 series router does not support the **interfacerange** command nor the interface range configuration mode.

Do not configure encapsulation on the native VLAN of an IEEE 802.1Q trunk without using the **native** keyword. (Always use the **native** keyword when *vlan-id* is the ID of the IEEE 802.1Q native VLAN.)

Subinterface Configuration Mode

Use the **second-dot1q** keyword to configure the IEEE 802.1Q-in-Q VLAN Tag Termination feature. 802.1Q in 802.1Q (Q-in-Q) VLAN tag termination adds another layer of 802.1Q tag (called "metro tag" or "PE-VLAN") to the 802.1Q tagged packets that enter the network. Double tagging expands the VLAN space, allowing service providers to offer certain services such as Internet access on specific VLANs for some customers and other types of services on other VLANs for other customers.

After a subinterface is defined, use the **encapsulationdot1q**command to add outer and inner VLAN ID tags to allow one VLAN to support multiple VLANs. You can assign a specific inner VLAN ID to the subinterface; that subinterface is unambiguous. Or you can assign a range or ranges of inner VLAN IDs to the subinterface; that subinterface is ambiguous.

Examples

The following example shows how to create the subinterfaces within the range 0.11 and 0.60 and apply VLAN ID 101 to the Fast Ethernet0/0.11 subinterface, VLAN ID 102 to Fast Ethernet0/0.12 (*vlan-id*= 101 + 12 - 11 = 102), and so on up to VLAN ID 150 to Fast Ethernet0/0.60 (*vlan-id*= 101 + 60 - 11 = 150):

```
Router(config)# interface range fastethernet0/0.11 - fastethernet0/0.60
Router(config-int-range)#
encapsulation dot1q 101
```

The following example shows how to terminate a Q-in-Q frame on an unambiguous subinterface with an outer VLAN ID of 100 and an inner VLAN ID of 200:

```
Router(config)# interface gigabitethernet1/0/0.1
Router(config-subif)#
encapsulation dot1q 100 second-dot1q 200
```

The following example shows how to terminate a Q-in-Q frame on an ambiguous subinterface with an outer VLAN ID of 100 and an inner VLAN ID in the range from 100 to 199 or from 201 to 600:

```
Router(config)# interface gigabitethernet1/0/0.1
Router(config-subif)#
encapsulation dot1q 100 second-dot1q 100-199,201-600
```

Related Commands

Command	Description
encapsulation isl	Enables the ISL, which is a Cisco proprietary protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches.
encapsulation sde	Enables IEEE 802.10 encapsulation of traffic on a specified subinterface in VLANs.
interface range	Specifies multiple subinterfaces on which subsequent commands are executed at the same time.
show vlans dot1q	Displays information about 802.1Q VLAN subinterfaces.

encapsulation (pseudowire)

To specify an encapsulation type for tunneling Layer 2 traffic over a pseudowire, use the **encapsulation** command in the appropriate configuration mode. To remove the encapsulation type, use the **no** form of this command.

encapsulation {**mpls** | **udp** | **l2tpv2** | **l2tpv3**}
no encapsulation

Syntax Description

mpls	Specifies that Multiprotocol Label Switching (MPLS) is used as the data encapsulation method.
udp	Specifies that UDP is used as the data encapsulation method.
l2tpv2	Specifies that Layer 2 Tunneling Protocol version 2 (L2TPv2) is used as the data encapsulation method.
l2tpv3	Specifies that L2TPv3 is used as the data encapsulation method.

Command Default

Encapsulation type for tunneling Layer 2 traffic is not configured.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
15.1(2)S	This command was modified. The **udp** keyword was added.
15.2(1)S	This command was modified. The **l2tpv2** and **l2tpv3** keywords were added in a release prior to Cisco IOS Release 15.2(1)S.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS Release XE 3.4S.
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 for MPLS encapsulation.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

To change the data encapsulation method for tunneling Layer 2 traffic over a pseudowire, follow these:

1. Use the **no pseudowire-class** command in global configuration mode to delete the pseudowire.
2. Use the **pseudowire-class** command to reestablish the pseudowire.
3. Change the encapsulation method using the **encapsulation** command

The following error message is displayed if you use the **no encapsulation mpls** or **encapsulation (l2tpv3)** command to change encapsulation on an existing pseudowire:

```
Encapsulation changes are not allowed on an existing pw-class.
```

You must configure the **ip local interface** command on the same pseudowire class to define the local IP address. All existing time-to-live (TTL) and type of service (TOS) setting values configured by the **ip ttl** and **ip tos (L2TP)** commands are allowed in the pseudowire class. The **ip local interface** command is applicable only when L2TP and UDP data encapsulation methods are used.

Note The **l2tpv2**, **l2tpv3**, and **udp** keywords are not available in interface configuration and template configuration modes.

Examples

The following example shows how to configure UDP as the data encapsulation method for the pseudowire class ether-pw:

```
Device(config)# pseudowire-class ether-pw
Device(config-pw-class)# encapsulation udp
```

The following example shows how to configure MPLS as the data encapsulation method for a pseudowire interface:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
```

The following example shows how to configure MPLS as the data encapsulation in template configuration mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
```

Related Commands

Command	Description
ip ttl	Configures the TTL byte in the IP headers of Layer 2 tunneled packets.
ip tos (L2TP)	Configures the TOS byte in the header of Layer 2 tunneled packets.
pseudowire-class	Specifies the name of a pseudowire class and enters pseudowire class configuration mode.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

exclude-address

To exclude an address from an IP explicit path, use the **exclude-address** command in global configuration mode after entering explicit path configuration mode via the **ip-explicit path** command. To remove an address exclusion from an IP explicit path, use the **no index** command.

exclude-address *A.B.C.D*
no index *number*

Syntax Description

A.B.C.D	Excludes an address from subsequent partial path segments. You can enter the IP address of a link or the router ID of a node.
number	Removes the specified address exclusion from an IP explicit path.

Command Default

Addresses are not excluded from an IP explicit path unless explicitly excluded by the **exclude-address** command.

Command Modes

Global configuration mode

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)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.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 Series Routers.

Usage Guidelines

An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path. If you enter the **exclude-address** command and specify the IP address of a link, the constraint-based Shortest Path First (SPF) routine does not consider that link when it sets up Multiprotocol Label Switching (MPLS) traffic engineering paths. If the excluded address is a flooded MPLS traffic engineering router ID, the constraint-based SPF routine does not consider that entire node. The person performing the configuration must know the router IDs of the routers because it will not be apparent whether the specified number is for a link or for a node.

Note MPLS traffic engineering will accept an IP explicit path that comprises either all excluded addresses configured by the **exclude-address** command or all included addresses configured by the **next-address** command, but not a combination of both.

Examples

The following example shows how to exclude IP addresses 10.0.0.125 and 10.0.0.135 from IP explicit path 500:

```
Router(config-ip-expl-path)# exclude-address 10.0.0.125
Explicit Path identifier 500:
 1: exclude-address 10.0.0.125
Router(config-ip-expl-path)# exclude-address 10.0.0.135
Explicit Path identifier 500:
 1: exclude-address 10.0.0.125
 2: exclude-address 10.0.0.135
Router(config-ip-expl-path)# end
```

To remove IP address 10.0.0.135 from the excluded addresses for explicit path 500, use the following commands:

```
Router(config)# ip explicit-path identifier 500
Router(cfg-ip-expl-path)# no index 1
Explicit Path identifier 500:
    2: exclude-address 10.0.0.135
Router(cfg-ip-expl-path)# end
```

Related Commands

Command	Description
ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies a specified path.

exit (LSP Attributes)

To exit from the label switched path (LSP) attribute list, use the **exit** command in LSP Attributes configuration mode.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

LSP Attributes configuration (config-lsp-attr)

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.

Usage Guidelines

Use this command after you have configured LSP-related attributes for a traffic engineering (TE) tunnel to exit the LSP attribute list and the LSP Attributes configuration mode.

Examples

The following example shows how to set up an LSP attribute list and exit the LSP Attributes configuration mode when the list is complete:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# priority 7 7
Router(config-lsp-attr)# affinity 0 0
Router(config-lsp-attr)# exit
```

Related Commands

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

exit-address-family

To exit from address-family configuration mode, use the **exit-address-family**command in address-family configuration mode.

exit-address-family

Syntax Description

This command has no arguments or keywords.

Command Default

The router remains in address-family configuration mode.

Command Modes

Address-family configuration (config-router-af) VRF address-family configuration (config-vrf-af)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(22)S	Enhanced Interior Gateway Routing Protocol (EIGRP) support was added in Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	EIGRP support was added in Cisco IOS Release 12.2(15)T.
12.2(18)S	EIGRP support was added.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
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)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Use the **exit-address-family** command to exit address-family configuration mode and return to router configuration mode.

This command can be abbreviated to **exit**.

Examples

The following example shows how to exit address-family configuration mode and return to router configuration mode:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453

Router(config-router-af)# exit-address-family
```

```
Router(config-router)#
```

The following example shows how to exit VRF address-family configuration mode and return to VRF configuration mode:

```
Router(config)# vrf definition vrf1
Router(config-vrf)# address-family ipv6
Router(config-vrf-af)# exit-address-family

Router(config-vrf)#
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
address-family ipv4	Enters IPv4 address family configuration mode.
address-family ipv6	Enters IPv6 address family configuration mode.
address-family nsap	Enters CLNS address family configuration mode.
address-family vpnv4	Enters VPNv4 address family configuration mode.
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address-family configuration mode.
router eigrp	Configures the EIGRP address-family process.

exp

To configure Multiprotocol Label Switching (MPLS) experimental (EXP) levels for a Frame Relay permanent virtual circuit (PVC) bundle member, use the **exp** command in Frame Relay VC-bundle-member configuration mode. To remove the EXP level configuration from the PVC, use the **no** form of this command.

exp {*level* | **other**}
no exp

Syntax Description

level	The MPLS EXP level or levels for this Frame Relay PVC bundle member. The range is from 0 to 7. A PVC bundle member can be configured with a single level, multiple individual levels, a range of levels, multiple ranges of levels, or a combination of individual levels and level ranges. Levels can be specified in ascending or descending order (although a subsequent **show running-config**command will display them in ascending order). Examples are as follows: • 0 • 0,2,3 • 6-5 • 0-2,4-5 • 0,1,2-4,7
other	Specifies that this Frame Relay PVC bundle member will handle all of the remaining MPLS EXP levels that are not explicitly configured on any other bundle member PVCs.

Command Default

EXP levels are not configured.

Command Modes

Frame Relay VC-bundle-member configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(16)BX	This command was integrated into Cisco IOS Release 12.2(16)BX.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Assignment of MPLS EXP levels to Frame Relay PVC bundle members lets you create differentiated services, because you can distribute the levels over the various PVC bundle members. You can map a single level or a range of levels to each discrete PVC in the bundle, which enables PVCs in the bundle to carry packets marked with different levels.

Use the **exp other** command to indicate that a PVC can carry traffic marked with EXP levels not specifically configured for other PVCs. Only one PVC in the bundle can be configured using the **exp other** command.

All EXP levels must be accounted for in the PVC bundle configuration, or the bundle will not come up. However, a PVC can be a bundle member but have no EXP level associated with it. As long as all valid EXP levels are handled by other PVCs in the bundle, the bundle can come up, but the PVC that has no EXP level configured will not participate in it.

The **exp** command is available only when MPLS is configured on the interface with the **mpls ip** command.

You can overwrite the EXP level configuration on a PVC by reentering the **exp** command with a new value.

The MPLS experimental bits are a bit-by-bit copy of the IP precedence bits. When Frame Relay PVC bundles are configured for IP precedence and MPLS is enabled, the **precedence** command is replaced by the **exp** command. When MPLS is disabled, the **exp** command is replaced by the **precedence** command.

Examples

The following example shows the configuration of four Frame Relay PVC bundle members in PVC bundle bundle1 configured with MPLS EXP level support:

```
interface serial 0.1 point-to-point
 encapsulation frame-relay
 ip address 10.1.1.1
 mpls ip
 frame-relay vc-bundle bundle1
 pvc 100 ny-control
 class control
 exp 7
 protect vc
 pvc 101 ny-premium
 class premium
 exp 6-5
 protect group
 no bump traffic
 bump explicit 7
 pvc 102 my-priority
 class priority
 exp 4-2
 protect group
 pvc 103 ny-basic
 class basic
 exp other
 protect group
```

Related Commands

Command	Description
bump	Configures the bumping rules for a specific PVC member of a bundle.
class	Associates a map class with a specified DLCI.
dscp (Frame Relay VC-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
match	Specifies which bits of the IP header to use for mapping packet service levels to Frame Relay PVC bundle members.
mpls ip	Enables label switching of IPv4 packets on an interface.

Command	Description
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.
protect	Configures a Frame Relay PVC bundle member with protected group or protected PVC status.

export map

To associate an export map with a VPN Routing and Forwarding (VRF) instance, use the **export map** command in IP VRF configuration or in VRF address family configuration mode. To remove the export map, use the **no** form of this command.

export map *map-name*
no export map *map-name*

Syntax Description

map-name	Identifies the route map to be used as an export map.

Command Default

No export maps are associated with a VRF instance.

Command Modes

IP VRF configuration (config-vrf)
VRF address family configuration (config-vrf-af)

Command History

Release	Modification
12.0(5)T	This command was introduced.
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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **export map** command is used to associate a route map with the specified VRF. The export map is used to filter routes that are eligible for export out of a VRF, based on the route target extended community attributes of the route. Only one export route map can be configured for a VRF.

An export route map can be used when an application requires finer control over the routes that are exported out of a VRF than the control that is provided by import and export extended communities configured for the importing and exporting VRFs.

You can access the **export map** command by using the **ip vrf** global configuration command. You can also access the **export map** command by using the **vrf definition** global configuration command followed by the **address-family** VRF configuration command.

Examples

In the following example, an export map is configured under the VRF, and an access list and route map are configured to specify which prefixes are exported:

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 1:1
Router(config-vrf)# export map BLUE
Router(config-vrf)# route-target import 2:1
Router(config-vrf)# exit
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

```
Router(config)# route-map BLUE permit 10

Router(config-route-map)# match ip address 1

Router(config-route-map)# set extcommunity rt 2:1
Router(config-route-map)# end
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
import map	Configures an import route map for a VRF.
ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
ip vrf	Configures a VRF routing table.
route-target	Creates a route-target extended community for a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

extended-port

Note Effective with Cisco IOS Release 12.4(20)T, the **extended-port** command is not available in Cisco IOS software.

To associate the currently selected extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interface with a particular external interface on the remotely controlled ATM switch, use the **extended-port** command in interface configuration mode.

extended-port *ctrl-if*{**bpx** *bpx-port-number* | **descriptor** *vsi-descriptor* | **vsi** *vsi-port-number*}

Syntax Description

ctrl-if	Identifies the ATM interface used to control the remote ATM switch. You must configure Virtual Switch Interface (VSI) on this interface using the **label-control-protocol** interface configuration command.
bpx *bpx-port-number*	Specifies the associated Cisco BPX interface using the native BPX syntax. *>slot.port* [.*>virtual port*] You can use this form of the command only when the controlled switch is a Cisco BPX switch.
descriptor *vsi-descriptor*	Specifies the associated port by its VSI physical descriptor. The *>vsi-descriptor* string must match the corresponding VSI physical descriptor.
vsi *vsi-port-number*	Specifies the associated port by its VSI port number. The *vsi-port-number* string must match the corresponding VSI physical port number.

Command Default

Extended MPLS ATM interfaces are not associated.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

The **extended-port** interface configuration command associates an XTagATM interface with a particular external interface on the remotely controlled ATM switch. The three alternate forms of the command permit the external interface on the controlled ATM switch to be specified in three different ways.

Examples

The following example shows how to associate an extended MPLS ATM interface and bind it to BPX port 2.3:

```
ATM(config)# interface XTagATM23
ATM(config-if)# extended-port atm0/0 bpx 2.3
```

The following example shows how to associate an extended MPLS ATM interface and bind it to port 2.4:

```
ATM(config)# interface XTagATM24
ATM(config-if)# extended-port atm0/0 descriptor 0.2.4.0
```

The following example shows how to associate an extended MPLS ATM interface and binds it to port 1622:

```
ATM(config)# interface XTagATM1622
ATM(config-if)# extended-port atm0/0 vsi 0x00010614
```

Related Commands

Command	Description
interface XTagATM	Enters interface configuration mode for an extended MPLS ATM (XTagATM) interface.
show controller vsi status	Displays a summary of each VSI-controlled interface.

flow-label enable

To enable the imposition and disposition of flow labels for a pseudowire for virtual private LAN services (VPLS), use the **flow-label enable** command in pseudowire-class configuration mode. To disable the imposition and disposition of flow labels, use the **no** form of this command.

flow-label enable
no flow-label enable

Syntax Description

This command has no arguments or keywords.

Command Default

Flow labels are not enabled.

Command Modes

pseudowire-class (config-pw-class)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

This command enables flow labels. MPLS adds flow labels to the label stack because they contain the flow information of a VC.

Examples

The following example configures a pseudowire and enables flow labels:

```
Router(config)# pseudowire-class try
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# flow-label enable
```

Related Commands

Command	Description
load-balance flow	Enables load balancing of traffic across multiple core interfaces using equal cost multipaths (ECMP) for virtual private LAN services (VPLS).

forward permit l2protocol all

To define the pseudowire that is used to transport bridge protocol data unit (BPDU) information between two network provider edge (N-PE) routers, use the **forward permit l2protocol all** command in L2 VFI configuration mode. To remove the pseudowire, use the **no** form of this command.

forward permit l2protocol all
no forward permit l2protocol all

Command Default

The pseudowire between the two N-PE routers is not defined.

Command Modes

L2 VFI configuration (config-vfi)

Command History

Release	Modification
12.2(33)SRC	This command was introduced as part of the hierarchical virtual private LAN service (H-VPLS) N-PE Redundancy for QinQ and Multiprotocol Label Switching (MPLS) Access feature.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS XE Release 3.2S	This command was integrated into a release prior to Cisco IOS XE Release 3.2S.
Cisco IOS XE Release 3.6S	In Cisco IOS XE Release 3.6S, support was added for the Cisco ASR 903 Router.
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.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the **l2vpn vfi context** command or **l2 vfi** command to enter L2 VFI configuration mode. Only one pseudowire between the two N-PE routers is allowed.

Examples

The following example shows how to create a VPLS pseudowire between the two N-PE routers:

```
Device(config)# l2 vfi vfi1 manual
Device(config-vfi)# vpn id 20
Device(config-vfi)# forward permit l2protocol all
Device(config-vfi)# neighbor 10.10.10.10 encapsulation mpls

Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 20
Device(config-vfi)# forward permit l2protocol all
Device(config-vfi)# member 10.10.10.10 encapsulation mpls
```

Related Commands

Command	Description
member (l2vpn vfi)	Specifies the routers that should form a point-to-point L2VPN VFI connection.
neighbor (L2VPN Pseudowire Switching)	Specifies the routers that should form a point-to-point Layer 2 VFI connection.
show vfi	Displays information related to the VFI.
vpn id	Sets or updates a VPN ID on a VRF instance.

import map

To configure an import route map for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **import map** command in VRF configuration or in VRF address family configuration mode. To remove the import map, use the **no** form of this command.

import [{**ipv4**}] [{**unicast** | **multicast**}] [*prefix-limit*] **map** *map-name*
no import [{**ipv4**}] [{**unicast** | **multicast**}] [*prefix-limit*] **map** *map-name*

Syntax Description

ipv4	(Optional) Specifies that IPv4 prefixes will be imported.
unicast	(Optional) Specifies that unicast prefixes will be imported.
multicast	(Optional) Specifies that multicast prefixes will be imported.
prefix-limit	(Optional) Limits the number of prefixes that will be imported. The default limit is 1000 prefixes. The range is from 1 to 2147483647 prefixes.
map-name	Identifies the route map to be used as an import route map for the VRF.

Command Default

A VRF has no import route map unless one is configured using the **import map** command.

Command Modes

VRF configuration (config-vrf)
VRF address family configuration (config-vrf-af)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use an import route map when an application requires finer control over the routes imported into a VRF than provided by the import and export extended communities configured for the importing and exporting VRF. You can also use the **import map** command to implement the BGP Support for IP Prefix Import from Global Table into a VRF Table feature.

The **import map** command associates a route map with the specified VRF. You can use a route map to filter routes that are eligible for import into a VRF, based on the route target extended community attributes of the route. The route map might deny access to selected routes from a community that is on the import list.

The **import map** command does not replace the need for a route-target import in the VRF configuration. You use the **import map** command to further filter prefixes that match a route-target import statement in that VRF.

You can access the **import map** command by using the **ip vrf** global configuration command. You can also access the **import map** command by using the **vrf definition** global configuration command followed by the **address-family** VRF configuration command.

Examples

The following example shows how to configure an import route map for a VRF:

```
Router(config)# ip vrf vrf1
Router(config-vrf)# import map importmap1
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
export map	Exports IP prefixes from a VRF table into the global table.
ip vrf	Configures a VRF routing table.
route-target	Creates a route-target extended community for a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

index

To insert or modify a path entry at a specific index, use the **index** command in IP explicit path configuration mode. To remove the path entry at the specified index, use the **no** form of this command.

index *index command*
no index *index*

Syntax Description

index	Index number at which the path entry will be inserted or modified. Valid values are from 0 to 65534.
command	An IP explicit path configuration command that creates or modifies a path entry. (You can use only the **next-address** command.)

Command Default

This command is disabled.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 example shows how to insert the next address at index 6:

```
Router(cfg-ip-expl-path)# index 6 next-address 10.3.29.3
Explicit Path identifier 6:
    6: next-address 10.3.29.3
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number. Commands might be renumbered as a result.
interface fastethernet	Enters the command mode for IP explicit paths and creates or modifies the specified path.
list	Displays all or part of the explicit paths.

Command	Description
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

instance (VLAN)

To map a VLAN or a group of VLANs to a multiple spanning tree (MST) instance, use the **instance** command in MST configuration mode. To return the VLANs to the default internal spanning tree (CIST) instance, use the **no** form of this command.

instance *instance-id* **vlans** *vlan-range*
no instance *instance-id*

Syntax Description

instance-id	Instance to which the specified VLANs are mapped; valid values are from 0 to 4094.
vlans *vlan-range*	Specifies the number of the VLANs to be mapped to the specified instance; valid values are from 1 to 4094.

Command Default

No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).

Command Modes

MST configuration mode (config-mst)

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 Cisco IOS Release 12.2 (17d)SXB.
12.2(18)SXF	This command was changed as follows: • You can configure up to 65 interfaces. • You can designate the *instance-id* from 1 to 4094.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

The **vlans***vlan-range* is entered as a single value or a range.

The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added or removed to the existing instances.

Any unmapped VLAN is mapped to the CIST instance.

Examples

The following example shows how to map a range of VLANs to instance 2:

```
Device(config-mst)# instance 2 vlans 1-100
Device(config-mst)#
```

The following example shows how to map a VLAN to instance 5:

```
Device(config-mst)# instance 5 vlans 1100
Device(config-mst)#
```

The following example shows how to move a range of VLANs from instance 2 to the CIST instance:

```
Device(config-mst)# no instance 2 vlans 40-60
Device(config-mst)#
```

The following example shows how to move all the VLANs that are mapped to instance 2 back to the CIST instance:

```
Device(config-mst)# no instance 2
Device(config-mst)#
```

Related Commands

Command	Description
name (MST configuration mode)	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.
spanning-tree mist configuration	Enters MST configuration mode.

inter-as-hybrid

To specify a Virtual Private Network (VPN) routing and forwarding (VRF) instance as an Option AB VRF, use the **inter-as-hybrid** command in VRF address family configuration mode. The Inter-AS Option AB feature is a hybrid of Inter-AS Option (10)A and Inter-AS Option (10)B network configurations, enabling the interconnection of different autonomous systems to provide VPN services. To remove the configuration, use the **no** form of this command.

inter-as-hybrid [**csc**] [**next-hop** {*ip-address* | **global**}]
no inter-as-hybrid

Syntax Description

csc	(Optional) Allocates a per-prefix label for imported routes. For routes received from Option AB peers that are imported into the VRF, the learned out label is installed in forwarding. The Carrier Supporting Carrier (CSC) is a hierarchical VPN model that allows small service providers, or customer carriers, to interconnect their IP or MPLS networks over an MPLS backbone.
next-hop	(Optional) Specifies the next-hop IP address to be set on paths that are imported into the VRF and that are received from an Option AB peer. The next-hop context is also set to the VRF, which imports these paths. If the **next-hop** keyword is not used, the received next hop is retained but the next-hop context (for paths received from Option AB peers) is still set to that of the VRF.
ip-address	(Optional) The IP address of the Inter-AS AB neighbor.
global	(Optional) Enables Inter-AS Option AB+. Specifies that the next-hop address for Border Gateway Protocol (BGP) updates to be set on paths that are imported to the VRF and that are received from an Option AB+ peer are placed in the global routing table. In this situation, the address used is the address of the interface that is at the remote end of the external BGP (eBGP) global shared link. The next-hop context is retained as global and not modified to that of the importing VRF.

Command Default

No VRF is specified as an Option AB VRF.

Command Modes

VRF address family configuration (config-vrf-af)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.0(1)SY	This command was modified. The **global** keyword was added.

Usage Guidelines

Routes imported to this VRF can be advertised to Option AB or Option AB+ peers and VPNv4 Interior Border Gateway Protocol (iBGP) peers. When routes are received from Option AB or Option AB+ peers and imported into the VRF, the next-hop table ID of the route is set to the table ID of the VRF.

The following usage guidelines apply to the **csc** keyword:

- If the **csc** keyword is not used, a per-VRF label is allocated for imported routes. For routes received from Option AB+ peers that are imported into the VRF, the learned out label is not installed in forwarding.
- If the **csc** keyword is used, when routes are received from Option AB or Option AB+ peers and are imported into the VRF, the learned out label is installed in forwarding..
- The **csc** and the **global** keywords are mutually exclusive.

Examples

The following example shows how to configure a VRF as an Option AB VRF:

```
Router(config)# vrf definition vrf1
Router(config-vrf) address-family ipv4
Router(config-vrf-af)# inter-as-hybrid
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
neighbor inter-as-hybrid	Configures the eBGP peer router (ASBR) as an Inter-AS Option AB peer.
rd	Creates routing and forwarding tables for a VPN.
route-target	Creates a route-target extended community for a VRF.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

interface auto-template

To create the template interface, use the **interface auto-template** command in global configuration mode. To delete this interface, use the **no** form of this command.

interface auto-template *interface-num*
no interface auto-template

Syntax Description

interface-num	Interface number. Valid values are from 1 to 25.

Command Default

No default behavior or values are required to create templates.

Command Modes

Global configuration (config)#

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 *interface-num* argument is optional.

Use the **shutdown** command to disable mesh tunnel interface creation when creating a template.

Examples

The following example shows how to create template interface 1:

```
Router(config)# interface auto-template 1
```

Related Commands

Command	Description
clear mpls traffic-eng auto-tunnel mesh	Removes all the mesh tunnel interfaces and re-creates them.
mpls traffic-eng auto-tunnel mesh	Enables autotunnel mesh groups globally.
show mpls traffic-eng auto-tunnel mesh	Displays the cloned mesh tunnel interfaces of each autotemplate interface and the current range of mesh tunnel interface numbers.

interface tunnel-tp

To create a Multiprotocol Label Switching (MPLS) transport profile (TP) tunnel and configure its parameters, use the **interface tunnel-tp**command in global configuration mode. To remove the MPLS-TP tunnel, use the **no** form of the command.

interface tunnel-tp *number*
no interface tunnel-tp *number*

Syntax Description

number	The number of the MPLS-TP tunnel.

Command Default

No MPLS-TP tunnel parameters are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Usage Guidelines

Use this command on endpoint routers to specify the parameters of the MPLS-TP tunnel.

This command also enters interface configuration mode (config-if). From that mode, you can configure the following MPLS-TP parameters:

Command	Description
bfd *bfd-template*	The Bidirectional Forwarding Detection (BFD) template for the tunnel. • If the BFD template for an MPLS-TP tunnel is updated after the tunnel is brought up, a BFD session is brought up on both the working and, if configured, the protect LSPs. • If the BFD template for a tunnel is changed, the BFD sessions for the working and protect LSPs is brought down and then brought back up with the new BFD template. • If a BFD template is not configured on an MPLS-TP tunnel, the initial LSP state will be DOWN.

Command	Description
protect-lsp	Enters protect LSP interface configuration mode (config-if-protect). From this mode, you can configure the following parameters: • Incoming label (**in-label** *num*). • Lock (**lockout)** • Number of the protect LSP (**lsp-number**). By default, the protect LSP number is 1. • Outgoing label and link numbers (**out-label** *num* **out-link** *num*) A protect LSP is a backup for a working LSP. If the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time forwarding reverts back to the working LSP. You can lock out traffic on either the working LSP or the protect LSP but not both. When traffic is locked out of the working or protect LSP, no traffic is forwarded on that LSP. The lock out of the LSP is signaled from one endpoint to the other. When one end has locked out one LSP, the other end may only lock out the same LSP. It is strongly advised to lock out the LSP from both ends, so that both sides know (locally) that the LSP is locked out in the absence of further signaling, which may be the case if connectivity of the LSP is broken due to maintenance for an extended time. In the absence of connectivity, a single-ended lock out expires at the remote end in under 15 minutes (256 * 3.5 seconds).
protection trigger [**ais** | **ldi** | **lkr**	(Optional) Specifies protection triggers for Alarm Indication Signal (AIS), Link Down Indication (LDI), Lock Report (LKR) messages. These triggers should be used in rare cases. They allow you to specify which of these fault notifications can trigger a protection switch. The default is to inherit the setting of the similar commands from the global settings of the protection trigger. This command allows a tunnel to override the global settings. The default for the global settings is that protection is triggered on receipt of LDI and LKR, but not AIS. (AIS is a nonfatal indication of potential issues, which turns into LDI when it is known to be fatal.) This command is useful when other devices send AIS or LDI in unexpected ways. For example, a device from another vendor sends AIS when there are link failures and never sends AIS with the LDI flag. In that case, you can configure the **protection trigger ais** command. If a device sends LDI when there is no actual failure, but there is a possible failure, and you want BFD to detect the actual failure and cause protection switching, you can configure the **no protection trigger ldi** command. To undo these configuration settings and resume inheriting the global settings, enter the **default protection trigger** [**ais** | **ldi** | **lkr**] command.
tp bandwidth *num*	(Optional) Transmit bandwidth, in kilobytes. Range: 1 to 10000000. Default: 0. With MPLS-TP, you cannot use the **bandwidth** command in interface configuration mode. You must use the **tp bandwidth** command.

Command	Description
tp destination *node-id* [**tunnel-tp** *num*] [**global-id** *num*]	Destination MPLS-TP node ID. **global-id** *num:* (Optional)The global ID used for the remote end of this MPLS-TP tunnel Range: 0 to 2147483647. Default: The global ID that is configured with the **mpls tp** command. **tunnel-tp** *num: (Optional)* The tunnel-TP number of the MPLS-TP tunnel destination. If the tunnel-TP number is not specified, the number assigned to the local tunnel is used.
tp source *node-id* **global-id** *num*	(Optional) Source MPLS-TP tunnel node ID. This is the ID of the endpoint router being configured. You can specify the source ID to override the router ID configured in the global MPLS-TP configuration. **global-id** *num:* (Optional) The global ID of the local endpoint for this tunnel. Range: 0 to 2147483647. Default: The global ID that is configured with the **mpls tp** command. The **tp source** command is optional and not typically used, because the global router ID and global ID can be used to identify the tunnel source at the endpoint. All tunnels on the router generally use the same (globally specified) source information.
tp tunnel-name *name*	(Optional) Specifies the name of the MPLS-TP tunnel. The TP tunnel name is displayed in **show mpls tp tunnel**command output. This command is useful for consistently identifying the tunnel at all endpoints and midpoints.
working-lsp	Enters working LSP interface configuration mode (config-if-working). From this mode, you can configure the following parameters: • Incoming label (**in-label** *num*). • Lock (**lockout).** • Number of the working LSP (**lsp-number**). By default, the working LSP number is 0. • Outgoing label and link numbers (**out-label** *num* **out-link** *num*) A working LSP is the primary LSP. If the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time forwarding reverts back to the working LSP. The lock out of the LSP is signaled from one endpoint to the other. When one end has locked out one LSP, the other end may only lock out the same LSP. It is strongly advised to lock out the LSP from both ends, so that both sides know (locally) that the LSP is locked out in the absence of further signaling, which may be the case if connectivity of the LSP is broken due to maintenance for an extended time. In the absence of connectivity, a single-ended lock out expires at the remote end in under 15 minutes (256 * 3.5 seconds).

Examples

The following example specifies the parameters for an MPLS-TP tunnel:

```
interface Tunnel-tp1
 description "MPLS-TP tunnel # 1"
 no ip address
 no keepalive
 tp bandwidth 10000
```

```
tp destination 10.1.1.1
bfd mpls-tp-bfd-2
working-lsp
 out-label 112 out-link 1
 in-label 211
protect-lsp
 out-label 115 out-link 2
 in-label 511
```

Related Commands

Command	Description
mpls tp	Specifies global values used across the MPLS TP implementation and applies to all tunnels and midpoint LSPs.
mpls tp link	Specifies the parameters for an MPLS TP link.
mpls tp lsp	Specifies the parameters for forwarding of a MPLS-TP LSP at the tunnel midpoint.
working-lsp	Enters working Label Switched Path (LSP) mode on a TP tunnel interface.

interface virtual-ethernet

To create a virtual Ethernet interface, use the **interface virtual-ethernet** command in privileged EXEC configuration mode. To remove the virtual Ethernet interface, use the **no** form of this command.

interface virtual-ethernet *num*
no interface virtual-ethernet *num*

Syntax Description

num	Specifies a unique number assigned to the virtual Ethernet interface. Valid values are 0 to 4094.

Command Default

Virtual Ethernet interfaces are not created.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

This command allows several ethernet virtual circuits (EVCs) to be bundled over a single pseudowire. The pseudowire terminating at this virtual Ethernet interface acts like a virtual ethernet trunk port. This allows Layer 2 protocols to be run over the pseudowire. Similar to a physical Ethernet interface, a virtual Ethernet interface allows configuration of Ethernet flow points.

Examples

The following example creates a virtual Ethernet interface:

```
Router(config)# interface virtual-ethernet 1
```

Related Commands

Command	Description
show interface virtual-ethernet	Displays the status of virtual Ethernet interfaces.

interface xtagatm

Note Effective with Cisco IOS Release 12.4(20)T, the **interface xtagatm** command is not available in Cisco IOS software.

To create an extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interface, use the **interface xtagatm** command in global configuration mode.

interface xtagatm *interface-number*

Syntax Description

interface-number	The interface number.

Command Default

XTagATM interfaces are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology.
12.4(20)T	This command was removed.

Usage Guidelines

XTagATM interfaces are virtual interfaces that are created on reference-like tunnel interfaces. An XTagATM interface is created the first time the **interface xtagatm** command is issued for a particular interface number. These interfaces are similar to ATM interfaces, except that the former only supports LC- ATM encapsulation.

Examples

The following example shows how to create an XTagATM interface with interface number 62:

```
Router(config)# interface xtagatm62
```

Related Commands

Command	Description
extended-port	Associates the currently selected extended XTagATM interface with a remotely controlled switch.

interworking

To enable Layer 2 VPN (L2VPN) interworking, use the **interworking** command in pseudowire class configuration or xconnect configuration mode. To disable L2VPN interworking, use the **no** form of this command.

interworking {**ethernet** | **ip** | **vlan**}
no interworking {**ethernet** | **ip** | **vlan**}

Syntax Description

ethernet	Causes Ethernet frames to be extracted from the attachment circuit and sent over the pseudowire. It is assumed that Ethernet has end-to-end transmission. Attachment circuit frames that do not contain Ethernet frames are dropped. In the case of VLAN, the VLAN tag is removed, which leaves a pure Ethernet frame.
ip	Causes IP packets to be extracted from the attachment circuit and sent over the pseudowire. The attachment circuit frames that do not contain IPv4 packets are dropped.
vlan	Causes Ethernet frames and the VLAN tag to be sent over the pseudowire. It is assumed that Ethernet has end-to-end transmission. The attachment circuit frames that do not contain Ethernet frames are dropped.

Command Default

L2VPN interworking is disabled.

Command Modes

Pseudowire class configuration (config-pw-class)

Xconnect configuration (config-xconnect)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(52)SE	This command was modified. The **vlan** keyword was added as part of the L2VPN Interworking: VLAN Enable/Disable Option feature.
12.2(33)SRE	This command was modified. The **vlan** keyword was added as part of the L2VPN Interworking: VLAN Enable/Disable Option feature.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
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 xconnect configuration mode.

Usage Guidelines

The table below shows which L2VPN interworking features support Ethernet, IP, and VLAN types of interworking.

Table 4: L2VPN Interworking Feature Support

L2VPN Interworking Feature	Interworking Support
Frame Relay to PPP	IP
Frame Relay to ATM AAL5	IP
Ethernet/VLAN to ATM AAL5	IP and Ethernet
Ethernet/VLAN to Frame Relay	IP and Ethernet
Ethernet/VLAN to PPP	IP
Ethernet to VLAN	IP, Ethernet, and VLAN
L2VPN Interworking: VLAN Enable/Disable Option for AToM	Ethernet VLAN

Examples

The following example shows a pseudowire class configuration that enables the L2VPN interworking:

```
Device(config)# pseudowire-class ip-interworking
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# interworking ip
```

The following example shows an xconnect configuration that enables L2VPN interworking:

```
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# interworking ip
```

Related Commands

Command	Description
encapsulation l2tpv3	Specifies that L2TPv3 is used as the data encapsulation method for tunneling IP traffic over the pseudowire.
encapsulation mpls	Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.

interval (MPLS-TP)

To configure the transmit and receive intervals between Bidirectional Forwarding Detection (BFD) packets and to specify the number of consecutive BFD control packets to miss before BFD declares that a peer is unavailable, use the **interval**command in BFD configuration mode. To disable interval values, use the **no** form of this command.

interval [**microseconds**] {**both** *time* | **min-tx** *time* **min-rx** *time*} [**multiplier** *multiplier-value*]
no interval

Syntax Description

microseconds	(Optional) Specifies, in microseconds, the rate at which BFD control packets are sent to and received from BFD peers. If the **microseconds** keyword is not specified, the interval defaults to milliseconds.
both *time*	Specifies the rate at which BFD control packets are sent to BFD peers and the rate at which BFD control packets are received from BFD peers.
min-tx *time*	Specifies the rate at which BFD control packets are sent to BFD peers.
min-rx *time*	Specifies, the rate at which BFD control packets are received from BFD peers.
multiplier *multiplier-value*	(Optional) Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. Range: 3 to 50. Default: 3.

Command Default

No session parameters are set.

Command Modes

BFD configuration (config-bfd)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Usage Guidelines

The **interval** command allows you to configure the session parameters for a BFD template.

Examples

The following example shows how to configure interval settings for the node1 BFD template:

```
Router(config)# bfd-template single-hop node1

Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3
```

Related Commands

Command	Description
bfd-template	Creates a BFD template and enters BFD configuration mode.

ip explicit-path

To enter the command mode for IP explicit paths and create or modify the specified path, use the **ip explicit-path** command in global configuration mode. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path. To disable this feature, use the **no** form of this command.

ip explicit-path {**name** *word* | **identifier** *number*} [{**enable** | **disable**}]
no explicit-path {**name** *word* | **identifier** *number*}

Syntax Description

name *word*	Name of the explicit path.
identifier *number*	Number of the explicit path. The range is 1 to 65535.
enable	(Optional) Enables the path.
disable	(Optional) Prevents the path from being used for routing while it is being configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Examples

The following example shows how to enter the explicit path command mode for IP explicit paths and creates a path numbered 500:

```
Router(config)# ip explicit-path identifier 500
Router(config-ip-expl-path)#
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number. Commands might be renumbered as a result.

Command	Description
index	Inserts or modifies a path entry at a specific index.
ip route vrf	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

ip flow-cache mpls label-positions

To enable Multiprotocol Label Switching (MPLS)-Aware NetFlow, use the **ip flow-cache mpls label-positions** command in global configuration mode. To disable MPLS-aware NetFlow, use the **no** form of this command.

ip flow-cache mpls label-positions [*label-position-1* [*label-position-2* [*label-position-3*]]] [**exp-bgp-prefix-fields**] [**no-ip-fields**] [**mpls-length**]
no ip flow-cache mpls label-positions

Syntax Description

label-position-l	(Optional) Position of an MPLS label in the incoming label stack. Label positions are counted from the top of the stack, starting with 1.
exp-bgp-prefix-fields	(Optional) Generates a MPLS Provider Edge (PE) PE-to-PE traffic matrix. The following IP-related flow fields are included: • Input interface • BGP Nexthop • MPLS Experimental (EXP) bits The MPLS label values will be set to zero on the Cisco 10000 in the display output of the **show ip cache verbose flow aggregation exp-bgp-prefix** command.
no-ip-fields	(Optional) Controls the capture and reporting of MPLS flow fields. If the **no-ip-fields** keyword is not specified, the following IP-related flow fields are included: • Source IP address • Destination IP address • Transport layer protocol • Source application port number • Destination application port number • IP type of service (ToS) • TCP flag If the **no-ip-fields** keyword is specified, the IP-related fields are reported with a value of 0.
mpls-length	(Optional) Controls the reporting of packet length. If the **mpls-length** keyword is specified, the reported length represents the sum of the MPLS packet payload length and the MPLS label stack length. If the **mpls-length** keyword is not specified, only the length of the MPLS packet payload is reported.

Command Default

MPLS-Aware NetFlow is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.0(25)S	The **no-ip-fields** and **mpls-length** keywords were added.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **exp-bgp-prefix-fields** keyword was added.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Use this command to configure the MPLS-aware NetFlow feature on a label switch router (LSR) and to specify labels of interest in the incoming label stack. Label positions are counted from the top of the stack, starting with 1. The position of the top label is 1, the position of the second label is 2, and so forth.

With MPLS-aware NetFlow enabled on the router, NetFlow collects data for incoming IP packets and for incoming MPLS packets on all interfaces where NetFlow is enabled in full or in sampled mode.

Caution When you enter the **ip flow-cache mpls label-positions** command on a Cisco 12000 series Internet router, NetFlow will stop collecting data for incoming IP packets on any Engine 4P line cards installed in the router on which NetFlow is enabled in full or in sampled mode. Engine 4P line cards in a Cisco 12000 series Internet router do not support NetFlow data collection of incoming IP packets and MPLS packets concurrently.

Tip MPLS-aware NetFlow is enabled in global configuration mode. NetFlow is enabled per interface.

Examples

The following example shows how to configure MPLS-aware NetFlow to capture the first (top), third, and fifth label:

```
Router(config)# ip flow-cache mpls label-positions 1 3 5
```

The following example shows how to configure MPLS-aware NetFlow to capture only MPLS flow information (no IP-related flow fields) and the length that represents the sum of the MPLS packet payload length and the MPLS label stack length:

```
Router(config)# ip flow-cache mpls label-positions no-ip-fields mpls-length
```

The following example shows how to configure MPLS PE-to-PE Traffic Statistics for Netflow:

```
Router(config)# ip flow-cache mpls label-positions 1 2 exp-bgp-prefix-fields
```

Related Commands

Command	Description
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.

Command	Description
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters.
ip flow egress	Enables NetFlow egress accounting for traffic that the router is forwarding.
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip multicast mpls traffic-eng

To enable IP multicast traffic on a tailend router enabled with Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) functionality, use the **ip multicast mpls traffic-eng** command in privileged EXEC mode. To disable IP multicast for MPLS TE P2MP on tailend routers, use the **no** form of this command.

ip multicast mpls traffic-eng [**range** {*access-list-numberaccess-list-name*}]
no ip multicast mpls traffic-eng [**range**]

Syntax Description

range	(Optional) Enables multicast for a specific set of multicast streams.
access-list-number	The specific number of the access list. Valid values are 100-199.
access-list-name	The specific name of the access list.

Command Default

MPLS TE P2MP functionality is not enabled.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

You configure this command on the tailend routers in an MPLS TE P2MP topology.

Examples

The following example enables multicast routing on tailend routers configured with MPLS TE P2MP functionality:

```
Router(config)# ip multicast-routing

Router(config)# ip multicast mpls traffic-eng
```

Related Commands

Command	Description
show ip mroute	Displays IP multicast forwarding on MPLS TE P2MP tailend routers.

ip path-option

To specify an explicit or dynamic path option for a particular destination address in a destination list, use the **ip path-option** command in traffic engineering destination list configuration mode. To remove the path option, use the **no** form of this command.

ip *ip-address* **path-option** *id* {**dynamic** | **explicit** {**name** *name* | **identifier** *number*} [**verbatim**]}
no ip *ip-address* **path-option** *id*

Syntax Description

ip-address	The destination address of the path.
id	The preference for this path option for the same destination address. The valid values are 1-1000. Only one path option is supported for each destination address.
dynamic	Specifies that the traffic engineering paths be dynamically computed.
explicit	Specifies that the traffic engineering paths be explicitly configured.
name *name*	Specifies the name of the explicit path.
identifier *number*	Specifies the number of the explicit path.
verbatim	(Optional) Specifies that the path should be sent out without any checking.

Command Default

Path options are not configured.

Command Modes

Traffic engineering destination list (cfg-te-dest-list)

Command History

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

Usage Guidelines

- The **ip path-option** command is supported at a sublabel switched path (sub-LSP) level.
- Point-to-multipoint traffic engineering supports only one path option per destination.

Examples

The following example shows the configuration of a destination list with explicit path options:

```
Router(config)# mpls traffic-eng destination list identifier 1
Router(cfg-te-dest-list)# ip 10.10.10.10 path-option 1 explicit identifier 1
```

Related Commands

Command	Description
mpls traffic-eng destination list	Specifies a MPLS traffic engineering point-to-multipoint destination list.

ip route static inter-vrf

To allow static routes to point to Virtual Private Network (VPN) routing and forwarding (VRF) interfaces other than those to which the static route belongs, use the **ip route static inter-vrf** command in global configuration mode. To prevent static routes from pointing to VRF interfaces in VRFs to which they do not belong, use the **no** form of this command.

ip route static inter-vrf
no ip route static inter-vrf

Syntax Description

This command has no arguments or keywords.

Command Default

Static routes are allowed to point to VRF interfaces in any VRF.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
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 **ip route static inter-vrf** command is turned on by default. The **no ip route static inter-vrf** command causes the respective routing table (global or VRF) to reject the installation of static routes if the outgoing interface belongs to a different VRF than the static route being configured. This prevents security problems that can occur when static routes that point to a VRF interface in a different VRF are misconfigured. You are notified when a static route is rejected, then you can reconfigure it.

For example, a static route is defined on a provider edge (PE) router to forward Internet traffic to a customer on the interface pos1/0, as follows:

```
Router(config)# ip route 10.1.1.1 255.255.255.255 pos 1/0
```

The same route is mistakenly configured with the next hop as the VRF interface pos10/0:

```
Router(config)# ip route 10.1.1.1 255.255.255.255 pos 10/0
```

By default, Cisco IOS software accepts the command and starts forwarding the traffic to both pos1/0 (Internet) and pos10/0 (VPN) interfaces.

If the static route is already configured that points to a VRF other than the one to which the route belongs when you issue the **no ip route static inter-vrf** command, the offending route is uninstalled from the routing table and a message similar to the following is sent to the console:

```
01:00:06: %IPRT-3-STATICROUTESACROSSVRF: Un-installing static route x.x.x.x/32
 from global routing table with outgoing interface intx/x
```

If you enter the **no ip route static inter-vrf** command before a static route is configured that points to a VRF interface in a different VRF, the static route is not installed in the routing table and a message is sent to the console.

Configuring the **no ip route static inter-vrf** command prevents traffic from following an unwanted path. A VRF static route points to a global interface or any other VRF interface as shown in the following **ip route vrf** commands:

- Interface serial 1/0.0 is a global interface:

```
Router(config)# no ip route static inter-vrf
Router(config)# ip route vrf vpn1 10.10.1.1 255.255.255.255 serial 1/0.0
```

- Interface serial 1/0.1 is in vpn2:

```
Router(config)# no ip route static inter-vrf
Router(config)# ip route vrf vpn1 10.10.1.1 255.255.255.255 serial 1/0.1
```

With the **no ip route static inter-vrf** command configured, these static routes are not installed into the vpn1 routing table because the static routes point to an interface that is not in the same VRF.

If you require a VRF static route to point to a global interface, you can use the **global** keyword with the **ip route vrf** command:

```
Router(config)# ip route vrf vpn1 10.12.1.1 255.255.255.255 serial 1/0.0 10.0.0.1 global
```

The **global** keyword allows the VRF static route to point to a global interface even when the **no ip route static inter-vrf** command is configured.

Examples

The following example shows how to prevent static routes that point to VRF interfaces in a different VRF:

```
Router(config)# no ip route static inter-vrf
```

Related Commands

Command	Description
ip route vrf	Establishes static routes for a VRF.

ip route vrf

To establish static routes for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **ip route vrf** command in global configuration mode. To disable static routes, use the **no** form of this command.

ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]
no ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]

Syntax Description

vrf-name	Name of the VRF for the static route.
prefix	IP route prefix for the destination, in dotted decimal format.
mask	Prefix mask for the destination, in dotted decimal format.
next-hop-address	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
interface	(Optional) Name of network interface to use.
interface-number	(Optional) Number identifying the network interface to use.
global	(Optional) Specifies that the given next hop address is in the non-VRF routing table.
distance	(Optional) An administrative distance for this route.
permanent	(Optional) Specifies that this route will not be removed, even if the interface shuts down.
tag *tag*	(Optional) Specifies the label (tag) value that can be used for controlling redistribution of routes through route maps.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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.
XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use a static route when the Cisco IOS software cannot dynamically build a route to the destination.

If you specify an administrative distance when you set up a route, you are flagging a static route that can be overridden by dynamic information. For example, Interior Gateway Routing Protocol (IGRP)-derived routes have a default administrative distance of 100. To set a static route to be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes each have a default administrative distance of 1.

Static routes that point to an interface are advertised through the Routing Information Protocol (RIP), IGRP, and other dynamic routing protocols, regardless of whether the routes are redistributed into those routing protocols. That is, static routes configured by specifying an interface lose their static nature when installed into the routing table.

However, if you define a static route to an interface not defined in a network command, no dynamic routing protocols advertise the route unless a **redistribute static** command is specified for these protocols.

If a VPNv4 prefix in a given VRF is added to the global routing table, and there is recirculation on the corresponding VPN label due to egress features (ACL, Netflow, or QoS) configured on the outgoing interface, the traffic is not routed inside the VRF routing table, but inside the global routing table. If the same prefix exists in the global table, it results in a Layer 3 loop. To avoid this occurrence, use the **mls mpls recir-agg** command to switch off the VPN-CAM used for the VRF lookups, and to allocate the reserved VLAN for every VRF instance configured on the Cisco 7600 series routers.

Supported Static Route Configurations

When you configure static routes in a Multiprotocol Label Switching (MPLS) or MPLS VPN environment, note that some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS releases 12.*x* T, 12.*x* M, and 12.0S. The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS release 12.2(25)S and later releases. Use the following guidelines when configuring static routes.

Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in an MPLS environment:

ip route *destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

ip route *destination-prefix mask* **interface1 next-hop1 ip route** *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the next hop can be reached through two paths:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the destination can be reached through two next hops:

ip route *destination-prefix mask* **next-hop1 ip route** *destination-prefix mask* **next-hop2**

Use the *interface* and *next-hop* arguments when specifying static routes.

Supported Static Routes in an MPLS VPN Environment

The following **ip route vrf** commands are supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

- • **ip route vrf** *vrf-name destination-prefix mask next-hop-address*
  • **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
  • **ip route vrf** *vrf-name destination-prefix mask interface1 next-hop1* **ip route vrf** *vrf-name destination-prefix ma sk interface2 next-hop2*

The following **ip route vrf** commands are supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the Internet gateway.

- • **ip route vrf** *vrf-name destination-prefix mask next-hop-address* **global**
  • **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address* (This command is supported when the next hop and interface are in the core.)

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interface:

ip route *destination-prefix mask* **interface1 next-hop1 ip route** *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS VPN Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

ip route vrf *destination-prefix mask next-hop-address* **global**

The following **ip route** commands are not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

ip route vrf *destination-prefix mask* **next-hop1 global ip route vrf** *destination-prefix mask* **next-hop2 global**

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

ip route vrf *vrf-name destination-prefix mask* **next-hop1 ip route vrf** *vrf-name destination-prefix mask* **next-hop2**

Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf** command is supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table on the customer equipment (CE) side. For example, the following command is supported when the destination prefix is the CE router's loopback address, as in external BGP (EBGP) multihop cases.

ip route vrf *vrf-name destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static nonrecursive routes and a specific outbound interfaces:

ip route *destination-prefix mask* **interface1 nexthop1 ip route** *destination-prefix mask* **interface2 nexthop2**

Examples

The following command shows how to reroute packets addressed to network 10.23.0.0 in VRF vpn3 to router 10.31.6.6:

```
Router(config)# ip route vrf vpn3 10.23.0.0 255.255.0.0 10.31.6.6
```

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.
redistribute static	Redistributes routes from another routing domain into the specified domain.

ip rsvp msg-pacing

Note Effective with Cisco IOS Release 12.2(13)T, the **ip rsvp msg-pacing** command is replaced by the **ip rsvp signalling rate-limit** command. See the **ip rsvp signalling rate-limit** command for more information.

To configure the transmission rate for Resource Reservation Protocol (RSVP) messages, use the **ip rsvp msg-pacing** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp msg-pacing [**period** *ms* [**burst** *msgs* [**maxsize** *qsize*]]]
no rsvp msg-pacing

Syntax Description

period *ms*	(Optional) Length of the interval, in milliseconds, during which a router can send the number of RSVP messages specified in the **burst** keyword. The value can be from 1 to 1000 milliseconds.
burst *msgs*	(Optional) Maximum number of RSVP messages that a router can send to an output interface during each interval specified in the *period* keyword. The value can be from 1 to 2000.
maxsize *qsize*	(Optional) Size of per-interface output queues in the sending router. Valid values are from 1 to 2000.

Command Default

RSVP messages are not paced. If you enter the command without the optional **burst** keyword, the transmission rate for RSVP messages is limited to 200 messages per second per outgoing interface. The default output queue size, specified in the **maxsize** keyword, is 500.

Command Modes

Global configuration (config)

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.
12.2(13)T	This command was replaced with the **ip rsvp signalling rate-limit** command.

Usage Guidelines

You can use this command to prevent a burst of RSVP traffic engineering signaling messages from overflowing the input queue of a receiving router. Overflowing the input queue with signaling messages results in the

router dropping some messages. Dropped messages substantially delay the completion of signaling for LSPs for which messages have been dropped.

If you enter the **ip rsvp msg-pacing** command without the optional **burst** keyword, the transmission rate for RSVP messages is limited to 200 messages per second per outgoing interface. The default output queue size, specified in the **maxsize** keyword, is 500.

Examples

The following example shows how to configure a router to send a maximum of 150 RSVP traffic engineering signaling messages in 1 second to a neighbor, and the size of the output queue is 750:

```
Router(config)# ip rsvp msg-pacing period 1 burst 150 maxsize 750
```

Related Commands

Command	Description
clear ip rsvp msg-pacing	Clears the RSVP message pacing output from the **show ip rsvp neighbor** command.

ip rsvp signalling hello (configuration)

To enable Hello globally on the router, use the **iprsvpsignallinghello**command in global configuration mode. To disable Hello globally on the router, use the **no** form of this command.

ip rsvp signalling hello
no ip rsvp signalling hello

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

To enable Hello globally on the router, you must enter this command. You also must enable Hello on the interface.

Examples

In the following example, Hello is enabled globally on the router:

```
Router(config)# ip rsvp signalling hello
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.

ip rsvp signalling hello (interface)

To enable hello on an interface where you need Fast Reroute protection, use the **iprsvpsignallinghello**command in interface configuration mode. To disable hello on an interface where you need Fast Reroute protection, use the **no** form of this command

ip rsvp signalling hello
no ip rsvp signalling hello

Syntax Description

This command has no arguments or keywords.

Command Default

No hellos are enabled.

Command Modes

Interface configuration (config-if)

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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You must configure hello globally on a router and on the specific interface.

Examples

In the following example, hello is enabled on an interface:

```
Router(config-if)# ip rsvp signalling hello
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello dscp	Sets the DSCP value that is in the IP header of the Hello messages sent out from the interface.
ip rsvp signalling hello refresh misses	Specifies how many Hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.
ip rsvp signalling hello refresh interval	Configures the Hello request interval.

ip rsvp signalling hello bfd (configuration)

To enable the Bidirectional Forwarding Detection (BFD) protocol globally on the router for Multiprotocol Label Switching (MPLS) traffic engineering (TE) link and node protection, use the **ip rsvp signalling hello bfd** command in global configuration mode. To disable BFD globally on the router, use the **no** form of this command.

ip rsvp signalling hello bfd
no ip rsvp signalling hello bfd

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is not enabled globally on the router for MPLS TE link and node protection.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

To enable the BFD protocol on the router, you must enter this command. You also must enter the **ip rsvp signalling hello bfd** command on the interface.

Examples

The following example allows you to use the BFD protocol on the router for MPLS TE link and node protection:

```
Router(config)# ip rsvp signalling hello bfd
```

Related Commands

Command	Description
ip rsvp signalling hello bfd (interface)	Enables the BFD protocol on an interface where you need MPLS TE link and node protection.
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

ip rsvp signalling hello bfd (interface)

To enable the Bidirectional Forwarding Detection (BFD) protocol on an interface for Multiprotocol Label Switching (MPLS) traffic engineering (TE) link and node protection, use the **ip rsvp signalling hello bfd** command in interface configuration mode. To disable BFD on an interface for MPLS TE link and node protection, use the **no** form of this command.

ip rsvp signalling hello bfd
no ip rsvp signalling hello bfd

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is not enabled on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

You must enter the **ip rsvp signalling hello bfd** command on the router and on the specific interface.

Examples

In the following example, the BFD protocol is enabled on an interface:

```
Router(config-if)# ip rsvp signalling hello bfd
```

Related Commands

Command	Description
ip rsvp signalling hello bfd (configuration)	Enables the BFD protocol on the router for MPLS TE link and node protection.
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

ip rsvp signalling hello dscp

To set the differentiated services code point (DSCP) value that is in the IP header of a Resource Reservation Protocol (RSVP) traffic engineering (TE) hello message sent from an interface, use the **iprsvpsignallinghellodscp** command in interface configuration mode. To set the DSCP value to its default, use the **no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **dscp** *num*
no ip rsvp signalling hello [**fast-reroute**] **dscp**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
num	DSCP value. Valid values are from 0 to 63.

Command Default

The default DSCP value is 48.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute** keyword was added.
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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If a link is congested, it is recommended that you set the DSCP to a value higher than 0 to reduce the likelihood that hello messages will be dropped.

You configure the DSCP per interface, not per flow.

The DSCP applies to the RSVP hellos created on a specific interface. You can configure each interface independently for DSCP.

If you issue the **iprsvpsignallinghellodscp** command without the optional **fast-reroute**keyword, the command applies to Fast Reroute hellos. This command is provided for backward compatibility; however, we recommend that you use the **iprsvpsignallinghellofast-reroutedscp**command.

Examples

In the following example, hello messages sent from this interface have a DSCP value of 30 and Fast Reroute capability is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute dscp 30
```

In the following example, hello messages sent from this interface have a DSCP value of 30 and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello dscp 30
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables hellos on an interface where you need Fast Reroute protection.
ip rsvp signalling hello refresh interval	Sets the hello refresh interval in hello messages.
ip rsvp signalling hello reroute refresh misses	Sets the missed refresh limit in hello messages.

ip rsvp signalling hello refresh interval

To configure the Resource Reservation Protocol (RSVP) traffic engineering (TE) hello refresh interval, use the **iprsvpsignallinghellorefreshinterval** command in interface configuration mode. To set the refresh interval to its default value, use the**no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **refresh interval** *interval-value*
no ip rsvp signalling hello [**fast-reroute**] **refresh interval**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
interval-value	Frequency, in milliseconds (msec), at which a node sends hello messages to a neighbor. Valid values are from 10 to 30000 msec. **Note** Values below the default of 200 msec are not recommended, because they can cause RSVP Hellos to falsely detect a neighbor down event and unecessarily trigger Fast ReRoute.

Command Default

The default frequencyat which a node sends hello messages to a neighbor is 200 msec.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute**keyword was added.
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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You can configure the hello request interval on a per-interface basis. A node periodically generates a hello message containing a Hello Request object for each neighbor whose status is being tracked. The frequency of those hello messages is determined by the hello interval.

If you issue the **iprsvpsignallinghellorefreshinterval**command without the optional **fast-reroute**keyword, the command applies to Fast Reroute hellos. This command is provided for backward compatibility; however, we recommend that you use the **iprsvpsignallinghellofast-rerouterefreshinterval**command.

Examples

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh interval 5000
```

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello refresh interval 5000
```

Related Commands

Command	Description
ip rsvp signalling hello dscp	Sets the DSCP value in hello messages.
ip rsvp signalling hello graceful-restart fresh interval	Sets the refresh interval in graceful restart hello messages.
ip rsvp signalling hello reroute refresh misses	Sets the missed refresh limit in hello messages.

ip rsvp signalling hello refresh misses

To specify how many Resource Reservation Protocol (RSVP) traffic engineering (TE) hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down, use the **iprsvpsignallinghellorefreshmisses** command in interface configuration mode. To return the missed refresh limit to its default value, use the **no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **refresh misses** *msg-count*
no ip rsvp signalling hello [**fast-reroute**] **refresh misses**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
msg-count	Number of sequential hello acknowledgments that a node can miss before RSVP considers the state expired and tears it down. Valid values are from 4 to 10.

Command Default

The default number of sequential hello acknowledgments is 4.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute** keyword was added.
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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T

Usage Guidelines

A hello comprises a hello message, a Hello Request object, and a Hello ACK object. Each request is answered by an acknowledgment. If a link is very congested or a router has a very heavy load, set this number to a value higher than the default value to ensure that hello does not falsely declare that a neighbor is down.

If you issue the **iprsvpsignallinghellorefreshmisses**command without the optional **fast-reroute**keyword, the command applies to Fast Reroute hellos and Fast Reroute capability is enabled by default. This command is provided for backward compatibility; however, we recommend that you use the **iprsvpsignallinghellofast-rerouterefreshmisses**command.

Examples

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down and Fast Reroute is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh misses 5
```

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down and Fast Reroute is enabled by default:

```
Router(config-if)# ip rsvp signalling hello refresh misses 5
```

Related Commands

Command	Description
ip rsvp signalling hello dscp	Sets the DSCP value in hello messages.
ip rsvp signalling hello refresh interval	Sets the refresh interval in hello messages.

ip rsvp signalling hello statistics

To enable Hello statistics on the router, use the **iprsvpsignallinghellostatistics** command in global configuration mode. To disable Hello statistics on the router, use the **no** form of this command.

ip rsvp signalling hello statistics
no ip rsvp signalling hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

In the following example, Hello statistics are enabled on the router:

```
Router(config)# ip rsvp signalling hello statistics
```

Related Commands

Command	Description
clear ip rsvp hello instance statistics	Clears Hello statistics for an instance.
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

ip vrf

To define a VPN routing and forwarding (VRF) instance and to enter VRF configuration mode, use the **ip vrf** command in global configuration mode. To remove a VRF instance, use the **no** form of this command.

ip vrf *vrf-name*
no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	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(14)S	This command was integrated into Cisco IOS 12.2(14)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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

The **ip vrf** *vrf-name* command creates a VRF instance named *vrf-name*. To make the VRF functional, a route distinguisher (RD) must be created using the **rd** *route-distinguisher* command in VRF configuration mode. The **rd** *route-distinguisher* command creates the routing and forwarding tables and associates the RD with the VRF instance named *vrf-name*.

The **ip vrf default** command can be used to configure a VRF instance that is a NULL value until a default VRF name can be configured. This is typically before any VRF related AAA commands are configured.

Examples

The following example shows how to import a route map to a VRF instance named VPN1:

```
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target both 100:2
Router(config-vrf)# route-target import 100:1
```

Related Commands

Command	Description
ip vrf forwarding (interface configuration)	Associates a VRF with an interface or subinterface.
rd	Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.

ip vrf forwarding (interface configuration)

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) instance with an interface or subinterface, use the **ip vrf forwarding** command in interface configuration mode. To disassociate a VRF, use the **no** form of this command.

ip vrf forwarding *vrf-name* [**downstream** *vrf-name2*]
no ip vrf forwarding *vrf-name* [**downstream** *vrf-name2*]

Syntax Description

vrf-name	Associates the interface with the specified VRF.
downstream	(Optional) Enables Half Duplex VRF (HDVRF) functionality on the interface and associates the interface with the downstream VRF.
vrf-name2	(Optional) Associates the interface with the specified downstream VRF.

Command Default

The default for an interface is the global routing table.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(6)	The downstream keyword was added to support MPLS VPN Half-Duplex VRFs.
12.3(11)T	This command was modified. Support was added for interfaces and subinterfaces that are configured with X.25 encapsulation.
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 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to associate an interface with a VRF. Executing this command on an interface removes the IP address. The IP address should be reconfigured. The **downstream** keyword is available on supported platforms with virtual interfaces. The **downstream** keyword associates the interfaces with a downstream VRF, which enables half duplex VRF functionality on the interface. Some functions operate in the upstream VRFs, and others operate in the downstream VRFs. The following functions operate in the downstream VRFs:

- • PPP peer routes are installed in the downstream VRFs.

- Authentication, authorization, and accounting (AAA) per-user routes are installed in the downstream VRFs.
- A Reverse Path Forwarding (RPF) check is performed in the downstream VRFs.

Forwarding Between X.25 Interfaces and Interfaces Configured for MPLS

This command enables IP forwarding between X.25 interfaces and interfaces configured for MPLS, which lets you connect customer premises equipment (CPE) devices to a provider edge (PE) router via an X.25 network by forwarding IP traffic between the CPE devices and the MPLS network. You must configure MPLS on the PE and provider routers in the network.

This command lets you perform an X.25 aggregation function on a PE router for several CPE devices with X.25 VCs into an MPLS network. The PE router performs the aggregation function of terminating X25 VCs and also performs the mapping function (in which VCs are mapped to the appropriate MPLS VRF domains).

Distributed CEF switching, CEF switching, and fast switching are not supported (only process switching is supported). Forwarding of IPv6 traffic is not supported.

Note Configuring IP VRF forwarding on an interface or subinterface that already has an IP address causes that IP address to be deleted from the running configuration. On an X.25 interface or subinterface, it does not cause any existing **x25 map ip** or **x25 pvc ip** statements to be deleted. Configuring an **x25 map ip** or **x25 pvc ip** statement with an IP address that matches an IP address configured on the same interface (or any subinterface of the same interface) might be rejected, even when the conflicting address is in another VRF instance.

For additional references, see CCITT 1988 Recommendation X.25 *(Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit)* , RFC 1356 *(Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode)* , and RFC 1461 *(SNMP MIB extension for Multiprotocol Interconnect over X.25)* .

Examples

The following example shows how to link a VRF to ATM interface 0/0:

```
Router(config)# interface atm0/0
Router(config-if)# ip vrf forwarding vpn1
```

The following example associates the VRF named U with the virtual-template 1 interface and specifies the downstream VRF named D:

```
Router> enable
Router# configure terminal
Router(config)# interface virtual-template 1
Router(config-if)# ip vrf forwarding U downstream D
Router(config-if)# ip unnumbered Loopback1
```

Related Commands

Command	Description
ip route vrf	Establishes static routes for a VRF.
ip vrf	Configures a VRF routing table.

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

ip vrf receive

To insert the IP address of an interface as a connected route entry in a Virtual Private Network (VPN) routing and forwarding instance (VRF) routing table, use the **ip vrf receive** command in interface configuration mode. To remove the connected entry from the VRF routing table, use the **no** form of this command.

ip vrf receive *vrf-name*
no ip vrf receive *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF into which you want to add the IP address of the interface.

Command Default

No IP address of an interface is inserted as connected route entry in a VRF routing table.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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.
12.2SX	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 ip vrf receive command supports VRF route selection for the following features:

- MPLS VPN: VRF Selection Based on Source IP Address
- MPLS VPN: VRF Selection Using Policy-Based Routing

This command is used to install a primary or secondary IP address of an interface as a connected route entry in the VRF routing table. These entries appear as “receive” entries in the Cisco Express Forwarding table. MPLS VPNs require Cisco Express Forwarding switching to make IP destination prefix-based switching decisions. This command can be used to selectively install the interface IP address in the VRF that is specified with the vrf-name argument. Only the local interface IP address is added to the VRF routing table. This command is used on a per-VRF basis. In other words, you must enter this command for each VRF in which you need to insert the IP address of the interface. This command does not remove the interface IP address from the global routing table.

Note This command cannot be used with the ip vrf forward command for the same interface.

VRF Selection Based on Source IP Address Guidelines

The **ip vrf receive** command is automatically disabled when the **no ip vrf** *vrf-name* command is entered for the local interface. An error message is displayed when the **ip vrf receive** command is disabled in this manner.

Interfaces where the VRF Selection Based on Source IP Address feature is enabled can forward packets that have an IP address that corresponds to an IP address entry in the VRF table. If the VRF table does not contain a matching IP address, the packet is dropped, by default, because there is no corresponding “receive” entry in the VRF entry.

VRF Selection Using Policy Based Routing Guidelines

You must enter the **ip policy route-map** command before the **ip vrf receive** command can be enabled. The ip vrf receive command is automatically disabled when either the **no ip policy route-map** *map-name* or the **no ip vrf** *vrf-name* command is entered for the local interface. An error message is displayed when the ip vrf receive command is disabled in this manner. With the VRF Selection Using Policy-Based Routing implementation of the VRF selection feature, a route map filters the VRF routes. If a match and set operation occurs in the route map but there is no receive entry in the local VRF table, the packet is dropped.

Examples

VRF Selection Based on Source IP Address

The following example shows how to configure Ethernet interface 0/2 (172.16.1.3) and insert its IP address in VRF1 and VRF2 with the ip vrf receive command. You must enter the ip vrf select source command on the interface or subinterface to enable VRF selection on the interface or subinterface. You must also enter the vrf selection source command in global configuration mode to populate the VRF selection table and to configure the VRF Selection Based on Source IP Address feature. (The vrf selection source command is not shown in this example.)

```
Router(config)# interface Ethernet0/2
Router(config-if)# ip address 172.16.1.3 255.255.255.255
Router(config-if)# ip vrf select source
Router(config-if)# ip vrf receive VRF1
Router(config-if)# ip vrf receive VRF2
Router(config-if)# end
```

VRF Selection Using Policy-Based Routing

The following example shows how to configure Ethernet interface 0/1 (192.168.1.2) and insert its IP address in VRF1 and VRF2 with the ip vrf receive command. You must configure an access list and a route map to allow the VRF Section Using Policy-Based Routing feature to select a VRF. (The access list and route map configuration are not shown in this example.)

```
Router(config)#  interface Ethernet0/1
Router(config-if)# ip address 192.168.1.2 255.255.255.255
Router(config-if)# ip policy route-map PBR-VRF-SELECTION
Router(config-if)# ip vrf receive VRF1
Router(config-if)# ip vrf receive VRF2
Router(config-if)# end
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip vrf	Configures a VRF routing table.
ip vrf select source	Enables VRF selection on an interface.

Command	Description
set vrf	Enables VRF selection and filtering under a route map.
vrf selection source	Populates a single source IP address, or range of source IP addresses, to a VRF selection table.

ip vrf select source

To enable the VRF Selection feature on a particular interface or subinterface, use the **ip vrf select source** command in interface configuration mode. To disable the VRF Selection feature on a particular interface or subinterface, use the **no** form of this command.

ip vrf select source
no ip vrf select source

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)SZ	This command was integrated into Cisco IOS Release 12.2(14)SZ to support the Cisco 7304 router.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S to support the Cisco 7304 router.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S to support the Cisco 7200 and 7500 series routers.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S to support the Cisco 7200 and 7500 series routers.
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.
12.2SX	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 **ip vrf select source** and the **ip vrf forwarding** commands are mutually exclusive. If the VRF Selection feature is configured on an interface, you cannot configure VRFs (using the **ip vrf forwarding** command) on the same interface.

Examples

The following example shows how to enable the VRF Selection feature on an interface:

```
Router(config-if)# ip vrf select source
```

The following example shows the message you receive after you have deleted the VRF Selection feature on an interface:

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)# interface pos4/0
Router (config-if)# no ip vrf select source
Router (config-if)#
INTERFACE_VRF_SELECT unset for POS4/0, slot: 4
Router (config-if)#
```

The following example shows the message you receive after you have enabled the VRF Selection feature on an interface:

```
Router (config-if)# ip vrf select source
Router (config-if)#
INTERFACE_VRF_SELECT set for POS4/0, slot: 4
Router (config-if)#
```

Related Commands

Command	Description
ip vrf receive	Adds all the IP addresses that are associated with an interface into a VRF table.
vrf selection source	Populates a single source IP address, or range of source IP addresses, to a VRF Selection table.

ip vrf sitemap

To configure Site of Origin (SoO) filtering on an interface, use the **ip vrf sitemap** command in interface configuration mode. To disable SoO filtering on an interface, use the **no** form of this command.

ip vrf sitemap *route-map*
no ip vrf sitemap

Syntax Description

route-map	The name of the route map that is configured with the as-number and network of the VPN site.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the re-advertisement of that prefix back to the source site can be prevented. The SoO extended community attribute uniquely identifies the site from which a PE router has learned a route.

Examples

The following example configures SoO filtering on an interface:

```
Router(config)# route-map Site-of-Origin permit 10
Router(config-route-map)# set extcommunity soo 100:1
Router(config-route-map)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip vrf forwarding RED
Router(config-if)# ip vrf sitemap Site-of-Origin
Router(config-if)# ip address 10.0.0.1 255.255.255.255
Router(config-if)# end
```

Related Commands

Command	Description
ip vrf forwarding	Associates a VRF with an interface or subinterface.

l2 pseudowire routing

To enter Layer 2 pseudowire routing configuration mode, use the **l2 pseudowire routing** command in global configuration mode. To exit Layer 2 pseudowire routing configuration mode, use the **no** form of this command.

l2 pseudowire routing
no l2 pseudowire routing

Syntax Description

This command has no arguments or keywords.

Command Default

Layer 2 pseudowire routing mode is not entered.

Command Modes

Global configuration (config)

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 **l2 pseudowire routing** command enters Layer 2 pseudowire routing configuration mode (config-l2_pw_rtg) from which you can use additional commands such as the **switching-point** command and the **terminating-pe tie-breaker** command. The **switching-point** command and the**terminating-pe tie-breaker** command are used to configure the L2VPN VPLS Inter-AS Option B feature. For more information about the L2VPN VPLS Inter-AS Option B feature, see the *Multiprotocol Label Switching Configuration Guide* .

Examples

The following example enables Layer 2 pseudowire routing configuration mode:

```
Router>
Router# enable
Router(config)# configure terminal
Router(config)# l2 pseudowire routing
Router(config-l2_pw_rtg)# terminating-pe tie-breaker
Router(config-l2_pw_rtg)# end
```

Related Commands

Command	Description
switching-point	Configures a switching point and specifies a VC ID range.
terminating-pe tie-breaker	Negotiates the behavior mode (either active or passive) for a TPE router.

l2 vfi autodiscovery

To enable the Virtual Private LAN Service (VPLS) provider edge (PE) router to automatically discover other PE routers that are part of the same VPLS domain, use the **l2 vfi autodiscovery** command in global configuration mode. To disable VPLS autodiscovery, use the **no** form of this command.

l2 vfi *vfi-name* **autodiscovery**
no l2 vfi *vfi-name* **autodiscovery**

Syntax Description

vfi-name	Specifies the name of the virtual forwarding instance. The virtual forwarding instance (VFI) identifies a group of pseudowires that are associated with a virtual switching instance (VSI).

Command Default

Layer 2 VFI autodiscovery is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

VPLS Autodiscovery enables each VPLS PE router to discover other PE routers that are part of the same VPLS domain. VPLS Autodiscovery also automatically detects when PE routers are added to or removed from the VPLS domain. Beginning with Cisco IOS Release 12.2(33)SRB, you no longer need to manually configure the VPLS neighbors and maintain the configuration when a PE router is added or deleted. However, you can still perform manual VPLS configuration even when you enable VPLS Autodiscovery.

Examples

The following example enables VPLS Autodiscovery on a PE router:

```
l2 vfi vfi2 autodiscovery
```

Related Commands

Command	Description
l2 vfi manual	Manually creates a Layer 2 VFI.

l2 vfi manual

To create a Layer 2 virtual forwarding instance (VFI) and enter Layer 2 VFI manual configuration mode, use the **l2vfimanual** command in global configuration mode. To remove the Layer 2 VFI, use the **no** form of this command.

l2 vfi *name* **manual**
no l2 vfi *name* **manual**

Syntax Description

name	Name of a new or existing Layer 2 VFI .

Command Default

The Layer 2 VFI is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF	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.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

A VFI is a collection of data structures used by the data plane, software-based or hardware-based, to forward packets to one or more virtual circuits (VC). It is populated and updated by both the control plane and the data plane and also serves as the data structure interface between the control plane and the data plane.

Within the Layer 2 VFI manual configuration mode, you can configure the following parameters:

- VPN ID of a Virtual private LAN service (VPLS) domain
- Addresses of other PE routers in this domain
- Type of tunnel signaling and encapsulation mechanism for each peer

Within the Layer 2 VFI manual configuration mode, the following commands are available:

- **vpn id** *vpn-id*
- [**no**] **neighbor***remote-router-id* {**encapsulation** {**l2tpv3** | **mpls**} | **pw-class***pw-name*| **no-split-horizon**}

Examples

This example shows how to create a Layer 2 VFI, enter Layer 2 VFI manual configuration mode, and configure a VPN ID:

```
Router(config)# l2 vfi vfitest1 manual
Router(config-vfi)# vpn id 303
```

Related Commands

Command	Description
l2 vfi point-to-point	Establishes a point-to-point Layer 2 VFI between two separate networks.
vpn id	Configures a VPN ID in RFC 2685 format. You can change the value of the VPN ID only after its configuration, and you cannot remove it.
neighbor	Specifies the type of tunnel signaling and encapsulation mechanism for each peer.

l2 vfi point-to-point

To establish a point-to-point Layer 2 virtual forwarding interface (VFI) between two separate networks, use the **l2 vfi point-to-point** command in global configuration mode. To disable the connection, use the **no** form of this command.

l2 vfi *name* **point-to-point**
no l2 vfi *name* **point-to-point**

Syntax Description

name	Name of the connection between the two networks.

Command Default

Point-to-point Layer 2 virtual forwarding interfaces are not created.

Command Modes

Global configuration (config)

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.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

If you disable L2VPN Pseudowire Switching with the **no l2 vfi point-to-point** command, the virtual circuits (VCs) are deleted.

Examples

The following example establishes a point-to-point Layer 2 VFI:

```
Router(config)# l2 vfi atomvfi point-to-point
```

Related Commands

Command	Description
neighbor (L2VPN Pseudowire Switching)	Establishes the two routers with which to form a connection.

l2vpn

To enter Layer 2 VPN (L2VPN) configuration mode and configure global L2VPN commands, use the **l2vpn** command in global configuration mode. To remove any global L2VPN configurations, use the **no** form of this command.

l2vpn
no l2vpn

Syntax Description

This command has no arguments or keywords.

Command Default

No global L2VPN commands are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support.
15.3(1)S	This command was integrated into Cisco IOS release 15.3(1)S.

Examples

The following example shows how to enter L2VPN configuration mode and configure a Layer 2 router ID:

```
Device(config)# l2vpn
Device(config-l2vpn)# router-id 10.1.1.1
```

l2vpn pseudowire tlv template

To create a template of pseudowire type-length-value (TLV) parameters to be used in a Multiprotocol Label Switching-Transport Profile (MPLS-TP) configuration, use the **l2vpn pseudowire tlv template** command in global configuration mode. To remove the template, use the **no** form of this command.

l2vpn pseudowire tlv template *template-name*
no l2vpn pseudowire tlv template *template-name*

Syntax Description

template-name	Name of the TLV template.

Command Default

Template for pseudowire TLV parameters is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **pseudowire tlv template** in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

This command will replace the **pseudowire tlv template** in future releases.

Examples

The following example shows how to create a TLV template named tlv3:

```
Device(config)# l2vpn pseudowire tlv template tlv3
```

Related Commands

Command	Description
tlv template	Specifies a TLV template to be used as part of local interface configuration.

l2vpn pseudowire static-oam class

To create a Layer 2 VPN (L2VPN) Operation, Administration, and Maintenance (OAM) class and specify the timeout intervals, use the **l2vpn pseudowire static-oam class** command in global configuration mode. To remove the specified class, use the **no** form of this command.

l2vpn pseudowire static-oam class *class-name*
no l2vpn pseudowire static-oam class *class-name*

Syntax Description

class-name	Name of the static pseudowire OAM class.

Command Default

Static pseudowire OAM classes are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **pseudowire-static-oam class** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the **l2vpn pseudowire static-oam class** command to create an OAM class and enter static pseudowire OAM configuration mode, from which you can enter timeout intervals.

Examples

The following example shows how to create a static OAM class named oam-class3 and enter static pseudowire OAM configuration mode:

```
Device(config)# l2vpn pseudowire static-oam class oam-class3
Device(config-st-pw-oam-class)# timeout refresh send 45
```

Related Commands

Command	Description
pseudowire-static-oam class	Creates an OAM class and specifies the timeout intervals
status protocol notification static	Invokes a specified class as part of the static pseudowire.

l2vpn subscriber

To create a Layer 2 VPN (L2VPN) subscriber authorization group and enter L2VPN subscriber group mode, use the **l2vpn subscriber** command in global configuration mode. To remove the L2VPN subscriber authorization group, use the **no** form of this command.

l2vpn subscriber authorization group *group-name*
no l2vpn subscriber authorization group *group-name*

Syntax Description

authorization group *group-name*	Specifies the name of the L2VPN subscriber authorization group.

Command Default

An L2VPN subscriber authorization group is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **l2 subscriber** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the **l2vpn subscriber** command to create a named service authorization group and enter L2VPN subscriber group mode.

Define multiple L2VPN subscriber authorization groups on the router. Each group defines a set of Any Transport over MPLS (AToM) peers using the peer's Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) router ID (IP address or IP address network) and virtual circuit (VC) ID or range. You must be sure to define mutually exclusive service authorization groups.

Use configuration commands available in L2VPN subscriber group mode to enable an AToM or label advertisement to be used for First Sign of Life (FSOL) processing.

When an AToM LDP label advertisement is received and there is a matching group, the Intelligent Services Gateway (ISG) control policy map is executed and the AAA attributes for the corresponding xconnect is downloaded from RADIUS. Thus, a dynamic xconnect is provisioned for the peer provider edge (PE). Use the **show derived-config interface** command to see the details of the xconnect that is downloaded.

To provide a description for the L2VPN subscriber authorization group, use the **description** command in L2VPN subscriber group mode.

Examples

The following example shows how to create a subscriber authorization group:

```
Device(config)# l2vpn subscriber authorization group group1
```

Related Commands

Command	Description
description (l2vpn)	Provides a description of the cross connect in an L2VPN multisegment pseudowire.
l2 subscriber	Creates an L2 subscriber authorization group and enter L2 subscriber group mode.
peer	Defines the target LDP PE peer information.
pseudowire (Layer 2)	Defines the maximum and watermark limits for pseudowires from a peer PE device.
service-policy type control (Layer 2)	Attaches an ISG control service policy to an L2 subscriber authorization group.

l2vpn vfi context

To establish a Layer 2 VPN (L2VPN) virtual forwarding interface (VFI) between two or more separate networks, use the **l2vpn vfi context** command in global configuration mode. To disable the connection, use the **no** form of this command.

l2vpn vfi context *name*
no l2vpn vfi context *name*

Syntax Description

name	Name of the VFI context.

Command Default

L2VPN VFIs are not established.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **l2 vfi** command in future releases.

Usage Guidelines

Use the **l2vpn vfi context** command to establish a VFI for specifying core-facing pseudowires in a Virtual Private LAN Services (VPLS). The VFI represents an emulated LAN or a VPLS forwarder from the VPLS architectural model when using an emulated LAN interface.

Examples

The following example shows how to establish an L2VPN VFI context:

```
Device(config)# l2vpn vfi context vfi1
```

Related Commands

Command	Description
l2 vfi	Establishes an L2 VFI.

l2vpn xconnect context

To create a Layer 2 VPN (L2VPN) cross connect context and enter xconnect configuration mode, use the **l2vpn xconnect context** command in global configuration mode. To remove the connection, use the **no** form of this command.

l2vpn xconnect context *context-name*
no l2vpn xconnect context *context-name*

Syntax Description

context-name	Name of the cross connect context.

Command Default

L2VPN cross connections are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **l2 vfi (point to point)**, **connect (L2VPN local switching)**, and **xconnect** commands in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the **l2vpn xconnect context** command to define a cross connect context that specifies the two members in Virtual Private Wire Service (VPWS)—attachment circuit to pseudowire, pseudowire to pseudowire (multisegment pseudowire), or attachment circuit to attachment circuit (local connection). The type of members specified, attachment circuit interface or pseudowire, automatically define the type of L2VPN service.

Examples

The following example shows how to establish an L2VPN cross connect context:

```
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# interworking ip
```

Related Commands

Command	Description
l2 vfi point to point	Establishes a point-to-point L2 VFI between two separate networks.

label (pseudowire)

To configure an Any Transport over MPLS (AToM) static pseudowire connection by defining local and remote circuit labels, use the **label** command in interface configuration mode. To remove the local and remote pseudowire labels, use the **no** form of this command.

label *local-pseudowire-label remote-pseudowire-label*
no label

Syntax Description

local-pseudowire-label	An unused static label that is within the range defined by the **mpls label range** command.
remote-pseudowire-label	The value of the peer provider edge router's local pseudowire label.

Command Default

Circuit labels are 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 L2VPN command modifications for cross-OS support. This command will replace the **mpls label** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

The **label** command is mandatory when configuring AToM static pseudowires and must be configured at both ends of the connection.

The **label** command checks the validity of the local pseudowire label and generates an error message if the label is invalid.

Examples

The following example shows configuration of an AToM static pseudowire connection on the local device:

```
Device# configure terminal
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# signaling protocol none
Device(config-if)# label 100 150
```

The following example shows configuration of an AToM static pseudowire connection on the remote device:

```
Device# configure terminal
Device(config)# interface pseudowire 200
Device(config-if)# encapsulation mpls
Device(config-if)# signaling protocol none
Device(config-if)# label 150 100
```

Related Commands

Command	Description
control-word (mpls)	Enables the MPLS control word in an AToM dynamic pseudowire connection.
mpls label	Configures an AToM static pseudowire connection by defining local and remote circuit labels.
mpls label range	Configures the range of local labels available for use on packet interfaces.
show l2vpn atom vc	Displays information about AToM VCs and AToM static pseudowires that have been enabled to route Layer 2 packets on a router.

list

To show all or part of the explicit path or paths, use the **list** command in IP explicit path configuration mode.

list [*starting-index-number*]

Syntax Description

starting-index-number	(Optional) Index number at which the explicit path(s) will start to be displayed. The range is 1 to 65535.

Command Default

Explicit paths are not shown.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 example shows how to list the explicit path:

```
Router(cfg-ip-expl-path)# list
Explicit Path name path1:
    1:next-address 10.0.0.1
    2:next-address 10.0.0.2
```

The following example shows how to list the explicit path starting at index number 2:

```
Router(cfg-ip-expl-path)# list 2
Explicit Path name path1:
    2:next-address 10.0.0.2
Router(cfg-ip-expl-path)#
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified 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 command mode for IP explicit paths, and creates or modifies the specified path.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

list (LSP Attributes)

To display the contents of a label switched path (LSP) attribute list, use the **list** command in LSP Attributes configuration mode.

list

Syntax Description

This command has no arguments or keywords.

Command Default

Contents of an LSP attribute list is not displayed.

Command Modes

LSP Attributes configuration (config-lsp-attr)

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.

Usage Guidelines

This command displays the contents of the LSP attribute list. You can display each of the following configurable LSP attributes using the **list** command: affinity, auto-bw, bandwidth, lockdown, priority, protection, and record-route.

Examples

The following example shows how to display the contents of an LSP attribute list identified with the string priority:

```
!
Router(config)# mpls traffic-eng lsp attributes priority
Router(config-lsp-attr)# priority 0 0
Router(config-lsp-attr)# list
 priority 0 0
Router(config-lsp-attr)#
```

Related Commands

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

load-balance flow

To enable load balancing of traffic across multiple core interfaces using equal cost multipaths (ECMP) for Virtual Private LAN Services (VPLS), use the **load-balance flow** command in the appropriate configuration mode. To disable load balancing of VPLS traffic, use the **no** form of this command.

load-balance flow[**ethernet** {**dst-mac** | **src-dst-mac** | **src-mac**}]
no load-balance flow

Syntax Description

ethernet	(Optional) Specifies the Ethernet pseudowire flow classification.
dst-mac	(Optional) Specifies the destination MAC address.
src-dst-mac	(Optional) Specifies the source and destination MAC address.
src-mac	(Optional) Specifies the source MAC address.

Command Default

Load balancing is disabled.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S. Support was added for the Cisco ASR 1000 Series Routers.
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.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

This command enables ECMP load balancing only for the pseudowire for which it was configured.

Examples

The following example shows how to configure a pseudowire and enable flow-based load balancing:

```
Device(config)# pseudowire-class try
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# load-balance flow
```

The following example shows how to configure a pseudowire and enable flow-based load balancing in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# load-balance flow
```

The following example shows how to configure a template and enable flow-based load balancing in template configuration mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# load-balance flow ethernet dst-mac
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
flow-label enable	Enables the imposition and disposition of flow labels.
load-balance flow-label	Enables the use of flow labels to load balance traffic across multiple core interfaces using ECMP for VPLS.

load-balance flow-label

To balance the load based on flow labels, use the **load-balance flow-label** command in pseudowire class configuration mode. To disable flow-label-based load balancing, use the **no** form of this command.

load-balance flow-label {**both** | **receive** | **transmit**}
no load-balance flow-label

Syntax Description

both	Inserts or discards flow labels on transmit or receive.
receive	Discards flow labels on receive.
transmit	Inserts flow labels on transmit.

Command Default

Load-balancing flow labels are disabled.

Command Modes

Pseudowire class configuration (config-pw-class)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Examples

The following example shows how to configure a pseudowire and enable flow-based labels for load balancing:

```
Device(config)# interface pseudowire 1001
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# neighbor 10.1.1.200 200
Device(config-pw-class)# signaling protocol ldp
Device(config-pw-class)# load-balance flow
Device(config-pw-class)# load-balance flow-label both
```

The following example shows how to configure a template and enable flow-based labels for load balancing in template configuration mode:

```
Device(config)# template type pseudowire fatpw
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# load-balance flow
Device(config-pw-class)# load-balance flow-label both
Device(config-pw-class)# end
Device(config)# interface pseudowire 100
Device(config-if)# source template type pseudowire fatpw
Device(config-if)# encapsulation mpls
Device(config-if)# neighbor 10.1.1.1 1
Device(config-if)# signaling protocol ldp
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
flow-label enable	Enables the imposition and disposition of flow labels.

Command	Description
load-balance flow	Enables load balancing of traffic across multiple core interfaces using ECMP for VPLS.

local interface

To specify the pseudowire type when configuring pseudowires in a Mutliprotocol Label Switching Transport Protocol (MPLS-TP) network, use the **local interface** command in virtual forwarding interface (VFI) neighbor configuration mode. This command enters enters VFI neighbor interface configuration mode. To disble the pseudowire type, use the **no** form of this command.

local interface *pseudowire-type*
no local interface *pseudowire-type*

Syntax Description

pseudowire-type	Psuedowire type by its number in hexadecimal format: 01 Frame Relay DLCI (Martini Mode) 02 ATM AAL5 SDU VCC transport 03 ATM transparent cell transport 04 Ethernet Tagged Mode 05 Ethernet 06 HDLC 07 PPP 08 SONET/SDH Circuit Emulation Service Over MPLS 09 ATM n-to-one VCC cell transport 0A ATM n-to-one VPC cell transport 0B IP Layer2 Transport 0C ATM one-to-one VCC Cell Mode 0D ATM one-to-one VPC Cell Mode 0E ATM AAL5 PDU VCC transport 0F Frame-Relay Port mode 10 SONET/SDH Circuit Emulation over Packet 11 Structure-agnostic E1 over Packet 12 Structure-agnostic T1 (DS1) over Packet 13 Structure-agnostic E3 over Packet 14 Structure-agnostic T3 (DS3) over Packet 15 CESoPSN basic mode 16 TDMoIP AAL1 Mode 17 CESoPSN TDM with CAS

Command Default

No pseudowire type is defined.

Command Modes

VFI neighbor configuration

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Usage Guidelines

The VC types 04 and 05 are supported.

Examples

The following example sets the pseudowire VC type to Ethernet and enters VFI neighbor interface configuration mode:

```
Router(config-vfi-neighbor)# local interface 5
R1(config-vfi-neighbor-interface)# tlv mtu 1 4 1500
```

lockdown (LSP Attributes)

To disable reoptimization of the label switched path (LSP), use the **lockdown** command in LSP Attributes configuration mode. To reenable reoptimization, use the **no** form of this command.

lockdown
no lockdown

Syntax Description

This command has no arguments or keywords.

Command Default

Reoptimization of the LSP is enabled.

Command Modes

LSP Attributes configuration (config-lsp-attr)

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.

Usage Guidelines

Use this command to set up in an LSP attribute list the disabling of reoptimization of an LSP triggered by a timer, or the issuance of the **mpls traffic-eng reoptimize** command, or a configuration change that requires the resignalling of an LSP.

To associate the LSP lockdown attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to configure disabling of reoptimization in an LSP attribute list:

```
Configure terminal
!
mpls traffic-eng lsp attributes 4
 bandwidth 1000
 priority 1 1
 lockdown
 end
```

Related Commands

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

logging (MPLS-TP)

To enable the display of Multiprotocol Label Switching (MPLS) transport profile (TP) events, use the **logging** command in MPLS-TP configuration mode. To disable the display of MPLS-TP events, use the **no** form of this command.

logging {**config-change** | **events**}
no logging {**config-change** | **events**}

Syntax Description

config-change	Displays events related to any configuration change to an MPLS-TP tunnel, link, or midpoint label switched path (LSP).
events	Displays events related to any interface or LSP state changes.

Command Default

Logging is not enabled.

Command Modes

MPLS-TP configuration mode (config-mpls-tp)

Command History

Release	Modification
15.1(3)S	This command was introduced.

Usage Guidelines

The following events are captured in the logs:

MPLS-TP Tunnel Down or MPLS-TP Tunnel Up:

```
%MPLS-TP-3-UPDOWN: Tunnel-tp<Tunnel_Num>, changed state to (Up | Down | AdminDown)
%LINK-3-UPDOWN: Interface Tunnel-tp<Tunnel_Num>, changed state to (Up | Down)
%LINK-5-CHANGED: Interface Tunnel-tp<Tunnel_Num>, changed state to administratively down
```

LSP Down or LSP Up:

```
%LSP-3-UPDOWN: (Working | Protect) LSP <LSP_ID> is (Up | Down): <Failure Condition>:<Failure
 Location>
```

Where:

- *LSP_ID* is the complete LSP ID
- *Failure Condition*is AIS, LDI, LKR, CC
- *Failure Location*is an IF ID in the form: [*Global_ID*] *Node_ID*::*IF_Num*

MPLS-TP Tunnel Switchover

```
%MPLS-TP-5-REDUNDANCY: Tunnel-tp<Tunnel_Num> Switched from (Working to Protect | Protect
to Working).
```

LSP Lockout or LSP Lockout Clear

```
%MPLS-TP-5-LOCKOUT: (Working | Protect) LSP <LSP_ID> (Entering | Exiting) Lock Down State
```

MPLS-TP Tunnel End-Point Created/Deleted/Modified

```
%MPLS-TP-5-CONFIG-CHANGED: Tunnel-tp<Tunnel_Num> is (Added | Updated | Deleted)
```

MPLS-TP Mid-Point Created/Deleted/Modified

```
%LSP-5-CONFIG-CHANGED: LSP <LSP_ID> is (Added | Updated | Deleted)
```

MPLS-TP Link Created/Deleted/Modified

```
%MPLS-TP-LINK-5-CONFIG-CHANGED: Link <Link_Num>, Interface <Interface_Name>, NextHop <IP
Address|MAC Address> (Added | Updated | Deleted).
```

Static MPLS Label Range updated

```
%MPLS-LABEL-5-CHANGED: (Static | Dynamic) Min/Max Label: <Min Label>/<Max Label>
```

Examples

The following example enables the display of interface or LSP state changes:

```
Router(config-mpls-tp)# logging events
```

Related Commands

Command	Description
debug mpls tp	Enables the display of MPLS-TP error messages.

logging pseudowire status

To enable system logging (syslog) reporting of pseudowire status events, use the **logging pseudowire status** command in L2VPN configuration mode. To disable syslog reporting of pseudowire status events, use the **no** form of this command.

logging pseudowire status
no logging pseudowire status

Syntax Description

This command has no arguments or keywords.

Command Default

Syslog reporting of pseudowire status events is disabled.

Command Modes

L2VPN configuration (config-l2vpn)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **xconnect logging pseudowire status** 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 enable syslog reporting of pseudowire status events:

```
Device(config)# l2vpn
Device(config-l2vpn)# logging pseudowire status
```

Related Commands

Command	Description
xconnect logging pseudowire status	Enables syslog reporting of pseudowire status events.

logging redundancy

To enable system message log (syslog) reporting of xconnect redundancy status events, use the **logging redundancy** command in L2VPN configuration mode. To disable syslog reporting of xconnect redundancy status events, use the **no** form of this command.

logging redundancy
no logging redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Syslog reporting of the status of the xconnect redundancy group is disabled.

Command Modes

L2VPN configuration (config-l2vpn)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **xconnect logging redundancy** 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 enable syslog reporting of the status of the xconnect redundancy group and shows the messages that are generated during switchover events:

```
Device(config)# l2vpn
Device(config-l2vpn)# logging redundancy
```

Related Commands

Command	Description
xconnect	Binds an Ethernet, 802.1q VLAN, or Frame Relay attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.
xconnect logging redundancy	Enables syslog reporting of the status of the xconnect redundancy group.

match mpls-label through mpls ldp atm control-mode

match cos

To match a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking, use the **matchcos** command in class-map configuration or policy inline configuration mode. To remove a specific Layer 2 CoS/ISL marking as a match criterion, use the **no** form of this command.

match cos cos-value [**cos-value** [**cos-value** [**cos-value**]]]
no match cos cos-value [**cos-value** [**cos-value** [**cos-value**]]]

Syntax Description

Supported Platforms Other Than the Cisco 10000 Series Routers	
cos-value	Specific IEEE 802.1Q/ISL CoS value. The *cos-value* is from 0 to 7; up to four CoS values, separated by a space, can be specified in one **matchcos** statement.
Cisco 10000 Series Routers	Specific packet CoS bit value. Specifies that the packet CoS bit value must match the specified CoS value. The *cos-value* is from 0 to 7; up to four CoS values, separated by a space, can be specified in one **matchcos** statement.
cos-value	

Command Default

Packets are not matched on the basis of a Layer 2 CoS/ISL marking.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.0(25)S	This command was integrated into Cisco IOS Release 12.0(25)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.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
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 integrated into Cisco IOS Release 12.2(33)SRC and support for the Cisco 7600 series routers was added.
12.4(15)T2	This command was integrated into Cisco IOS Release 12.4(15)T2.

Release	Modification
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and support for the Cisco 7300 series router was added.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **service-policytypeperformance-monitorinline**command.

Examples

In the following example, the CoS values of 1, 2, and 3 are successful match criteria for the interface that contains the classification policy named cos:

```
Router(config)# class-map cos
Router(config-cmap)# match cos 1 2 3
```

In the following example, classes named voice and video-n-data are created to classify traffic based on the CoS values. QoS treatment is then given to the appropriate packets in the CoS-based-treatment policy map (in this case, the QoS treatment is priority 64 and bandwidth 512). The service policy configured in this example is attached to all packets leaving Fast Ethernet interface 0/0.1. The service policy can be attached to any interface that supports service policies.

```
Router(config)# class-map voice
Router(config-cmap)# match cos 7
Router(config)# class-map video-n-data
Router(config-cmap)# match cos 5
Router(config)# policy-map cos-based-treatment
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 64
Router(config-pmap-c)# exit
Router(config-pmap)# class video-n-data
Router(config-pmap-c)# bandwidth 512
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet0/0.1
Router(config-if)# service-policy output cos-based-treatment
```

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a CoS value of 2 will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match cos 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Example of the match cos Command for Matching Traffic Classes Inside a 802.1p Domain by CoS values in Cisco IOS Release 12.2(33)SCF

The following example shows how to match traffic classes for the 802.1p domain with packet CoS values:

```
Router> enable
Router# config terminal
Router(config)# class-map cos7
Router(config-cmap)# match cos 2
Router(config-cmap)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
show class-map	Displays all class maps and their matching criteria.

match mpls experimental topmost

To match the experimental (EXP) value in the topmost label header, use the **matchmplsexperimentaltopmost**command in class-map configuration or policy inline configuration mode. To remove the EXP match criterion, use the no form of this command.

match mpls experimental topmost number
no match mpls experimental topmost number

Syntax Description

number	Multiprotocol Label Switching (MPLS) EXP field in the topmost label header. Valid values are 0 to 7.

Command Default

No EXP match criterion is configured for the topmost label header.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

You can enter this command on the input interfaces and the output interfaces. It will match only on MPLS packets.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **service-policytypeperformance-monitorinline**command.

Examples

The following example shows that the EXP value 3 in the topmost label header is matched:

```
Router(config)# class-map mpls exp
Router(config-cmap)# match mpls experimental topmost 3
```

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a EXP value of 3 in the topmost label header will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match mpls experimental topmost 3
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
set mpls experimental topmost	Sets the MPLS EXP field value in the topmost MPLS label header at the input or output interfaces.

match mpls-label

To redistribute routes that include Multiprotocol Label Switching (MPLS) labels if the routes meet the conditions specified in the route map, use the **match mpls-label** command in route-map configuration mode. To disable this function, use the **no** form of this command.

match mpls-label
no match mpls-label

Syntax Description

This command has no arguments or keywords.

Command Default

Routes with MPLS labels are not redistributed.

Command Modes

Route-map configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

A route map that includes this command can be used in the following instances:

- With the **neighbor route-map in** command to manage inbound route maps in BGP
- With the **redistribute bgp** command to redistribute route maps in an IGP

Use the route-map global configuration command, and the **match** and **set** route map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria--the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match route-map**configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command will be ignored; that is, the route will

not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Examples

The following example shows how to create a route map that redistributes routes if the following conditions are met:

- The IP address of the route matches an IP address in access control list 2.
- The route includes an MPLS label.

```
Router(config-router)# route-map incoming permit 10
Router(config-route-map)# match ip address 2
Router(config-route-map)# match mpls-label
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set mpls-label	Enables a route to be distributed with an MPLS label if the route matches the conditions specified in the route map.

maximum routes

To limit the maximum number of routes in a Virtual Private Network (VPN) routing and forwarding (VRF) instance to prevent a provider edge (PE) router from importing too many routes, use the **maximum routes** command in VRF configuration mode or in VRF address family configuration mode. To remove the limit on the maximum number of routes allowed, use the **no** form of this command.

maximum routes *limit* {**warning-only** | *warn-threshold* [**reinstall** *reinstall-threshold*]}
no maximum routes

Syntax Description

limit	The maximum number of routes allowed in a VRF. The range is 1 to 4294967295 routes. All values within this range can be configured for IPv4. For IPv6, however, only values greater than the current number of IPv6 routes present in the Routing Information Base (RIB) for the specified VRF is allowed.
warn-threshold	The warning threshold value expressed as a percentage (from 1 to 100) of the *limit* value. When the number of routes reaches the specified percentage of the limit, a warning message is generated.
warning-only	Issues a system message logging (syslog) error message when the maximum number of routes allowed for a VRF exceeds the threshold. However, additional routes are still allowed.
reinstall *reinstall-threshold*	(Optional) Specifies reinstallation of a route previously rejected because the maximum route limit was exceeded. The *reinstall-threshold* is expressed as a percentage (from 1 to 100) of the *limit* value, but it does not take effect until the limit has been reached. When the number of routes reaches the specified percentage of the limit, a warning message is generated, but routes are still accepted. When the number of routes reaches the limit, the router rejects new routes and does not accept any more until the number of routes drops below the specified percentage of the *reinstall-threshold*.

Command Default

No limit is set on the maximum number of routes allowed.

Command Modes

VRF address family configuration (config-vrf-af)
VRF configuration (config-vrf)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(13)T	Support for Simple Network Management Protocol (SNMP) notifications was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **reinstall** *reinstall-threshold* keyword and argument were added.

Release	Modification
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SRC	Support for this command was added for IPv6 address families under the **vrf definition** command.
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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

All values within the range for the *limit* argument can be configured for IPv4. For IPv6, however, only values greater than the current number of IPv6 routes present in the RIB for the specified VRF is allowed.

The **maximum routes** command can be configured in one of two ways:

- Generate a warning message when the *limit* value is exceeded
- Generate a warning message when the *warn-threshold* value is reached

To limit the number of routes allowed in the VRF, use the **maximum routes** *limit* command with the *warn-threshold* argument. The *warn-threshold* argument generates a warning and does not allow the addition of routes to the VRF when the maximum number set by the *limit* argument is reached. The software generates a warning message every time a route is added to a VRF when the VRF route count is above the warning threshold. The software also generates a route rejection notification when the maximum threshold is reached and every time a route is rejected after the limit is reached.

To set a number of routes at which you receive a notification, but which does not limit the number of routes that can be imported into the VRF, use the **maximum routes** *limit* command with the **warn-only** keyword.

To configure the router to generate SNMP notifications (traps or informs) for these values, use the **snmp-server enable traps mpls vpn** command in global configuration mode.

Examples

The following example shows how to set a limit threshold of VRF routes to 1000. When the number of routes for the VRF reaches 1000, the router issues a syslog error message, but continues to accept new VRF routes.

```
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# maximum routes 1000 warning-only
```

The following example shows how to set the maximum number of VRF routes allowed to 1000 and set the warning threshold at 80 percent of the maximum. When the number of routes for the VRF reaches 800, the router issues a warning message. When the number of routes for the VRF reaches 1000, the router issues a syslog error message and rejects any new routes.

```
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 200:1
Router(config-vrf)# route-target import 200:1
Router(config-vrf)# maximum routes 1000 80
```

The following example shows how to use the **reinstall** keyword to control the maximum number of VRF routes allowed. In this example, the router issues a warning when the number of routes exceeds 800 (80% of 1000 routes), but it still accept routes. When the number of new routes reaches 1000 (the limit), the router rejects them and does not accept more until the number of routes drops below 900 (90% of 1000) installed routes.

```
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 200:1
Router(config-vrf)# route-target import 200:1
Router(config-vrf)# maximum routes 1000 80 reinstall 90
```

The following example for an IPv6 address family defined under the **vrf definition** command shows how to set the maximum number of VRF routes allowed to 500 and set the warning threshold at 50 percent of the maximum. When the number of routes for the VRF reaches 250, the router issues a warning message. When the number of routes for the VRF reaches 500, the router issues a syslog error message and rejects any new routes.

```
Router(config)# vrf definition vrf1
Router(config-vrf)# address-family ipv6
Router(config-vrf-af)# maximum routes 500 50
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
import map	Configures an import route map for a specified VRF for more control over routes imported into the VRF.
ip vrf	Specifies a name for a VRF routing table and enters VRF configuration mode (for IPv4 only).
rd	Creates VRF routing and forwarding tables and specifies the default route distinguisher for a VPN.
route-target	Configures a VRF route target community for importing and exporting extended community attributes.
snmp-server enable traps mpls vpn	Enables the router to send MPLS VPN-specific SNMP notifications (traps and informs).
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

medium p2p

To configures the interface as point-to-point, use the **medium p2p** command in interface configuration mode. To return the interface to its normal mode, use the **no** form of this command.

medium p2p
no medium p2p

Syntax Description

This command has no arguments or keywords.

Command Default

Interfaces are configured to connect to multiple devices.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Usage Guidelines

This command allows the router to send and receive all Multiprotocol Label Switching (MPLS) transport profile (TP) packets using a common multicast MAC address knowing that it is communicating with only one other device.

Examples

The following example configures the interface as point-to-point:

```
Router(config)# interface eth0/0

Router(config-if)# medium p2p
```

Related Commands

Command	Description
mpls tp link	Configures MPLS-TP link parameters.

member (l2vpn vfi)

To specify the devices that form a point-to-point Layer 2 VPN (L2VPN) virtual forwarding interface (VFI) connection, use the **member** command in L2 VFI configuration mode. To disconnect the devices, use the **no** form of this command.

member {*ip-address* [{*vc-id*}] {**encapsulation mpls** | **template** *name*} | **pseudowire** *pw-int-number* [*ip-address* [{*vc-id*}] {**encapsulation mpls** | **template** *name*}]}
no member {*ip-address* [{*vc-id*}] {**encapsulation mpls** | **template** *name*} | **pseudowire** *pw-int-number* [*ip-address* [{*vc-id*}] {**encapsulation mpls** | **template** *name*}]}

Syntax Description

ip-address	IP address of the VFI neighbor.
vc-id	(Optional) Virtual circuit (VC) identifier.
encapsulation mpls	Specifies Multiprotocol Label Switching (MPLS) as the encapsulation type.
template *name*	Specifies the template name.
pseudowire *pw-int-number*	Specifies the pseudowire interface number.

Command Default

Devices that form a point-to-point L2VPN VFI connection are not specified.

Command Modes

L2 VFI configuration (config-vfi)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **neighbor (VPLS)** 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 configure an L2VPN VFI connection:

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# member 10.10.10.10 1 encapsulation mpls
```

Related Commands

Command	Description
neighbor (VPLS)	Specifies the type of tunnel signaling and encapsulation mechanism for each VPLS peer.

member (bridge-domain)

To bind a service instance to a bridge domain instance, use the **member** command in bridge-domain configuration mode. To unbind a service instance from a bridge domain instance, use the **no** form of this command.

member *interface-type-number* **service-instance** *service-id* [**split-horizon group** *group-id*]
no member *interface-type-number* **service-instance** *service-id* [**split-horizon group** *group-id*]

Syntax Description

interface-type-number	Interface type and number. The accepted values are any of the following interfaces support Ethernet Virtual Connection (EVC) service instances: • Physical interface • Port-channel • Mac-tunnel • Overlay interface • Layer 2 virtual forwarding interface (L2 VFI)
service-instance	Configures the service instance.
service-id	Numerical identifier of the service instance. The range is from 1 to 8000.
split-horizon	(Optional) Configures a port or service instance as a member of a split-horizon group.
group	(Optional) Defines the split-horizon group.
group-id	(Optional) Identifier for the split-horizon group. The range is from 1 to 65533. • On the Cisco ASR 1000 Series Routers, the only values supported are **0** and **1**.

Command Default

Service instances are not bound to a bridge domain instance.

Command Modes

Bridge-domain configuration (config-bdomain)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **bridge-domain (service instance)** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use either the **bridge-domain (service instance)** command in service instance configuration mode or the **member** command in bridge-domain configuration mode to configure a bridge domain service. The commands cannot be used in combination for the same bridge domain.

Use the **member** command to bind a service instance to a bridge domain instance. Bridge domains cannot be configured for a service instance without encapsulation also being configured. The **bridge-domain** command configures components on a bridge domain.

When you use the **no** form of this command, a service instance is unbound from a bridge domain instance. However, the service instance and encapsulation configuration are retained.

Examples

The following example shows how to bind a service instance to a bridge domain instance:

```
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# exit
Device(config)# bridge-domain 200
Device(config-bdomain)# member gigabitethernet0/0/0 service-instance 1000 split-horizon
group 0
```

Related Commands

Command	Description
bridge-domain (**config**)	Configures components on a bridge domain.
bridge-domain (service instance)	Binds a service instance or a MAC tunnel to a bridge domain instance.
ethernet evc	Defines an EVC and enters EVC configuration mode.
ethernet service instance	Configures an Ethernet service instance on an interface and enters service instance configuration mode.

member (xconnect)

To specify devices that form a Layer 2 VPN (L2VPN) cross connect, use the **member** command in xconnect configuration mode. To disconnect the devices, use the **no** form of this command.

member *ip-address vc-id* {**encapsulation mpls** | **template** *template-name*} [**group** *group-name* [**priority** *number*]]

Pseudowire Interfaces
member pseudowire *interface-number* [*ip-address vc-id* {**encapsulation mpls** | **template** *template-name*}] [**group** *group-name* [**priority** *number*]]

Gigabit Ethernet and Port-channel Interfaces
member{**gigabitethernet** | **port-channel**} *interface-number*[**service-instance** *id*] [**group** *group-name* [**priority** *number*]]

ATM Interfaces
member atm *interface-number* [{**pvc** {*vpi-value* | *vpi-value/vci-value*} | **pvp** *vpi-value*}] [**group** *group-name* [**priority** *number*]]

POS and CEM Interfaces
member {**pos** *interface-number* | **cem** *interface-number circuit-id*} [**group** *group-name* [**priority** *number*]]

Syntax Description

ip-address	IP address of the peer.
vcid	Specifies the virtual circuit (VC) ID. The range is from 1 to 4294967295.
encapsulation mpls	Specifies Multiprotocol Label Switching (MPLS) as the data encapsulation method.
template *template-name*	(Optional) Specifies the template to be used for encapsulation and protocol configuration. The maximum size is 32 characters.
group *group-name*	(Optional) Specifies the cross-connect member redundancy group name.
priority *number*	(Optional) Specifies the cross-connect member priority. The range is from 0 to 16. The highest priority is 0. Lowest priority is 16.
pseudowire	Specifies pseudowire as the attachment circuit type.
interface-number	Specifies the interface number.
gigabitethernet	Specifies Gigabit Ethernet interface as the attachment circuit type.
port-channel	Specifies port-channel interface as the attachment circuit type.
service-instance *id*	(Optional) Specifies the service instance identifier.
pvc	(Optional) Specifies the ATM permanent virtual circuit (PVC) parameters.

vpi-value	Virtual Path Identifier (VPI) value. The range is from 0 to 255.
vpi-value/vci-value	VPI/virtual circuit identifier (VCI) identifier. The range is from 0 to 255.
pvp	(Optional)Specifies the ATM permanent virtual path (PVP) parameters.
pos *interface-number*	Specifies packet-over-sonet (POS) as the attachment circuit type.
cem *interface-number circuit-id*	Specifies circuit emulation (CEM) as the attachment circuit type.

Command Default

Devices that form an L2VPN cross connect are not specified.

Command Modes

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.

Usage Guidelines

The **member** command specifies the two members of the Virtual Private Wired Service (VPWS), multisegment pseudowire, or local connect services. For VPWS, one member is an attachment circuit and the other member is a pseudowire interface. For a multisegment pseudowire, both members are pseudowire interfaces. For local connect, both members are active interfaces.

When both pseudowire interface and peer information are specified, it dynamically creates the interface using the pseudowire number specified using the **pseudowire** *pw-interface-number* keyword-argument pair.

Configure the group name to specify which of the two possible groups the member belongs to. The group name must be configured if the member has an associated redundant member belonging to a redundant member group. You can also configure the group name even if there are no backup members so that the member can be given an easy-to-understand descriptive name.

Configure a priority for each member so that the active member can be chosen based on the priority when there are multiple redundant members. The default priority for a member is 0 (highest). Each member in the same group must have a unique priority.

There can only be two groups, with a maximum of four members in one group and exactly one member in the other group for redundancy (one member is for active redundancy and the other three are for backup redundancy). If the group name is not specified, only two members can be configured in the L2VPN cross-connect context.

Examples

The following example shows a typical configuration of a Layer 2 cross connect:

```
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# member 10.1.1.1 200 encapsulation mpls
```

Related Commands

Command	Description
connect (l2vpn local switching)	Creates Layer 2 data connections between two ports on the same device.

Command	Description
l2 vfi point-to-point	Establishes a point-to-point Layer 2 VFI between two separate networks.
xconnect	Binds an attachment circuit to a pseudowire and configures an AToM static pseudowire.

metric-style narrow

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

metric-style narrow [**transition**] [{**level-1** | **level-2** | **level-1-2**}]
no metric-style narrow [**transition**] [{**level-1** | **level-2** | **level-1-2**}]

Syntax Description

transition	(Optional) Instructs the router to use both old- and new-style TLVs.
level-1	(Optional) Enables this command on routing level 1.
level-2	(Optional) Enables this command on routing level 2.
level-1-2	(Optional) Enables this command on routing levels 1 and 2.

Command Default

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

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Examples

The following example shows how to configure the router to generate and accept old-style TLVs on router level 1:

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

Related Commands

Command	Description
metric-style transition	Configures a router to generate both old-style and new-style TLVs.

Command	Description
metric-style wide	Configures a router to generate and accept only new-style TLVs.

metric-style transition

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

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

Syntax Description

level-1	(Optional) Enables this command on routing level 1.
level-2	(Optional) Enables this command on routing level 2.
level-1-2	(Optional) Enables this command on routing levels 1 and 2.

Command Default

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

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Examples

The following example shows how to configure a router to generate and accept both old-style and new-style TLVs on router level 2:

```
Router(config-router)# metric-style transition level-2
```

Related Commands

Command	Description
metric-style narrow	Configures a router to generate and accept old-style TLVs.
metric-style wide	Configures a router to generate and accept only new-style TLVs.

metric-style wide

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

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

Syntax Description

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

Command Default

The Multiprotocol Label Switching (MPLS) traffic engineering image generates only old-style TLVs. To do MPLS traffic engineering, new-style TLVs that have wider metric fields must be generated.

Command Modes

Router configuration (config-router)

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 train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

Command	Description
metric-style narrow	Configures a router to generate and accept old-style TLVs.
metric-style transition	Configures a router to generate and accept both old-style and new-style TLVs.

mls ipv6 vrf

To enable IPv6 globally in a virtual routing and forwarding (VRF) instance, use the mls ipv6 vrf command in global configuration mode. To remove this functionality, use the no form of the command.

mls ipv6 vrf
no mls ipv6 vrf

Syntax Description

This command has no arguments or keywords.

Command Default

VRFs are supported only for IPv4 addresses.

Command Modes

Global configuration

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 and implemented on the Catalyst 6500 series switches.

Usage Guidelines

You must enable the mls ipv6 vrf command in global configuration mode in order to enable IPv6 in a VRF. If this command is not used, a VRF is supported only for the IPv4 address family.

Configuring the mls ipv6 vrf command makes the router reserve the lower 255 hardware IDs for IPv6 regardless of whether IPv6 is enabled. Other applications that make use of these hardware IDs then cannot use that space.

To remove the **mls ipv6 vrf** command from the running configuration, the user needs to remove all IPv6 VRFs from the router and reload the system.

Examples

The following example shows how to enable IPv6 in a VRF globally:

```
Router(config)# mls ipv6 vrf
```

Related Commands

Command	Description
vrf definition	Configure a VRF routing table instance and enters VRF configuration mode.
show running-config vrf	Displays the subset of the running configuration of a router that is linked to a specific VRF instance or to all VRFs configured on the router.

mls mpls

To enable Multiprotocol Label Switching (MPLS) recirculation, use the **mls mpls** command in global configuration mode. To disable MPLS recirculation, use the **no** form of this command.

mls mpls {**recir-agg** | **tunnel-recir**}
no mls mpls {**recir-agg** | **tunnel-recir**}

Syntax Description

recir-agg	Recirculates the MPLS aggregated-label packets (only new aggregated labels are impacted).
tunnel-recir	Recirculates the tunnel-MPLS packets.

Command Default

MPLS recirculation is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17b)SXA	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

If you do not enable tunnel-MPLS recirculation, the IPv4 and IPv4-tunneled packets that have to be labeled (for example, the packets that are encapsulated with an MPLS header) will be corrupted when they are transmitted from the Cisco 7600 series router.

Use the **mls mpls recir-agg** command to switch off the VPN-CAM use for the VRF lookups and to allocate the reserved VLAN for every VRF instance configured on the Cisco 7600 series routers. This command is a pre-requisite to ensure that the egress features (ACL, Netflow, or QoS) work properly in scenarios where a VRF route is reachable through a static global route through a non-VRF interface.

Examples

The following example shows how to enable aggregated-label MPLS recirculation:

```
Router(config)# mls mpls recir-agg
```

The following example shows how to enable tunnel-MPLS recirculation:

```
Router(config)# mls mpls tunnel-recir
```

The following example shows how to disable aggregated-label MPLS recirculation:

```
Router(config)# no mls mpls recir-agg
```

The following example shows how to disable tunnel-MPLS recirculation:

```
Router(config)# no mls mpls tunnel-recir
```

mls mpls (guaranteed bandwidth traffic engineering)

To configure the guaranteed bandwidth traffic engineering flow parameters globally, use the **mls mpls** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls mpls {**gb-te-burst** *burst* | **gb-te-cir-ratio** *ratio* | **gb-te-dscp** *dscp-value* [**markdown**] | **gb-te-enable** [**global-pool**]}
no mls mpls {**gb-te-burst** *burst* | **gb-te-cir-ratio** *ratio* | **gb-te-dscp** *dscp-value* [**markdown**] | **gb-te-enable** [**global-pool**]}

Syntax Description

gb-te-burst *burst*	Specifies the burst duration for the guaranteed bandwidth traffic engineering flows; the range is 100 to 30000 milliseconds.
gb-te-cir-ratio *ratio*	Specifies the ratio for the committed information rate policing; the range is 1 to 100 percent.
gb-te-dscp *dscp-value*	Specifies the differentiated services code point (DSCP) map for the guaranteed bandwidth traffic engineering flows; the range is 0 to 63.
markdown	(Optional) Marks down or drops the nonconforming flows.
gb-te-enable	Enables the guaranteed bandwidth traffic engineering flow policing.
global-pool	(Optional) Specifies using resources allocated from the global pool to the police traffic engineering flows.

Command Default

The default settings are as follows:

- *burst* is 1000 milliseconds.
- *ratio* is 1 percent.
- *dscp-value* is 40.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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.

Usage Guidelines

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

Use the **mls qos map dscp-exp** command to reset the Exp value of the Multiprotocol Label Switching (MPLS) packet when the out-label gets swapped.

If you do not enable tunnel-MPLS recirculation, the IPv4 and IPv4-tunneled packets that need to be labeled (for example, the packets that are encapsulated with an MPLS header) will be corrupted when they are transmitted from the Cisco 7600 series router.

Use the **show erm statistics** command to display the Forwarding Information Base (FIB) Ternary Content Addressable Memory (TCAM) exception status for IPv4, IPv6, and MPLS protocols.

Examples

This example shows how to specify the burst duration for the guaranteed bandwidth traffic engineering flows:

```
Router(config)# mls mpls gb-te-burst 2000
Router(config)#
```

This example shows how to specify the ratio for CIR policing:

```
Router(config)# mls mpls gb-te-ratio 30
Router(config)#
```

This example shows how to specify the DSCP map for the guaranteed bandwidth traffic engineering flows and to drop the nonconforming flows:

```
Router(config)# mls mpls gb-te-dscp 25 markdown
Router(config)#
```

This example shows how to enable the guaranteed bandwidth traffic engineering flow policing:

```
Router(config)# mls mpls gb-te-enable
Router(config)#
```

Related Commands

Command	Description
show erm statistics	Displays the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

mls mpls (recirculation)

To enable Multiprotocol Label Switching (MPLS) recirculation, use the **mls mpls** command in global configuration mode. To disable MPLS recirculation, use the **no** form of this command.

mls mpls {**recir-agg** | **tunnel-recir**}
no mls mpls {**recir-agg** | **tunnel-recir**}

Syntax Description

recir-agg	Recirculates the MPLS aggregated-label packets (new aggregated labels are impacted only).
tunnel-recir	Recirculates the tunnel-MPLS packets.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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.

Usage Guidelines

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

Use the **mls mpls tunnel-recirc** command and keyword combination to enable tunnel-MPLS recirculation to avoid packet corruption when any IPv6 or IPv4 payload is tunneled on a Cisco 7600 series router.

Use the **show erm statistics** command to display the Forwarding Information Base (FIB) Ternary Content Addressable Memory (TCAM) exception status for IPv4, IPv6, and MPLS protocols.

Examples

This example shows how to enable the aggregated-label MPLS recirculation:

```
Router(config)# mls mpls recir-agg
Router(config)#
```

This example shows how to enable the tunnel-MPLS recirculation:

```
Router(config)# mls mpls tunnel-recir
Router(config)#
```

This example shows how to disable the aggregated-label MPLS recirculation:

```
Router(config)# no mls mpls recir-agg
Router(config)#
```

This example shows how to disable the tunnel-MPLS recirculation:

```
Router(config)# no mls mpls tunnel-recir
Router(config)#
```

Related Commands

Command	Description
show erm statistics	Displays the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

mls mpls qos input uniform-mode

To enable Multiprotocol Label Switching (MPLS) quality of service (QoS) marking of ingress packets to be copied into the differentiated services code point (DSCP) field of the ingress packet, use the **mls mpls qos input uniform-mode** command in interface configuration mode. To disable the copying operation, use the **no** form of this command.

mls mpls qos input uniform-mode
no mls mpls qos input uniform-mode

Syntax Description

This command has no arguments or keywords.

Command Default

No marking operation is performed on the incoming packets or the GRE headers.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

This command is supported only in PFC3C mode or PFC3CXL mode.

Enter the **show mls qos** command to verify the configuration.

Examples

The following example shows how to enable the original QoS marking of ingress packets to be copied into the DSCP field and copied in the GRE header:

```
Router(config-if)# mls mpls qos input uniform-mode
```

Related Commands

Command	Description
show mls qos	Displays MLS QoS information.

monitor event-trace (EXEC)

To monitor and control the event trace function for a specified Cisco IOS software subsystem component, use the **monitor event-trace** command in privileged EXEC mode.

monitor event-trace *facility* {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] [**WORD**] | **enable** | **one-shot**}

Syntax Description

facility	Name of the Cisco IOS software subsystem component that is the subject of the event trace. To get a list of components that support event tracing, use the **monitor event-trace ?** command. The facility may consist of multiple keywords (for example, **monitor event-trace atom event** ...).
clear	Clears existing trace messages from the memory on the networking device.
continuous	Continuously displays the latest event trace entries.
disable	Disables event tracing for the specified component.
dump	Writes the event trace results to the file configured using the **monitor event-trace** command in global configuration mode. The trace messages are saved in binary format.
pretty	(Optional) Saves the event trace message in ASCII format.
WORD	URL to store event data.
enable	Enables event tracing.
one-shot	Clears any existing trace information from memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the **monitor event-trace** command in global configuration mode.

Command Default

Event trace monitoring is disabled.

Command Modes

Privileged EXEC (#)

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 in Cisco IOS Release 15.3(1)S.
15.3(2)S	This command was integrated in Cisco IOS Release 15.3(2)S.
Cisco IOS XE Release 3.9S	This command was integrated in Cisco IOS XE Release 3.9S.

Usage Guidelines

Use the **monitor event-trace** command to control what, when, and how event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the **monitor event-trace** command in global configuration mode.

Note The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace** command in global configuration mode for each instance of a trace.

The Cisco IOS software allows for the subsystem components to define whether support for event tracing is enabled or disabled at boot time. You can enable or disable event tracing in two ways: using the **monitor event-trace** command in privileged EXEC mode or using the **monitor event-trace**command in global configuration mode. To disable event tracing, you would enter either of these commands with the **disable** keyword. To enable event tracing again, you would enter either of these commands with the **enable** keyword.

To determine whether you can enable event tracing on a subsystem, use the **monitor event-trace ?** command to get a list of software components that support event tracing. To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace** command to display trace messages.

Use the **show monitor event-trace** command to display trace messages. Use the **monitor event-trace** *facility* **dump** command to save trace message information for a single event. By default, trace information is saved in binary format. If you want to save trace messages in ASCII format, for additional application processing, use the **monitor event-trace** *facility* **dump pretty** command.

To write the trace messages for all events that are currently enabled on a networking device to a file, enter the **monitor event-trace dump** command.

To configure the file to which you want to save trace information, use the **monitor event-trace** command in global configuration mode. The trace messages are saved in a binary format.

Examples

The following example shows the privileged EXEC commands to stop event tracing, clear the current contents of memory, and reenable the trace function for the interprocess communication (IPC) component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Device# monitor event-trace ipc disable

Device# monitor event-trace ipc clear

Device# monitor event-trace ipc enable
```

The following example shows how the **monitor event-trace one-shot** command accomplishes the same function as the previous example except in one command. In this example, once the size of the trace message file has been exceeded, the trace is terminated.

```
Device# monitor event-trace ipc one-shot
```

The following example shows the command for writing trace messages for an event in binary format. In this example, the trace messages for the IPC component are written to a file.

```
Device# monitor event-trace ipc dump
```

The following example shows the command for writing trace messages for an event in ASCII format. In this example, the trace messages for the MBUS component are written to a file.

```
Device# monitor event-trace mbus dump pretty
```

Catalyst 6500 Series Switches and Cisco 7600 Series Routers Examples Only

This example shows how to stop event tracing, clear the current contents of memory, and reenable the trace function for the SPA component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Device# monitor event-trace spa disable

Device# monitor event-trace spa clear

Device# monitor event-trace spa enable
```

Related Commands

Command	Description
monitor event-trace (global)	Configures event tracing for a specified Cisco software subsystem component.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.
show monitor event-trace	Displays event trace messages for Cisco software subsystem components.

monitor event-trace (global)

To configure event tracing for a specified Cisco IOS software subsystem component, use the **monitor event-trace** command in global configuration mode.

monitor event-trace *facility* [{**dump-file** *WORD* | {**exclude** | **include**} *subset1* [*subset2* **. . .**] | **size** *numbers* | **stacktrace** [*depth*]}]

Syntax Description

facility	Name of the Cisco IOS software subsystem component that is the subject of the event trace. To get a list of components that support event tracing, use the **monitor event-trace ?** command. The facility may consist of multiple keywords (for example, **monitor event-trace atom event** ...).
disable	Disables event tracing for the specified component.
dump-file *WORD*	Specifies the file where event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.
exclude *subset1* [*subset2...]*	Excludes a subset of debug types.
include *subset1* [*subset2...]*	Includes a subset of debug types.
size *numbers*	Sets the number of messages that can be written to memory for a single instance of a trace. Valid values are from1 to 65536. Note that some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace** *component* **parameters** command. When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
stacktrace*[depth]*	Enables the stack trace at tracepoints and specifies the depth of the stack trace stored. Valid values are from 1 to 16.

Command Default

Event tracing is enabled or disabled depending on the software component.

Command Modes

Global configuration (config)

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 in Cisco IOS Release 15.3(1)S.

Release	Modification
15.3(2)S	This command was integrated in Cisco IOS Release 15.3(2)S.
Cisco IOS XE Release 3.9S	This command was integrated in Cisco IOS XE Release 3.9S.

Usage Guidelines

Use the **monitor event-trace** command to enable or disable event tracing and to configure event trace parameters for Cisco IOS software subsystem components.

Note Event tracing is intended for use as a software diagnostic tool and should be configured only under the direction of a Technical Assistance Center (TAC) representative. In Cisco IOS software images that do not provide subsystem support for the event trace function, the **monitor event-trace** command is not available.

The Cisco IOS software allows the subsystem components to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default two ways: using the **monitor event-trace** command in privileged EXEC mode or using the **monitor event-trace** command in global configuration mode.

Additionally, default settings do not show up in the configuration file. If the subsystem software enables event tracing by default, the **monitor event-trace** *component* **enable** command does not show up in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem creates a command entry in the configuration file.

Note The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace** command for each instance of a trace.

To determine whether you can enable event tracing on a subsystem, use the **monitor event-trace ?** command to get a list of software components that support event tracing.

To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace** command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

Examples

The following example shows how to enable event tracing for the interprocess communication (IPC) subsystem component in Cisco IOS software and configure the size to 4096 messages. The trace messages file is set to ipc-dump in slot0 (flash memory).

```
Device> configure terminal
Device# monitor event-trace ipc enable

Device# monitor event-trace ipc dump-file slot0:ipc-dump

Device# monitor event-trace ipc size 4096
```

When you select Cisco Express Forwarding as the component for which to enable event tracing, you can use the following additional arguments and keywords: **monitor event-trace cef** [**events** | **interface** | **ipv6** | **ipv4**] [**all**]

The following example shows how to enable event tracing for IPv4 or IPv6 events of the Cisco Express Forwarding component in Cisco IOS software:

```
Device> configure terminal
Device# monitor event-trace cef ipv4 enable

Device> configure terminal
Device# monitor event-trace cef ipv6 enable
```

The following example shows what happens when you try to enable event tracing for a component (in this case, adjacency events) when it is already enabled:

```
Device> configure terminal
Device# monitor event-trace adjacency enable
%EVENT_TRACE-6-ENABLE: Trace already enabled.
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls the event trace function for a specified Cisco IOS software subsystem component.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.
show monitor event-trace	Displays event trace messages for Cisco software subsystem components.

monitor peer bfd

To enable pseudowire fast-failure detection capability in a bidirectional forwarding detection (BFD) configuration, use the **monitor peer bfd** command in the appropriate configuration mode. To disable pseudowire fast-failure detection, use the **no** form of this command.

monitor peer bfd [**local interface** *interface-type*]
no monitor peer bfd [**local interface**]

Syntax Description

local interface *interface-type*	(Optional) Specifies the local interface for the source address to use when locating a BFD configuration.

Command Default

Pseudowire fast-failure detection is disabled.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into a release prior to Cisco IOS XE Release 3.6S.
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.

Examples

The following example shows how to enable pseudowire fast-failure detection capability:

```
Device(config)# interface Loopback0
Device(config-if)# ip address 10.1.1.1 255.255.255.255
Device(config-if)# exit
Device(config)# pseudowire-class mpls
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# monitor peer bfd local interface Loopback0
```

The following example shows how to enable pseudowire fast-failure detection capability in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# monitor peer bfd local interface gigabitethernet0/0/0
```

The following example shows how to enable pseudowire fast-failure detection capability in template configuration mode:

```
Device(config)# template type pseudowire 1
Device(config-template)# encapsulation mpls
Device(config-template)# monitor peer bfd local interface gigabitethernet0/0/0
```

Related Commands

Command	Description
bfd map	Configures a BFD map that associates timers and authentication with multihop templates.
bfd-template	Creates a BFD template and enters BFD configuration mode.
encapsulation (Any Transport over MPLS)	Configures the AAL encapsulation for AToM.
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
pseudowire-class	Specifies the name of a Layer 2 pseudowire class.

mpls atm control-vc

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm control-vc** command is not available in Cisco IOS software.

To configure the control-VC virtual path identifier (VPI) and virtual circuit identifier (VCI) values for the initial link to the Multiprotocol Label Switching (MPLS) peer, use the **mpls atm control-vc** command in interface configuration mode. To unconfigure the values, use the **no** form of this command.

mpls atm control-vc *vpi vci*
no mpls atm control-vc *vpi vci*

Syntax Description

vpi	Virtual path identifier, in the range of 0 to 4095.
vci	Virtual circuit identifier, in the range of 0 to 65535.

Command Default

0/32

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology. The VPI range of values was extended to 4095.
12.4(20)T	This command was removed.

Usage Guidelines

Use this command to establish the LDP session and to carry non-IP traffic. The default VPI VCI for the control VC is (0, 32). If for any reason you need to have a different control-VC, use the **mpls atm control-vc** command to configure any VPI VCI allowed by the vpi and vci arguments for the control VC.

Examples

The following example shows how to create an MPLS subinterface on a router and select VPI 1 and VCI 34 as the control VC:

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# mpls ip
Router(config-if)# mpls atm control-vc 1 34
```

Related Commands

Command	Description
mpls ip (interface)	Enables label switching of IPv4 packets on an interface.

mpls atm cos

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm cos** command is not available in Cisco IOS software.

To change the configured bandwidth allocation for class of service (CoS), use the **mpls atm cos** command in global configuration mode.

mpls atm cos {**available** | **standard** | **premium** | **control**} *weight*

Syntax Description

available	The weight for the available class. This is the lowest class priority.
standard	The weight for the standard class. This is the next lowest class priority.
premium	The weight for the premium class. This is the next highest class priority.
control	The weight for the control class. This is the highest class priority.
weight	The total weight for all CoS traffic classes. The range is 0 to 100.

Command Default

Available 50%, control 50%

Command Modes

Global configuration (config)

Command History

Release	Modifications
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology.
12.4(20)T	This command was removed.

Examples

The following example shows how to configure the XTagATM interface for CoS traffic:

```
Router(config)# interface xtagatm12
Router(config-if)# extended-port atm1/0 descriptor 1.2
Router(config-if)# mpls ip
Router(config-if)# mpls atm cos available 49
Router(config-if)# mpls atm cos standard 50
Router(config-if)# mpls atm cos premium 0
Router(config-if)# mpls atm cos control 1
```

mpls atm disable-headend-vc

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm disable-headend-vc** command is not available in Cisco IOS software.

To remove all headend virtual circuits (VCs) from the Multiprotocol Label Switching (MPLS) Label Switch Controller (LSC) and disable its ability to function as an edge label switch router (LSR), use the **mpls atm disable-headend-vc** command in global configuration mode. To restore the headend VCs of the MPLS LSC and restore full edge LSR functionality, use the **no** form of this command.

mpls atm disable-headend-vc
no mpls atm disable-headend-vc

Syntax Description

This command has no arguments or keywords.

Command Default

Edge LSR is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)DC	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology.
12.4(20)T	This command was removed.

Usage Guidelines

This command prevents the LSC from initiating headend label VCs (LVCs), and thus reduces the number of LVCs used in the network.

Examples

The following example shows how to disable the MPLS LSC from acting like an edge LSR and therefore cannot create headend LVCs:

```
mpls atm disable-headend-vc
```

mpls atm multi-vc

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm multi-vc** command is not available in Cisco IOS software.

To configure a router subinterface to create one or more label virtual circuits (VCs) over which packets of different classes are sent, use the **mpls atm multi-vc** command in ATM subinterface submode. To remove the label virtual circuits, use the **no** form of this command.

mpls atm multi-vc
no mpls atm multi-vc

Syntax Description

This command has no arguments or keywords.

Command Modes

ATM subinterface submode (config-subif)

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.
12.4(20)T	This command was removed.

Usage Guidelines

This command is valid only on ATM MPLS subinterfaces.

Examples

The following example shows how to configure interface ATM2/0/0.1 on the networking device for MPLS quality of service (QoS) multi-VC mode:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ATM2/0/0.1 mpls

Router(config-subif)# mpls atm multi-vc
Router(config-subif)# exit
Router(config)# exit
```

Related Commands

Command	Description
mpls cos-map	Creates a class map that specifies how classes map to label virtual circuits when they are combined with a prefix map.

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

mpls atm vpi

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm vpi** command is not available in Cisco IOS software.

To configure the range of values to use in the virtual path identifier (VPI) field for label virtual circuits (LVCs), use the **mpls atm vpi** command in interface configuration mode. To clear the range of values, use the **no** form of this command.

mpls atm vpi *vpi*[{*-high*}][{**vci-range** *low-high*}]
no mpls atm vpi *vpi*[{*-high*}][{**vci-range** *low-high*}]

Syntax Description

vpi	Virtual path identifier, low end of range (0 to 4095).
- vpi	(Optional) Virtual path identifier, high end of range (0 to 4095).
vci-range *low - high*	(Optional) Range of virtual channel identifier (VCI) values the subinterface can use for the VPI(s).

Command Default

The default VPI range is 1-1.

The default VCI range is 33-65535.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology. The **vci-range** keyword was added. The VPI range of values was extended to 4095.
12.4(20)T	This command was removed.

Usage Guidelines

You might need to change the default VPI range on the switch if:

- It is an administrative policy to use a VPI value other than 1, the default VPI.
- There are many LVCs on an interface.

To configure ATM MPLS on a router interface (for example, an ATM Interface Processor), you must enable an MPLS subinterface.

Note The **mpls atm control-vc** and the **mpls atm vpi** subinterface level configuration commands are available on any interface that can support ATM labeling.

Use this command to select an alternate range of VPI values for ATM label assignment on this interface. The two ends of the link negotiate a range defined by the intersection of the range configured at each end.

- To configure the VPI range for an edge label switch router (edge LSR) subinterface connected to another router or to an LSC, limit the range to four VPIs.
- For an ATM-LSR, the VPI range specified must lie within the range that was configured on the ATM switch for the corresponding ATM switch interface.
- If the LDP neighbor is a router, the VPI range can be no larger than two. For example, you can specify from 5 to 6 (a range of two), not 5 to 7 (a range of three). If the LDP neighbor is a switch, the maximum VPI range is 0 to 255.

If you use the **vci-range** keyword, you must specify a VPI value.

Examples

The following example shows how to create a subinterface and selects a VPI range from VPI 1 to VPI 3:

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# mpls ip
Router(config-if)# mpls atm vpi 1-3
```

The following example shows how to create a subinterface with a VPI of 240 and a VCI range between 33 and 4090:

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# mpls ip
Router(config-if)# mpls atm vpi 240 vci-range 33-4090
```

Related Commands

Command	Description
mpls atm control-vc	Configures VPI and VCI values for the initial link to an MPLS peer.

mpls atm vp-tunnel

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm vp-tunnel** command is not available in Cisco IOS software.

To specify an interface or a subinterface as a virtual path (VP) tunnel, use the **mpls atm vp-tunnel** command in interface configuration mode. To remove the VP tunnel from an interface or subinterface, use the **no** form of this command.

mpls atm vp-tunnel *vpi*[{**vci-range** *low-high*}]
no mpls atm vp-tunnel *vpi*[{**vci-range** *low-high*}]

Syntax Description

vpi	Virtual path identifier (VPI) value for the local end of the tunnel (0 to 4095).
vci-range *low-high*	(Optional) Range of virtual channel identifier (VCI) values the VP tunnel can use.

Command Default

If you do not specify a VCI range for the VP tunnel, the tunnel uses the default VCI range of 33-65535.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) terminology. The **vci-range** keyword was added. The VPI range of values was extended to 4095.
12.4(20)T	This command was removed.

Usage Guidelines

The **mpls atm vp-tunnel** and the **mpls atm vpi** commands are mutually exclusive.

This command is available on both extended MPLS ATM (XTagATM) interfaces and on LC-ATM subinterfaces of router ATM interfaces. The command is not available on the LS1010, where all subinterfaces are automatically VP tunnels.

It is not necessary to use the **mpls atm vp-tunnel** command on an XTagATM interface in most applications. The switch learns (through VSI interface discovery) whether the XTagATM interface is a tunnel, the VPI value of the tunnel, and tunnel status.

Examples

The following example shows how to create an MPLS subinterface VP tunnel with a VPI value of 4:

```
Router(config-if)# mpls atm vp-tunnel 4
```

The following example shows how to create a VP tunnel with a value of 240 and a VCI range of 33 to 4090:

```
Router(config-if)# mpls atm vp-tunnel 240 vci-range 33-4090
```

mpls bgp forwarding

To enable an interface to receive Multiprotocol Label Switching (MPLS) packets when the signaling of MPLS labels is through the use of the Border Gateway Protocol (BGP), use the **mpls bgp forwarding** command in interface configuration mode. To disable this configuration, use the **no** form of this command.

mpls bgp forwarding
no mpls bgp forwarding

Syntax Description

This command has no arguments or keywords.

Command Default

MPLS forwarding by BGP is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(29)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)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

Use the **mpls bgp forwarding** command when you want to enable MPLS forwarding on directly connected loopback interfaces. This command is automatically generated by BGP for directly connected nonloopback neighbors.

Examples

The following example shows how to configure BGP to enable MPLS forwarding on a directly connected loopback interface, Ethernet 0/0:

```
interface ethernet 0/0
 mpls bgp forwarding
```

Related Commands

Command	Description
ip vrf forwarding	Associates a VRF with an interface or subinterface.

mpls control-word

To enable the Multiprotocol Label Switching (MPLS) control word in an Any Transport over MPLS (AToM) static pseudowire connection, use the**mpls control-word** command in xconnect configuration mode. To disable the control word, use the **no** form of this command.

mpls control-word
no mpls control-word

Syntax Description

This command has no arguments or keywords.

Command Default

The control word is included in connections.

Command Modes

Xconnect configuration

Command History

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

Usage Guidelines

This command is used when configuring AToM static pseudowires, and is mandatory when configuring Frame Relay data-link connection identifier (DLCI) and ATM adaptation layer 5 (AAL5) attachment circuits.

Because the control word is included by default, it may be necessary to explicitly disable this command in AToM static pseudowire configurations.

When the **mpls control-word** command is used in static pseudowire configurations, the command must be configured the same way on both ends of the connection to work correctly, or else the provider edge routers will not be able to exchange control messages to negotiate inclusion or exclusion of the control word.

Examples

The following example shows the configuration for both sides of an AToM static pseudowire connection:

```
Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# xconnect 10.131.191.251 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 100 150
Router(config-if-xconn)# no mpls control-word
Router(config-if-xconn)# exit
Router(config-if)# exit
Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# xconnect 10.132.192.252 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 150 100
Router(config-if-xconn)# no mpls control-word
Router(config-if-xconn)# exit
Router(config-if)# exit
```

Related Commands

Command	Description
mpls label	Configures an AToM static pseudowire connection by defining local and remote pseudowire labels.
mpls label range	Configures the range of local labels available for use on packet interfaces.
show mpls l2transport vc	Displays information about AToM VCs and AToM static pseudowires that have been enabled to route Layer 2 packets on a router.
xconnect	Binds an attachment circuit to a pseudowire, and configures an AToM static pseudowire.

mpls cos-map

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

To create a class map that specifies how classes map to label virtual circuits (VCs) when they are combined with a prefix map, use the **mpls cos-map** command in global configuration mode.

mpls cos-map *cos-map*

Syntax Description

cos-map	Number from 1 to 155 that identifies the class map.

Command Default

No class maps are specified.

Command Modes

Global configuration (config)

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.
12.4(20)T	This command was removed.

Examples

The following example shows how to create a class map:

```
Router(config)# mpls cos-map 55
Router(config-mpls-cos-map)# class 1 premium
Router(config-mpls-cos-map)# exit
Router(config)#
```

Related Commands

Command	Description
mpls cos-map	Displays the QoS map used to assign a quantity of label virtual circuits and the associated class of service for those label virtual circuits.

mpls experimental

To configure Multiprotocol Label Switching (MPLS) experimental (EXP) levels for a virtual circuit (VC) class that can be assigned to a VC bundle and thus applied to all VC members of that bundle, use the **mplsexperimental**command in VC-class configuration mode. To remove the MPLS EXP levels from the VC class, use the **no** form of this command.

To configure the MPLS EXP levels for a VC member of a bundle, use the **mplsexperimental**command in bundle-vc configuration mode. To remove the MPLS EXP levels from the VC, use the **no** form of this command.

mpls experimental [{**other***range*}]
no mpls experimental

Syntax Description

other	(Optional) Specifies any MPLS EXP levels in the range from 0 to 7 that are not explicitly configured. This is the default.
range	(Optional) A single MPLS EXP level specified as a number from 0 to 7, or a range of levels, specified as a hyphenated range.

Command Default

Defaults to **other**, that is, any MPLS EXP levels in the range from 0 to 7 that are not explicitly configured.

Command Modes

VC-class configuration for a VC class (config-vc-class)
Bundle-vc configuration for ATM VC bundle members (config-if-atm-member)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(26)S	This command was implemented on the Cisco 10000 series router.
12.0(29)S	This command was integrated into Cisco IOS Release 12.0(29)S.
12.2(16)BC	This command was implemented on the ESR-PRE2.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Usage Guidelines

Assignment of MPLS EXP levels to VC bundle members allows you to create differentiated service because you can distribute the MPLS EXP levels over the different VC bundle members. You can map a single level or a range of levels to each discrete VC in the bundle, thereby enabling VCs in the bundle to carry packets marked with different levels. Alternatively, you can configure a VC with the **mplsexperimentalother** command to indicate that it can carry traffic marked with levels not specifically configured for it. Only one VC in the bundle can be configured with the **mplsexperimentalother** command to carry all levels not specified. This VC is considered the default one.

To use this command in VC-class configuration mode, enter the **vc-classatm** global configuration command before you enter this command. This command has no effect if the VC class that contains the command is attached to a standalone VC, that is, if the VC is not a bundle member.

To use this command to configure an individual bundle member in bundle-VC configuration mode, first enter the **bundle** command to enact bundle configuration mode for the bundle to which you want to add or modify the VC member to be configured. Then use the **pvc-bundle** command to specify the VC to be created or modified and enter bundle-VC configuration mode.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next highest MPLS EXP level):

- VC configuration in bundle-VC mode
- Bundle configuration in bundle mode (with the effect of assigned VC class configuration)
- Subinterface configuration in subinterface mode

Note If you are using an ATM interface, you must configure all MPLS EXP levels (ranging from 0 to 7) for the bundle. For this configuration, Cisco recommends configuring one member of the bundle with the **mplsexperimentalother** command. The **other** keyword defaults to any MPLS EXP level in a range from 0 to 7 that is not explicitly configured.

Examples

The following example configures a class named control-class that includes an **mplsexperimental**command that, when applied to a bundle, configures all VC members of that bundle to carry MPLS EXP level 7 traffic. Note that VC members of that bundle can be individually configured with the **mplsexperimental**command at the bundle-vc level, which would supervene.

```
vc-class atm control-class
 mpls experimental 7
```

The following example configures a permanent virtual circuit (PVC) 401, named control-class, to carry traffic with MPLS EXP levels in the range of 4 to 2, overriding the level mapping set for the VC through VC-class configuration:

```
pvc-bundle control-class 401
 mpls experimental 4-2
```

Related Commands

Command	Description
bump	Configures the bumping rules for a VC class that can be assigned to a VC bundle.
bundle	Creates a bundle or modifies an existing bundle, and enters bundle configuration mode.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
protect	Configures a VC class with protected group or protected VC status for application to a VC bundle member.
pvc-bundle	Adds a VC to a bundle as a member and enters bundle-VC configuration mode to configure that VC bundle member.
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.

Command	Description
vbr-nrt	Configures the VBR-nrt QoS and specifies the output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.
vc-class atm	Creates a VC class for an ATM PVC, SVC, or ATM interface, and enters VC-class configuration mode.

mpls export interval

To configure the collection and export of Multiprotocol Label Switching (MPLS) Prefix/Application/Label (PAL) information to a NetFlow collector, use the **mpls export interval** command in global configuration mode. To disable the collecting and exporting of the MPLS PAL information, use the **no** form of this command.

mpls export interval *minutes*
no mpls export interval

Syntax Description

minutes	Time interval, in minutes, between full MPLS PAL table exports. The range is 0 to 10080.

Command Default

No capture or export of PAL table entries is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
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.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **mpls export interval** command to configure the collection and export of MPLS PAL information to a NetFlow collector. The collector can be the Cisco NetFlow Collection Engine or a third-party collector application.

The *minutes*argument specifies the number of minutes between one export of the entire MPLS PAL table and the next export of the entire table. We recommend that you select a time interval from 360 minutes (6 hours) to 1440 minutes (24 hours) depending on the size of your network. If you want to trigger an immediate export of the PAL table, disable the functionality (**no mpls export interval** command) and reconfigure the command with the *minutes* argument greater than zero.

If you enter the command with a periodic interval of zero, entries of the MPLS PAL table are not exported repeatedly, but PAL label tracking still occurs and PAL information is exported to the collector when a label is allocated. To display the entire MPLS PAL table, use the **show mpls flow mappings** command.

The *minutes* argument that you specify is the least amount of time that passes before another export of the MPLS PAL table. The system might choose to delay the MPLS PAL table export, if the PAL export queue already contains a large number of entries. This might occur if the export queue contains tens of thousands of entries, for example, if the export occurred at a time when thousands of routes just came up, or if NetFlow did not have the time to clear the export queue from either a previous export of the full table or a previous time when thousands of routes came up in a brief period.

Examples

The following example shows how to configure a time interval of 720 minutes (12 hours) between exports of the entire MPLS PAL table to a NetFlow collector:

```
Router> enable
Router# configure terminal
Router(config)# mpls export interval 720
Router(config)# exit
```

Related Commands

Command	Description
mpls export vpnv4 prefixes	Configures the tracking and export of VPNv4 label information from the MPLS PAL table to a NetFlow collector.
show mpls flow mappings	Displays all entries in the MPLS PAL table.

mpls export vpnv4 prefixes

To configure the tracking and export of VPN IPv4 (VPNv4) label information from the Multiprotocol Label Switching (MPLS) Prefix/Application/Label (PAL) table to a NetFlow collector, use the **mpls export vpnv4 prefixes** command in global configuration mode. To disable the tracking and exporting of VPNv4 label information, use the **no** form of this command.

mpls export vpnv4 prefixes
no mpls export vpnv4 prefixes

Syntax Description

This command has no arguments or keywords.

Command Default

VPNv4 labels are exported from the MPLS PAL table with a destination prefix of 0.0.0.0.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
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.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **mpls export vpnv4 prefixes** command to enable the tracking and export of VPNv4 label information from the MPLS PAL table.

In MPLS PAL table records, the default prefix stored for labels allocated by VPNs, Border Gateway Protocol (BGP) IPv4, or BGP VPNv4 is intentionally 0.0.0.0 because VPN prefixes may be reused; other VPNs may use the same prefix.

If you configure the **mpls export vpnv4 prefixes** command, the MPLS PAL table stores the VPN prefix and its associated route distinguisher (RD). The use of an RD removes any ambiguity among VPN prefixes. Even if IP addresses are reused, the addition of an RD creates a unique prefix.

Examples

The following example shows how to configure the tracking and exporting of VPNv4 label information from the MPLS PAL table to a NetFlow collector:

```
Router> enable
Router# configure terminal
Router(config)# mpls export interval 720
Router(config)# mpls export vpnv4 prefixes
Router(config)# exit
```

The full MPLS PAL table with MPLS VPNv4 label information is configured to export to the NetFlow collector every 720 minutes (12 hours).

Related Commands

Command	Description
mpls export interval	Configures the collection and export of MPLS PAL information to a NetFlow collector.
show mpls flow mappings	Displays all entries in the MPLS PAL table.

mpls forwarding bgp

To enable Multiprotocol Label Switching (MPLS) nonstop forwarding on an interface that uses Border Gateway Protocol (BGP) as the label distribution protocol, use the **mpls forwarding bgp** command in interface configuration mode. To disable MPLS nonstop forwarding on the interface, use the **no** form of this command.

mpls forwarding bgp
no mpls forwarding bgp

Syntax Description

This command has no arguments or keywords.

Command Default

MPLS nonstop forwarding is not enabled on the interface.

Command Modes

Interface configuration

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 router.
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

Configure this command on the interfaces of the BGP peers that send and receive labels. If this command is not configured on an interface and a stateful switchover occurs, packets received from an interface are dropped until the BGP session is established in the new route processor.

Issue this command to enable nonstop forwarding on interfaces that use BGP to distribute labels for the following types of VPNs:

- MPLS VPN--Carrier Supporting Carrier--IPv4 BGP Label Distribution
- MPLS VPN--Inter-AS--IPv4 BGP Label Distribution

Examples

In the following examples, an interface is configured to save BGP labels in the event of a stateful switchover:

Cisco 7000 Series Example

```
Router(config)# interface Pos1/0
Router(config-if)# mpls forwarding bgp
```

Cisco 10000 Series Example

```
Router(config)# interface Pos1/0/0
Router(config-if)# mpls forwarding bgp
```

Related Commands

Command	Description
bgp graceful-restart	Enables BGP Graceful Restart on the router.

mpls ip (global configuration)

To enable Multiprotocol Label Switching (MPLS) forwarding of IPv4 packets along normally routed paths for the platform, use the **mpls ip** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ip
no mpls ip

Syntax Description

This command has no arguments or keywords.

Command Default

Label switching of IPv4 packets along normally routed paths is enabled for the platform.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
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.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

MPLS forwarding of IPv4 packets along normally routed paths (sometimes called dynamic label switching) is enabled by this command. For a given interface to perform dynamic label switching, this switching function must be enabled for the interface and for the platform.

The **no** form of this command stops dynamic label switching for all platform interfaces regardless of the interface configuration; it also stops distribution of labels for dynamic label switching. However, the no form of this command does not affect the sending of labeled packets through label switch path (LSP) tunnels.

For an LC-ATM interface, the **no** form of this command prevents the establishment of label virtual circuits (LVCs) originating at, terminating at, or passing through the platform.

Examples

The following example shows that dynamic label switching is disabled for the platform, and all label distribution is terminated for the platform:

```
Router(config)# no mpls ip
```

Related Commands

Command	Description
mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for the associated interface.

mpls ip (interface configuration)

To enable Multiprotocol Label Switching (MPLS) forwarding of IPv4 packets along normally routed paths for a particular interface, use the **mpls ip** command in interface configuration mode. To disable this configuration, use the **no** form of this command.

mpls ip
no mpls ip

Syntax Description

This command has no arguments or keywords.

Command Default

MPLS forwarding of IPv4 packets along normally routed paths for the interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
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)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

MPLS forwarding of IPv4 packets along normally routed paths is sometimes called dynamic label switching. If dynamic label switching has been enabled for the platform when this command is issued on an interface, label distribution for the interface begins with the periodic transmission of neighbor discovery Hello messages on the interface. When the outgoing label for a destination routed through the interface is known, packets for the destination are labeled with that outgoing label and forwarded through the interface.

The **no** form of this command causes packets routed out through the interface to be sent unlabeled; this form of the command also terminates label distribution for the interface. However, the no form of the command does not affect the sending of labeled packets through any link-state packet (LSP) tunnels that might use the interface.

For an LC-ATM interface, the **no** form of this command prevents the establishment of label virtual circuits (LVCs) beginning at, terminating at, or passing through the interface.

Examples

The following example shows how to enable label switching on the specified Ethernet interface:

```
Router(config)# configure terminal
Router(config-if)# interface e0/2
Router(config-if)# mpls ip
```

The following example shows that label switching is enabled on the specified vlan interface (SVI) on a Cisco ASR 901 series router:

```
Router(config)# configure terminal
Router(config-if)# interface vlan 1
Router(config-if)# mpls ip
```

Related Commands

Command	Description
mpls ldp maxhops	Limits the number of hops permitted in an LSP established by the downstream on demand method of label distribution.
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.

mpls ip default-route

To enable the distribution of labels associated with the IP default route, use the **mpls ip default-route** command in global configuration mode.

mpls ip default-route

Syntax Description

This command has no arguments or keywords.

Command Default

No distribution of labels for the IP default route.

Command Modes

Global configuration

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was modified to reflect new Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) terminology.
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

Dynamic label switching (that is, distribution of labels based on routing protocols) must be enabled before you can use the **mpls ip default-route** command.

Examples

The following example shows how to enable the distribution of labels associated with the IP default route:

```
Router# configure terminal
Router(config)# mpls ip
Router(config)# mpls ip default-route
```

Related Commands

Command	Description
mpls ip (global configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform.
mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.

mpls ip encapsulate explicit-null

To encapsulate all packets forwarded from the interface or subinterface with an explicit NULL label header, use the **mpls ip encapsulate explicit-null** command in interface configuration or subinterface configuration mode. To disable this function, use the **no** form of this command.

mpls ip encapsulate explicit-null
no mpls ip encapsulate explicit-null

Syntax Description

This command has no arguments or keywords.

Command Default

Packets are sent out without an explicit NULL label header.

Command Modes

Interface configuration
Subinterface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This is a per-interface command. The command establishes an explicit NULL LSP at the customer edge (CE) router. If MPLS is configured on a router and you enter this command, an error message occurs. This command is also supported on the Cisco 2600 series and Cisco 3600 series platforms.

Examples

The following example shows how to encapsulate all packets forwarded onto the interface or subinterface with an explicit NULL label header:

```
Router(config-if)# mpls ip encapsulate explicit-null
```

mpls ip propagate-ttl

To control the generation of the time-to-live (TTL) field in the Multiprotocol Label Switching (MPLS) header when labels are first added to an IP packet, use the **mpls ip propagate-ttl** command in global configuration mode. To use a fixed TTL value (255) for the first label of the IP packet, use the **no** form of this command.

mpls ip propagate-ttl
no mpls ip propagate-ttl [{**forwarded** | **local**}]

Syntax Description

forwarded	(Optional) Prevents the **traceroute** command from showing the hops for forwarded packets.
local	(Optional) Prevents the **traceroute** command from showing the hops only for local packets.

Command Default

This command is enabled. The TTL field is copied from the IP header. A traceroute command shows all of the hops in the network.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.1(5)T	The keywords **forwarded** and **local** were added to this command.
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

By default, the **mpls ip propagate-ttl** command is enabled and the IP TTL value is copied to the MPLS TTL field during label imposition. To disable TTL propagation for all packets, use the **no mpls ip propagate-ttl** command. To disable TTL propagation for only forwarded packets, use the **no mpls ip propagate forwarded** command. Disabling TTL propagation of forwarded packets allows the structure of the MPLS network to be hidden from customers, but not the provider.

This feature supports the IETF draft document ICMP Extensions for Multiprotocol Label Switching, draft-ietf-mpls-label-icmp-01.txt. The document can be accessed at the following URL:

http://www2.ietf.org/internet-drafts/draft-ietf-mpls-label-icmp-01.txt

Examples

The following example shows how to disable the TTL field in the MPLS header for only forwarded packets:

```
Router(config)# no mpls ip propagate-ttl forwarded
```

Related Commands

Command	Description
traceroute	Displays the routes that packets take through a network to their destinations.

mpls ip ttl-expiration pop

To specify how a packet with an expired time-to-live (TTL) value is forwarded, use the **mpls ip ttl-expiration pop** command in global configuration mode. To disable this function, use the **no** form of this command.

mpls ip ttl-expiration pop *labels*
no mpls ip ttl-expiration pop *labels*

Syntax Description

labels	The maximum number of labels in the packet necessary for the packet to be forwarded by means of the global IP routing table.

Command Default

The packets are forwarded by the original label stack. However, in previous versions of Cisco IOS software, the packets were forwarded by the global routing table by default.

12.0S	Packets are forwarded through the use of the global routing table.
12.0ST	Packets are forwarded through the use of the original label stack.
12.1T	Packets are forwarded through the use of the original label stack.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
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

You can specify that the packet be forwarded by the global IP routing table or by the packet's original label stack. The forwarding method is determined by the number of labels in the packet. You specify the number of labels as part of the command. If the packet contains the same or fewer labels than you specified, it is forwarded through the use of the global IP routing table. If the packet contains more labels than you specified, the packet is forwarded through the use of the original label stack.

This command is useful if expired TTL packets do not get back to their source, because there is a break in the Interior Gateway Protocol (IGP) path. Currently, MPLS forwards the expired TTL packets by reimposing the original label stack and forwarding the packet to the end of a label switched path (LSP). (For provider edge routers forwarding traffic over a Virtual Private Network (VPN), this is the only way to get the packet back to the source.) If there is a break in the IGP path to the end of the LSP, the packet never reaches its source.

If packets have a single label, that label is usually a global address or terminal VPN label. Those packets can be forwarded through the use of the global IP routing table. Packets that have more than one label can be forwarded through the use of the original label stack. Enter the **mpls ip ttl-expiration pop 1** command to enable forwarding based on more than one label. (This is the most common application of the command.)

Examples

The following example shows how to enable forwarding based on more than one label:

```
Router(config)# mpls ip ttl-expiration pop 1
```

Related Commands

Command	Description
traceroute	Displays the routes that packets take through a network to their destinations.

mpls ipv6 source-interface

Note Effective with Cisco IOS Release 12.2(25)S, the **mpls ipv6 source-interface** command is not available in Cisco IOS 12.2S releases. Effective with Cisco IOS Release 12.4(15)T, the **mpls ipv6 source-interface** command is not available in Cisco IOS 12.4T releases.

To specify an IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over a Multiprotocol Label Switching (MPLS) network, use the **mpls ipv6 source-interface** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ipv6 source-interface *type number*
no mpls ipv6 source-interface

Syntax Description

type number	The interface type and number whose IPv6 address is to be used as the source for locally generated IPv6 packets to be sent over an MPLS backbone. **Note** A space between the *type* and *number* arguments is not required.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(20)S	This command was integrated into Cisco IOS Release 12.2(20)S.
12.2(25)S	This command was removed from Cisco IOS Release 12.2(25)S.
12.4(15)T	This command was removed from Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **mpls ipv6 source-interface** command with the **neighbor send-label** address family configuration command to allow IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers, configured to run both IPv4 and IPv6, forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).

The **mpls ipv6 source-interface** command was removed from Cisco IOS software as per RFC 3484, which defines how the source address of a locally generated packet must be chosen. This command will be removed from the other Cisco IOS release trains in which it currently appears.

Examples

The following example shows loopback interface 0 being configured as a source address for locally generated IPv6 packets :

```
interface Loopback0
 ip address 192.168.99.5 255.255.255.255
 ipv6 address 2001:0DB8::1/32
!
mpls ipv6 source-interface loopback0
```

Related Commands

Command	Description
neighbor send-label	Advertises the capability of the router to send MPLS labels with BGP routes.

mpls l2transport route

To enable routing of Any Transport over MPLS (AToM) packets over a specified virtual circuit (VC), use the **mpls l2transport route** command in the appropriate command mode. To delete the VC, use the **no** form of this command on both provider edge (PE) routers.

mpls l2transport route *destination vc-id*
no mpls l2transport route *destination vc-id*

Syntax Description

destination	Specifies the Label Distribution Protocol (LDP) IP address of the remote PE router.
vc-id	Assigns a VC number to the virtual circuit between two PE routers.

Command Default

Routing of MPLS packets over a specified VC is disabled.

Command Modes

Depending on the AToM transport type you are configuring, you use the **mpls l2transport route** command in one of the following command modes:

Transport Type	Command Mode
ATM AAL5 and cell relay	ATM VC configuration mode
Ethernet VLAN	Subinterface or interface configuration mode
Frame Relay	Connect submode
HDLC and PPP	Interface configuration mode

Command History

Release	Modification
12.1(8a)E	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(14)SX	This command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
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.

Usage Guidelines

A Multiprotocol Label Switching (MPLS) VC runs across an MPLS cloud to connect interfaces on two PE routers.

Use this command on each PE router to route packets across the MPLS cloud to the interface of the other PE router. Specify the LDP IP address of the other PE router for the destination parameter. Do not specify the IP address of the router from which you are issuing the command.

You can choose any number for the VC ID. However, the VC ID must be unique per pair of routers. Therefore, in large networks, it may be necessary to track the VC ID assignments to ensure that a VC ID does not get assigned twice.

Cisco 7600 Series Routers

Cisco 7600 series routers equipped with a Supervisor Engine 2 must be equipped with either an optical services module (OSM) or a FlexWAN port adapter that is facing the MPLS network with a Layer 2 Ethernet port (non-OSM) facing the customer.

The **mpls l2transport route** command enables the virtual connection used to route the VLAN packets. The types of virtual connections used are as follows:

- VC Type 4--Allows all the traffic in a VLAN to use a single VC across the MPLS network.
- VC Type 5--Allows all traffic on a port to share a single VC across the MPLS network.

During the VC setup, VC type 5 is advertised. If the peer advertises VC type 4, the VC type is changed to type 4 and the VC is restarted. The change only happens from type 5 to type 4 and never from type 4 to type 5.

An MPLS VLAN virtual circuit in Layer 2 runs across an MPLS cloud to connect the VLAN interfaces on two PE routers.

Use the mpls l2transport route command on the VLAN interface of each PE router to route the VLAN packets in Layer 2 across the MPLS cloud to the VLAN interface of the other PE router. Specify the IP address of the other PE router for the destination parameter. Do not specify the IP address of the router from which you are issuing the command.

You can choose any value for the virtual-connection ID. However, the virtual-circuit ID must be unique to each virtual connection. In large networks, you may need to track the virtual-connection ID assignments to ensure that a virtual-connection ID does not get assigned twice.

The routed virtual connections are supported on the main interfaces, not subinterfaces.

Examples

The following examples show how to enable routing of MPLS packets over a specified VC. Two routers named PE1 and PE2 establish a VC to transport packets. PE1 has IP address 172.16.0.1, and PE2 has IP address 192.168.0.1. The VC ID is 50.

ATM AAL5 over MPLS Example

At PE1, enter the following commands:

```
PE1_Router(config)# interface atm5/0.100
PE1_Router(config-if)# pvc ½00
PE1_Router(config-atm-vc)# encapsulation aal5
PE1_Router(config-atm-vc)# mpls l2transport route
 192.168.0.1 50
```

At PE2, enter the following commands:

```
PE2_Router(config)# interface atm5/0.100
PE2_Router(config-if)# pvc ½00
PE2_Router(config-atm-vc)# encapsulation aal5
PE2_Router(config-atm-vc)# mpls l2transport route 172.16.0.1 50
```

ATM Cell Relay over MPLS Example

At PE1, enter the following commands:

```
PE1_Router(config)# interface atm5/0.100
PE1_Router(config-if)# pvc ½00 l2transport
PE1_Router(config-atm-vc)# encapsulation aal0
PE1_Router(config-atm-vc)# mpls l2transport route
 192.168.0.1 50
```

At PE2, enter the following commands:

```
PE2_Router(config)# interface atm5/0.100
PE2_Router(config-if)# pvc ½00 l2transport
PE2_Router(config-atm-vc)# encapsulation aal0
PE2_Router(config-atm-vc)# mpls l2transport route 172.16.0.1 50
```

Ethernet over MPLS Example

At PE1, enter the following commands:

```
PE1_Router(config)# interface GigabitEthernet1/0.2
PE1_Router(config-subif)# encapsulation dot1Q 200
PE1_Router(config-subif)# mpls l2transport route 192.168.0.1 50
```

At PE2, enter the following commands:

```
PE2_Router(config)# interface GigabitEthernet2/0.1
PE2_Router(config-subif)# encapsulation dot1Q 200
PE2_Router(config-subif)# mpls l2transport route 172.16.0.1 50
```

Frame Relay over MPLS Example

At PE1, enter the following commands:

```
PE1_Router(config)# connect frompls1 Serial5/0 1000 l2transport
PE1_Router(config-fr-pw-switching)# mpls l2transport route 192.168.0.1 50
```

At PE2, enter the following commands:

```
PE2_Router(config)# connect frompls2 Serial2/0 102 l2transport
PE2_Router(config-fr-pw-switching)# mpls l2transport route 172.16.0.1 50
```

HDLC over MPLS Example

At PE1, enter the following commands:

```
PE1_Router(config)# interface Serial3/0
PE1_Router(config-if)# encapsulation hdlc
PE1_Router(config-if)# mpls l2transport route 192.168.0.1 50
```

At PE2, enter the following commands:

```
PE2_Router(config)# interface Serial1/0
PE2_Router(config-if)# encapsulation hdlc
PE2_Router(config-if)# mpls l2transport route 172.16.0.1 50
```

PPP over MPLS Example

At PE1, enter the following commands:

```
PE1_Router(config)# interface Serial3/0
PE1_Router(config-if)# encapsulation ppp
PE1_Router(config-if)# mpls l2transport route 192.168.0.1 50
```

At PE2, enter the following commands:

```
PE2_Router(config)# interface Serial1/0
PE2_Router(config-if)# encapsulation ppp
PE2_Router(config-if)# mpls l2transport route 172.16.0.1 50
```

Related Commands

Command	Description
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

mpls label

To configure an Any Transport over MPLS (AToM) static pseudowire connection by defining local and remote circuit labels, use the **mpls label** command in xconnect configuration mode. To remove the local and remote pseudowire labels, use the **no** form of this command.

mpls label *local-pseudowire-label remote-pseudowire-label*
no mpls label

Syntax Description

local-pseudowire-label	An unused static label that is within the range defined by the **mpls label range** command.
remote-pseudowire-label	The value of the peer provider edge router's local pseudowire label.

Command Default

No default labels.

Command Modes

Xconnect configuration

Command History

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

Usage Guidelines

This command is mandatory when configuring AToM static pseudowires, and must be configured at both ends of the connection.

The **mpls label** command checks the validity of the local pseudowire label and will generate an error message if the label is invalid.

Examples

The following example shows configurations for both ends of an AToM static pseudowire connection:

```
Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# no ip address
Router(config-if)# xconnect 10.131.191.251 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 100 150
Router(config-if-xconn)# exit
Router(config-if)# exit
Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# no ip address
Router(config-if)# xconnect 10.132.192.252 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 150 100
Router(config-if-xconn)# exit
Router(config-if)# exit
```

Related Commands

Command	Description
mpls control-word	Enables sending the MPLS control word in an AToM static pseudowire connection.

Command	Description
mpls label range	Configures the range of local labels available for use on packet interfaces.
show mpls l2transport vc	Displays information about AToM VCs and AToM static pseudowires that have been enabled to route Layer 2 packets on a router.
xconnect	Binds an attachment circuit to a pseudowire, and configures an AToM static pseudowire.

mpls label mode

To configure per virtual routing and forwarding (VRF) labels, use the **mpls label mode** command in global configuration mode. To disable the configuration, use the **no** form of this command.

mpls label mode {**vrf** *vrf-name* | **all-vrfs**} **protocol bgp-vpnv4** {**per-prefix** | **per-vrf** | **per-ce** | **vrf-conn-aggr**}
no mpls label mode {**vrf** *vrf-name* | **all-vrfs**} **protocol bgp-vpnv4** {**per-prefix** | **per-vrf** | **per-ce** | **vrf-conn-aggr**}

Syntax Description

vrf	Configures a single VPN routing and forwarding (VRF) domain.
vrf-name	Name for the single VRF to configure.
all-vrfs	Configures a label mode for all VRFs on the router.
protocol	Specifies a protocol to use for the label mode.
bgp-vpnv4	Specifies the IPv4 VRF address-family protocol for the label mode configuration.
per-prefix	Specifies per-prefix label mode.
per-vrf	Specifies per-VRF label mode.
per-ce	Specifies per-CE label mode.
vrf-conn-aggr	Specifies per-VRF label mode for connected and Border Gateway Protocol (BGP) aggregates in the VRF.

Command Default

Per-vrf label mode is the default for connected routes and BGP aggregate routes on the Cisco 6500 routers. Per-prefix label mode is the default for all other local routes.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **vrf-conn-aggr** keyword was added.
Cisco IOS XE Release 3.10S	This command was modified. The **per-ce** keyword was added.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Examples

The following example shows how to configure all VRFs to per-vrf label mode:

```
Device> enable
Device# configure terminal
Device(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
```

Examples

The following example shows how to configure per-ce label mode:

```
Device> enable
Device# configure terminal
Device(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-ce
```

Related Commands

Command	Description
debug ip bgp vpn4 unicast	Displays debugging messages for VPNv4 unicast routes.
show ip vrf detail	Displays the assigned label mode for the VRF.
show mpls forwarding-table	Displays the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB).

mpls label mode (6VPE)

To configure the MPLS VPN 6VPE per VRF Label feature, use the **mpls label mode** command in global configuration mode. To disable the MPLS VPN 6VPE per VRF Label feature, use the **no** form of this command.

mpls label mode {**vrf** *vrf-name* | **all-vrfs**} **protocol** {**bgp-vpnv6** | **all-afs**} {**per-prefix** | **per-vrf**}
no mpls label mode {**vrf** *vrf-name* | **all-vrfs**} **protocol** {**bgp-vpnv6** | **all-afs**} {**per-prefix** | **per-vrf**}

Syntax Description

vrf *vrf-name*	Configures a single VPN routing and forwarding (VRF) domain. • *vrf-name*- --The name for the single VRF you want to configure.
all-vrfs	Configures a label mode for all VRFs on the router.
protocol	Specifies a protocol to use for the label mode. • **bgp-vpnv6** --Specifies the IPv6 VRF address-family protocol for the label mode configuration. • **all-afs** --Configures a label mode for all address families (AFs) on the router. • If a VRF is configured with the **all-afs** label mode, you cannot change the label mode for individual AFs. To configure each of the AFs for different label modes, you must first remove the **all-afs** mode keyword. Similarly, if individual AFs are configured with different label modes, the **all-afs** label mode for the VRF is not accepted. • The **all-afs** label mode keyword has higher precedence over the individual AF label mode keywords (**vrf** or **all-vrfs**).
per-prefix	Specifies per-prefix label mode.
per-vrf	Specifies per-vrf label mode.

Command Default

The command default for connected routes and Border Gateway Protocol (BGP) aggregate routes on the Cisco 7600 router is **Per-vrf-aggr** label mode. The command default for all other local routes is **Per-prefix** label mode.

Command Modes

Global configuration (config)#

Command History

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

Examples

The following example configures all VRFs to per-vrf mode:

```
Router(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
```

Related Commands

Command	Description
debug ip bgp vpnv6 unicast	Displays debugging messages for VPNv6 unicast routes.
show vrf detail	Displays the assigned label mode for the VRF.

mpls label protocol (global configuration)

To specify the Label Distribution Protocol (LDP) for a platform, use the **mpls label protocol** command in global configuration mode. To restore the default LDP, use the **no** form of this command.

mpls label protocol {**ldp** | **tdp**}
no mpls label protocol

Syntax Description

ldp	Specifies that LDP is the default label distribution protocol.
tdp	Specifies that Tag Distribution Protocol (TDP) is the default label distribution protocol.

Command Default

LDP is the default label distribution protocol.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4(3)	The command default changed from TDP to LDP.
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.

Release	Modification
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

If neither the global mpls label protocol ldp command nor the interface mpls label protocol ldp command is used, all label distribution sessions use LDP.

Note Use caution when upgrading the image on a router that uses TDP. Ensure that the TDP sessions are established when the new image is loaded. You can accomplish this by issuing the global configuration command **mpls label protocol tdp**. Issue this command and save it to the startup configuration before loading the new image. Alternatively, you can enter the command and save the running configuration immediately after loading the new image.

Examples

The following command establishes LDP as the label distribution protocol for the platform:

```
Router(config)# mpls label protocol ldp
```

Related Commands

Command	Description
mpls ldp maxhops	Limits the number of hops permitted in an LSP established by the Downstream on Demand method of label distribution.
show mpls interfaces	Displays information about one or more or all interfaces that are configured for label switching.

mpls label protocol (interface configuration)

To specify the label distribution protocol for an interface, use the **mpls label protocol** command in interface configuration mode. To remove the label distribution protocol from the interface, use the **no** form of this command.

mpls label protocol {**ldp** | **tdp** | **both**}
no mpls label protocol

Syntax Description

ldp	Specifies that the label distribution protocol (LDP) is to be used on the interface.
tdp	Specifies that the tag distribution protocol (TDP) is to be used on the interface.
both	Specifies that both label and tag distribution protocols are to be supported on the interface.

Command Default

If no protocol is explicitly configured for an interface, the label distribution protocol that was configured for the platform is used. To set the platform label distribution protocol, use the global **mpls label protocol** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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.

Release	Modification
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)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

To successfully establish a session for label distribution for a link connecting two label switch routers (LSRs), the link interfaces on the LSRs must be configured to use the same label distribution protocol. If there are multiple links connecting two LSRs, all of the link interfaces connecting the two LSRs must be configured to use the same protocol.

The both option is intended for use with interfaces to multiaccess networks, such as Ethernet and FDDI, where some peers might use LDP and others use TDP. When you specify the both option, the LSR sends both LDP and TDP discovery hello messages and responds to both types of messages.

Examples

The following example shows how to establish LDP as the label distribution protocol for the interface:

```
Router(config-if)# mpls label protocol ldp
```

Related Commands

Command	Description
show mpls interfaces	Displays information about one or more interfaces that are configured for label switching.

mpls label range

To configure the range of local labels available for use with Multiprotocol Label Switching (MPLS) applications on packet interfaces, use the**mpls label range** command in global configuration mode. To revert to the platform defaults, use the **no** form of this command.

mpls label range *minimum-value maximum-value* [**static** *minimum-static-value maximum-static-value*]
no mpls label range

Syntax Description

minimum-value	The value of the smallest label allowed in the label space. The default is 16.
maximum-value	The value of the largest label allowed in the label space. The default is platform-dependent.
static	(Optional) Reserves a block of local labels for static label assignments. If you omit the **static** keyword and the *minimum-static-value maximum-static-value* arguments, no labels are reserved for static assignment.
minimum-static-value	(Optional) The minimum value for static label assignments. There is no default value.
maximum-static-value	(Optional) The maximum value for static label assignments. There is no default value.

Command Default

The platform's default values are used.

Command Modes

Global configuration

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was modified to use the new MPLS Internet Engineering Task Force (IETF) terminology and CLI syntax.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S. The static keyword was added.
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(16)	The output was modified to display the upper and lower minimum static label values in the help lines instead of the default range.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. The default values for the following arguments were modified: *maximum-value*, *minimum-static-value*, and *maximum-static-value*. The "Usage Guidelines" changed.

Usage Guidelines

The labels 0 through 15 are reserved by the IETF (see RFC 3032, MPLS Label Stack Encoding, for details) and cannot be included in the range specified in the **mpls label range** command. If you enter a 0 in the command, you will get a message that indicates that the command is an unrecognized command.

The label range defined by the**mpls label range** command is used by all MPLS applications that allocate local labels (for dynamic label switching, MPLS traffic engineering, MPLS Virtual Private Networks (VPNs), and so on).

If you specify a new label range that does not overlap the range currently in use, the new range does not take effect until you reload the router or the router undergoes a Stateful Switchover (SSO) when you are using Cisco IOS Release 12.0S and older software. Later software with the new MPLS Forwarding Infrastructure (MFI), 12.2SR, 12.2SB, 12.2(33)XHI, 12.2(25)SE, and 12.5 allows immediate use of the new range. Existing label bindings, which may violate the newly-configured ranges, remain active until the binding is removed through other methods.

You can use label distribution protocols, such as Label Distribution Protocol (LDP) and Resource Reservation Protocol (RSVP), to reserve a generic range of labels from 16 through 1048575 for dynamic assignment.

You specify the optional **static** keyword, to reserve labels for static assignment. The MPLS Static Labels feature requires that you configure a range of labels for static assignment. You can configure static bindings only from the current static range. If the static range is not configured or is exhausted, then you cannot configure static bindings.

The range of label values is 16 to 1048575. The maximum value defaults to 1048575, but might be limited to a lower value on certain platforms. Some platforms may support only 256,000 or 512,000 labels. Refer to your platform documentation for the default maximum label value.

If you configure the dynamic label space from 16 to 1048575, the static label space can be in a range that is outside the chosen dynamic label space. The upper and lower minimum static label values are displayed in the help line. For example, if you configure the dynamic label with a minimum value of 100 and a maximum value of 1000, the help lines display as follows:

```
Router(config)# mpls label range 100 1000 static ?
<1001-1048575>  Upper Minimum static label value
<16-99>         Lower Minimum static label value
Reserved Label Range  --> 0    to 15
Available Label Range --> 16   to 1048575
Dynamic Label Range   --> 100  to 1000
Lower End Range       --> 16   to 99
Upper End Range       --> 1001 to 1048575
```

In this example, you can configure a static range from one of the following ranges: 16 to 99 or 1001 to 1048575.

If the lower minimum static label space is not available, the lower minimum is not displayed in the help line. For example:

```
Router(config)# mpls label range 16 400 static ?
  <401-1048575>  Upper Minimum static label value
```

In this example, you can configure a static range with a minimum static value of 401 and a maximum static value of up to 1048575.

If an upper minimum static label space is not available, then the upper minimum is not displayed in the help line:

```
Router(config)# mpls label range 1000 1048575 static ?
  <16-999>  Lower Minimum static label value
```

In this example, the range for static label assignment is 16 to 999.

If you configure the dynamic label space with the default minimum (16) and maximum (1048575) values, no space remains for static label assignment, help lines are not displayed, and you cannot configure static label bindings. For example:

```
Router(config)# mpls label range 16 1048575 ?
  <cr>
```

Examples

The following example shows how to configure the size of the local label space. In this example, the minimum static value is set to 200, and the maximum static value is set to 120000.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mpls label range 200 120000
Router(config)#
```

If you had specified a new range that overlaps the current range (for example, the new range of the minimum static value set to 16 and the maximum static value set to 120000), then the new range takes effect immediately.

The following example show how to configure a dynamic local label space with a minimum static value set to 1000 and the maximum static value set to 1048575 and a static label space with a minimum static value set to 16 and a maximum static value set to 999:

```
Router(config)# mpls label range 1000 1048575 static 16 999
Router(config)#
```

In the following output, the **show mpls label range** command, executed after a reload, shows that the configured range is now in effect:

```
Router# show mpls label range
Downstream label pool: Min/Max label: 1000/1048575
Range for static labels: Min/Max/Number: 16/999
```

The following example shows how to restore the label range to its default value:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no mpls label range
Router(config)# end
```

Related Commands

Command	Description
show mpls forwarding table	Displays the contents of the MPLS LFIB.
show mpls label range	Displays the range of the MPLS local label space.

mpls ldp address-message

To specify advertisement of platform addresses to an LC-ATM label distribution protocol (LDP) peer, use the **mpls ldp address-message** command in interface configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp address-message
no mpls ldp address-message

Syntax Description

This command has no arguments or keywords.

Command Default

LDP Address and Address Withdraw messages are not sent to LC-ATM LDP peers.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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 LDP specification includes Address and Address Withdraw messages used by a label switch router (LSR) to advertise its addresses to its peers.

An LSR uses the addresses it learns from peers when operating in Downstream Unsolicited label advertisement mode to convert between route next hop addresses (found in the LSR routing table) and peer LDP identifiers.

The ability to map between the IP address and the peer LDP identifier is required so that:

- When the Multiprotocol Label Switching (MPLS) forwarding engine (the Label Forwarding Information Base [LFIB]) asks for labels for a given destination prefix and next hop address, the LSR can find the label learned (if any) from the next hop. The LSR maintains learned labels in its label information base (LIB) tagged by the LDP ID of the advertising LSR.
- When the LSR learns a label for destination prefix P from an LDP peer, it can determine if that peer (known to the LSR by its LDP identifier) is currently the next hop for P.

In principle, an LSR operating in Downstream On Demand (DoD) mode for an LC-ATM interface does not need this information for two reasons:

- The LSR should know from the routing table the next hop interface.
- Only one DoD peer exists per LC-ATM interface.

Consequently, Cisco platforms do not normally send Address and Address Withdraw messages to LC-ATM peers.

Some LDP implementations might require the information learned in Address and Address Withdraw messages for LC-ATM. The **mpls ldp address-message** command is provided to enable interoperability with implementation vendors that require Address messages for LC-ATM.

Note Cisco platforms always advertise their addresses in Address and Address Withdraw messages for LDP sessions operating in Downstream Unsolicited label advertisement mode.

Examples

The following is an example of the **mpls ldp address-message** command:

```
Router(config-if)# mpls ldp address-message
```

Related Commands

Command	Description
show mpls interfaces	Displays information about one or more or all interfaces that are configured for label switching.

mpls ldp advertise-labels

To control the distribution of locally assigned (incoming) labels by means of label distribution protocol (LDP), use the **mpls ldp advertise-labels** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp advertise-labels [**vrf** *vpn-name*] [{**interface** *interface* | **for** *prefix-access-list* [**to** *peer-access-list*]}]
no mpls ldp advertise-labels [**vrf** *vpn-name*] [{**interface** *interface* | **for** *prefix-access-list* [**to** *peer-access-list*]}]

Syntax Description

vrf *vpn-name*	(Optional) Specifies the Virtual Private Network (VPN) routing and forwarding (VFR) instance for label advertisement.
interface *interface*	(Optional) Specifies an interface for label advertisement of an interface address.
for *prefix-access-list*	(Optional) Specifies which destinations should have their labels advertised.
to *peer-access-list*	(Optional) Specifies which LDP neighbors should receive label advertisements. An LSR is identified by its router ID, which consists of the first 4 bytes of its 6-byte LDP identifier.

Command Default

The labels of all destinations are advertised to all LDP neighbors. If the **vrf** keyword is not specified, this command applies to the default routing domain. If the **interface** keyword is not specified, no label is advertised for the interface address.

Command Modes

Global configuration

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP and to make the command consistent with the way Cisco IOS software interprets the *prefix-access-list* argument.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.

Release	Modification
12.0(22)S	This command was integrated into Cisco IOS Release 12.(22)S. The **interface***interface* keyword and argument were added.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
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

This command is used to control which labels are advertised to which LDP neighbors. To prevent the distribution of any locally assigned labels, use the **no mpls ldp advertise-labels** command with no optional parameters. To reenable the distribution of all locally assigned labels to all LDP neighbors, use the **mpls ldp advertise-labels** command with no optional parameters.

You can execute multiple **mpls ldp advertise-labels** commands. In the aggregate, such commands determine how the LSR advertises local labels. The following rules describe the effects of multiple commands:

1. Every **mpls ldp advertise-labels** command has a (prefix acl, peer acl) pair associated with it. The *access list* pair associated with the this command (in the absence of both the **for** and **to** keywords) is (none, none); the *access list* pair associated with the **mpls ldp advertise-labels** for prefix acl command (in the absence of the **to** keyword) is (prefix-acl, none).
2. A given prefix can have, at most, one (prefix acl, peer acl) pair that applies to it, as in the following explanation:
   a. A given (prefix acl, peer acl) pair applies to a prefix only if the prefix acl matches the prefix. A match occurs if the prefix acl permits the prefix.
   b. If more than one (prefix acl, peer acl) pair from multiple **mpls ldp advertise-labels** commands matches a prefix, the (prefix acl, peer acl) pair in the first such command (as determined by the **show running-config** command) applies to the prefix.
3. When an LSR is ready to advertise a label for a prefix, the LSR:
   a. Determines whether a (prefix acl, peer acl) pair applies to the prefix.
   b. If none applies, and if the **mpls ldp advertise-labels** command has been configured, the label for the prefix is not advertised to any peer; otherwise, the label is advertised to all peers.
   c. If a (prefix acl, peer acl) pair applies to the prefix, and if the prefix acl denies the prefix, the label is not advertised to any peer.
   d. If the prefix acl permits the prefix and the peer acl is none (that is, the command that applies to the prefix is an **mpls ldp advertise-labels** for prefix acl command without the **to** keyword), then the label is advertised to all peers.
   e. If the prefix acl permits the prefix and there is a peer acl, then the label is advertised to all peers permitted by the peer acl.

Note The **mpls ldp advertise-labels** command has no effect on an LC-ATM interface. Such an interface behaves as though this command had not been executed.

Normally, LDP advertises labels only for IP prefixes that are in the routing table. You can use the **mpls ldp advertise-labels** interface command to force LDP to advertise a label for a prefix constructed from an interface address and a 32-bit mask. Such a prefix is not usually in the routing table.

Examples

In the following example, the router is configured to advertise no locally assigned labels to any LDP neighbors:

```
Router(config)# no mpls ldp advertise-labels
```

In the following example, the router is configured to advertise to all LDP neighbors only the labels for networks 10.101.0.0 and 10.221.0.0:

```
Router(config)# ip access-list standard pfx-filter
Router(config-std-nacl)# permit 10.101.0.0 0.0.255.255
Router(config-std-nacl)# permit 10.221.0.0 0.0.255.255
Router(config-std-nacl)# exit
Router(config)# mpls ldp advertise-labels for pfx-filter
Router(config)# no mpls ldp advertise-labels
```

In the following example, the router is configured to advertise the label for network 10.165.200.0 only to LSR 10.200.110.55, the label for network 10.35.35.55 only to LSR 10.150.25.25, and the labels for all other prefixes to all LSRs:

```
Router(config)# ip access-list standard pfx-filter1
Router(config-std-nacl)# permit 10.165.200.0
Router(config-std-nacl)# exit
Router(config)# ip access-list standard lsr-filter1
Router(config-std-nacl)# permit 10.200.110.55
Router(config-std-nacl)# exit
Router(config)# ip access-list standard pfx-filter2
Router(config-std-nacl)# permit 10.35.35.55
Router(config-std-nacl)# exit
Router(config)# ip access-list standard lsr-filter2
Router(config-std-nacl)# permit 10.150.25.25
Router(config-std-nacl)# exit
Router(config)# mpls ldp advertise-labels for pfx-filter1 to lsr-filter1
Router(config)# mpls ldp advertise-labels for pfx-filter2 to lsr-filter2
```

The output of the **show mpls ip binding detail** command includes the (prefix acl, peer acl) pairs that apply to each prefix. For this example, the applicable pairs are as follows:

```
Router# show mpls ip binding detail

Advertisement spec:
 Prefix acl = pfx-filter1; Peer acl = lsr-filter1
 Prefix acl = pfx-filter2; Peer acl = lsr-filter2
  10.35.35.55/8, rev 109
 in label:     16
  Advertised to:
  10.150.25.25:0
 out label:    imp-null  lsr: 10.200.110.55:0     inuse
```

```
 out label:    imp-null  lsr: 10.150.25.25:0
 Advert acl(s): Prefix acl pfx-filter2, Peer acl lsr-filter2
  10.165.200.0/8, rev 108
 in label:     imp-null
  Advertised to:
  10.200.110.55:0
 out label:    16        lsr: 10.200.110.55:0
 out label:    19        lsr: 10.150.25.25:0
 Advert acl(s): Prefix acl pfx-filter1, Peer acl lsr-filter1
  10.0.0.33/32, rev 98
 out label:    imp-null  lsr: 10.150.25.25:0
  10.0.0.44/32, rev 99
 in label:     imp-null
  Advertised to:
  10.200.110.55:0           10.150.25.25:0
  10.150.25.25/32, rev 101
 in label:     20
  Advertised to:
  10.200.110.55:0           10.150.25.25:0
 out label:    19        lsr: 10.200.110.55:0
 out label:    imp-null  lsr: 10.150.25.25:0     inuse
  10.0.0.44/32, rev 103
 in label:     imp-null
  Advertised to:
  10.200.110.55:0           10.150.25.25:0
 out label:    20        lsr: 10.200.110.55:0
 out label:    18        lsr: 10.150.25.25:0
  10.200.110.55/32, rev 104
 in label:     17
  Advertised to:
  10.200.110.55:0           10.150.25.25:0
 out label:    imp-null  lsr: 10.200.110.55:0     inuse
 out label:    17        lsr: 10.150.25.25:0
Router#
```

In the following example, the **vrf** keyword is specified to configure label advertisement in the VPN routing and forwarding instance named vpn1:

```
Router(config)# mpls ldp advertise-labels vrf vpn1 for pfx-filter1 to lsr-filter1
Router(config)# mpls ldp advertise-labels vrf vpn1 for pfx-filter2 to lsr-filter2
```

The following example uses the **interface** keyword to configure label advertisement for a /32 prefix constructed from the IP address of ethernet interface 1/1:

```
Router(config)# mpls ldp advertise-labels interface ethernet1/1
```

Related Commands

Command	Description
mpls ldp advertise-labels old-style	Uses the method of earlier software releases to interpret the for prefix-access-list parameter for the **mpls ldp advertise-labels** command.
show mpls ip binding detail	Displays detailed information about label bindings, including the access lists, if any, controlling which local labels are advertised to which LDP neighbors.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class,

mpls ldp advertise-labels old-style

To cause the **for** *prefix-access-list* parameter of the **mpls ldp advertise-labels** command to be interpreted according to the method used in earlier Cisco IOS software versions, use the **mpls ldp advertise-labels old-style** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp advertise-labels [**vrf** *vpn-name*] **old-style**
no mpls ldp advertise-labels [**vrf** *vpn-name*] **old-style**

Syntax Description

vrf *vpn-name*	(Optional) Specifies the VPN routing and forwarding (VRF) instance for label advertisement.

Command Default

If this command is not specified, the **for** *prefix-access-list* parameter in any **mpls ldp advertise-labels** commands is interpreted according to the rules specified under the "Usage Guidelines" section for the **mpls ldp advertise-labels** command. If the **vrf** *vpn-name* parameter is not specified, this command applies to the default routing domain.

Command Modes

Global configuration

Command History

Release	Modification
12.0(14)ST	This command was introduced to add Multiprotocol Label Switching (MPLS) VPN support for lable distribution protocol (LDP) and to cause the **for** *prefix-access-list* parameter in the command to be interpreted in the same way as in earlier Cisco IOS releases.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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 method for interpreting the for prefix-access-list parameter in the **mpls ldp advertise-labels** command is defined by Rule 2.a in the "Usage Guidelines" section in the **mpls ldp advertise-labels** command. This Rule 2.a follows normal access list conventions.

However, earlier Cisco IOS software versions used a different method for interpreting the **for** *prefix-access-list* parameter in **mpls ldp advertise-labels** command. For those earlier software versions, Rule 2.a read as follows:

2. A given prefix can have, at most, one (prefix acl, peer acl) pair that applies to it.

a. A given (prefix acl, peer acl) pair applies to a prefix only if the prefix acl matches the prefix. A match occurs if the prefix acl explicitly permits or denies the prefix by means of a permit or deny command. A prefix acl that contains a permit any or deny any command matches any prefix.

This earlier Rule 2.a departed from normal access list conventions in that:

- An explicit deny (including a deny any) that matches the prefix causes the (*prefixacl* , *peeracl*) pair to apply to the prefix.
- Explicit deny any and implicit deny any (which all access lists have) have different effects, in that the explicit deny any causes the access list pair to apply to all prefixes, but the implicit deny any has no effect.

Use the **mpls ldp advertise-labels old-style** command to force the use of the old-style method of interpreting the **for** *prefix-access-list* parameter used by earlier software versions if the following apply:

- A configuration developed for use with earlier software versions depends on this previous method for interpreting the **for** *prefix-access-list* parameter in **mpls ldp advertise-labels** commands.
- It is inconvenient to update the configuration to work with Rule 2.a as it appears under the "Usage Guidelines" section of the **mpls ldp advertise-labels** command.

Examples

The following command causes the old-style method of interpreting the for prefix-access-list parameter to be used in executing **mpls ldp advertise-labels** commands:

```
Router# mpls ldp advertise-labels old-style
```

In the following example, the **vrf** keyword is specified to configure label advertisement in the VFR instance named vpn1:

```
Router(config)# mpls ldp advertise-labels vrf vpn1 old-style
```

Related Commands

Command	Description
mpls ldp advertise-labels	Controls the distribution of locally assigned labels by means of LDP.

mpls ldp atm control-mode

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls ldp atm control-mode** command is not available in Cisco IOS software.

To control the mode used for handling label binding requests on LC-ATM interfaces, use the **mpls ldp atm control-mode** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp atm control-mode {**ordered** | **independent**}
no mpls ldp atm control-mode {**ordered** | **independent**}

Syntax Description

ordered	Delays a label binding in response to a Label Request message from a label distribution protocol (LDP) neighbor until a label binding has been received from the next hop LDP neighbor for the destination in question.
independent	Returns a label binding immediately in response to a Label Request message from an LDP neighbor. Any packets for the destination in question are discarded by the label switch router (LSR) until a label binding from the next hop LSR has been received.

Command Default

The default is ordered control mode.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect MPLS IETF command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(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.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.4(20)T	This command was removed.

Usage Guidelines

Use of ordered control mode by an ATM device acting as a transit LSR in an ATM cloud ensures that the device will receive labeled packets to forward only after it has learned the outgoing labels required by MPLS to forward the packets. Ordered control mode relieves the device of the burden of reassembling cells into packets that must be forwarded by means of the normal (non-MPLS) packet forwarding or discard mechanisms.

Use of independent control mode on ATM transit LSRs might slightly reduce the time an ATM edge router must wait to use an ATM label switched path (LSP) it has initiated. Independent control mode eliminates the need for the edge router to wait for the Label Request/Label Mapping signaling to traverse the ATM cloud from edge router ingress to egress and back before it can send packets into the LSP. However, there is a risk that an ATM transit device might receive labeled packets before it has learned the outgoing labels required for MPLS forwarding, thus forcing the transit device to reassemble the cells into a packet that it is likely to discard.

Examples

In the following example, the mode for handling LDP Label Request messages is set to independent for the platform:

```
Router(config)# mpls ldp atm control-mode independent
```

mpls ldp atm vc-merge through mpls static binding ipv4

mpls ldp atm vc-merge

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls ldp atm vc-merge** command is not available in Cisco IOS software.

To control whether the vc-merge (multipoint-to-point) capability is supported for unicast label virtual circuits (LVCs), use the **mpls ldp atm vc-merge** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp atm vc-merge
no mpls ldp atm vc-merge

Syntax Description

This command has no arguments or keywords.

Command Default

The ATM-VC merge capability is enabled by default if the hardware supports this feature; otherwise, the feature is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect MPLS IETF command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E and implemented on the Catalyst 6500 switch and the Cisco 7600 router.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was implemented on the Cisco MGX 8850 and MGX 8950 switches equipped with a Cisco MGX RPM-PR c.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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 and implemented on the Cisco 10000(PRE-1) router.
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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.4(20)T	This command was removed.

Usage Guidelines

Use of VC merge helps conserve ATM labels by allowing incoming LSPs from different sources for the same destination to be merged onto a single outgoing VC.

Examples

In the following example, the ATM-VC merge capability is disabled:

```
Router# no mpls ldp atm vc-merge
```

Related Commands

Command	Description
show mpls atm-ldp capability	Displays the ATM MPLS capabilities negotiated with LDP neighbors for LC-ATM interfaces.

mpls ldp autoconfig

To enable Label Distribution Protocol (LDP) on interfaces for which an Open Shortest Path First (OSPF) instance or Intermediate System-to-Intermediate System (IS-IS) instance has been defined, use the **mpls ldp autoconfig** command in router configuration mode. To disable this feature, use the **no** form of this command.

For OSPF
mpls ldp autoconfig [**area** *area-id*]
no mpls ldp autoconfig [**area** *area-id*]

For IS-IS
mpls ldp autoconfig [{*level-1*|*level-2*}]
no mpls ldp autoconfig

Syntax Description

area *area-id*	(Optional) Enables LDP on the interfaces belonging to the specified OSPF area.
level-1 | *level-2*	(Optional) Enables LDP for a specified IS-IS level. If an interface is enabled for the same level as autoconfiguration, then LDP is enabled over that interface. If the interface has a different level than autoconfiguration, LDP is not enabled. By default, without the use of these arguments, the configuration is applied to both the levels.

Command Default

LDP is not enabled on interfaces. If an OSPF area or an IS-IS level is not specified, LDP is enabled on all interfaces belonging to the OSPF or IS-IS process.

Command Modes

Router configuration

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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.0(32)SY	This command was modified to support IS-IS processes in Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Release 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

- You can specify this command multiple times to enable LDP on different routing areas with interfaces running OSPF.

- If LDP is disabled globally, the **mpls ldp autoconfig** command fails. LDP must be enabled globally by means of the global **mpls ip** command first.
- If the **mpls ldp autoconfig** command is configured, you cannot issue the global **no mpls ip** command. If you want to disable LDP, you must issue the **no mpls ldp autoconfig** command first.
- The **mpls ldp autoconfig** command is supported only with OSPF and IS-IS interior gateway protocols (IGPs).
- The MPLS LDP Autoconfiguration feature supports IS-IS only in Cisco IOS Release 12.0(32)SY.
- For interfaces running IS-IS processes, you can enable Multiprotocol Label Switching (MPLS) for each interface using the router mode command **mpls ldp autoconfig** or **mpls ldp igp autoconfig** at the interface level.
- For IS-IS interfaces, the level for which an interface is configured must be compatible with the level for which autoconfiguration is desired.
- For IS-IS interfaces, each application of the configuration command overwrites the earlier configuration. If initial autoconfiguration is enabled for level-1 and a later configuration specifies level-2, LDP is enabled only on IS-IS level-2 interfaces.

Examples

In the following example, MPLS LDP Autoconfiguration is enabled for OSPF area 5:

```
Router(config-router)# mpls ldp autoconfig area 5
```

Related Commands

Command	Description
mpls ldp igp autoconfig	Enables LDP on an interface.
show mpls interfaces	Displays information about interfaces configured for LDP.
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls ldp backoff

To configure parameters for the label distribution protocol (LDP) backoff mechanism, use the **mpls ldp backoff** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp backoff *initial-backoff maximum-backoff*
no mpls ldp backoff *initial-backoff maximum-backoff*

Syntax Description

initial-backoff	Number from 5 to 2147483, inclusive, that defines the initial backoff value in seconds. The default is 15 seconds.
maximum-backoff	Number from 5 to 2147483, inclusive, that defines the maximum backoff value in seconds. The default value is 120 seconds.

Command Default

The initial backoff value is 15 seconds and grows to a maximum value of 120 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was implemented on the Cisco MGX 8850 and MGX 8950 switches equipped with a Cisco MGX RPM-PR card.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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 LDP backoff mechanism prevents two incompatibly configured label switch routers (LSRs) from engaging in an unthrottled sequence of session setup failures. For example, an incompatibility arises when two neighboring routers attempt to perform LC-ATM (label-controlled ATM) but the two are using different ranges of VPI/VCI values for labels.

If a session setup attempt fails due to an incompatibility, each LSR delays its next attempt (that is, backs off), increasing the delay exponentially with each successive failure until the maximum backoff delay is reached.

The default settings correspond to the lowest settings for initial and maximum backoff values defined by the LDP protocol specification. You should change the settings from the default values only if such settings result in undesirable behavior.

Examples

The following command shows how to set the initial backoff delay to 30 seconds and the maximum backoff delay to 240 seconds:

```
Router(config)# mpls ldp backoff 30 240
```

Related Commands

Command	Description
show mpls ldp backoff	Displays information about the configured session setup backoff parameters and any potential LDP peers with which session setup attempts are being throttled.
show mpls ldp parameters	Displays current LDP parameters.

mpls ldp discovery

To configure the interval between transmission of consecutive Label Distribution Protocol (LDP) discovery hello messages, or the hold time for a discovered LDP neighbor, or the neighbors from which requests for targeted hello messages may be honored, use the **mpls ldp discovery** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp discovery {**hello** {**holdtime** | **interval**} *seconds* | **targeted-hello** {**holdtime** | **interval**} *seconds* | **accept** [**from** *acl*]}
no mpls ldp discovery {**hello** {**holdtime** | **interval**} | **targeted-hello** {**holdtime** | **interval**} | **accept** [**from** *acl*]}

Syntax Description

hello	Configures the intervals and hold times for directly connected neighbors.
holdtime	Defines the period of time a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor. The default value for the **holdtime** keyword is 15 seconds for link hello messages and 90 seconds for targeted hello messages.
interval	Defines the period of time between the sending of consecutive hello messages. The default value for the **interval** keyword is 5 seconds for link hello messages and 10 seconds for targeted hello messages.
seconds	Hold time or interval in seconds: • The default hold time is 15 seconds for link hello messages and 90 seconds for targeted hello messages. • The default interval is 5 seconds for link hello messages and 10 seconds for targeted hello messages.
targeted-hello	Configures the intervals and hold times for neighbors that are not directly connected (for example, LDP sessions that run between the endpoints of an LSP tunnel).
accept	Configures the router to respond to requests for targeted hello messages from all neighbors or from neighbors specified by the optional acl argument.
from *acl*	(Optional) The IP access list that specifies the neighbor from which requests for targeted hello messages may be honored. **Caution** Ensure that the access control list (ACL) is properly configured with the LDP sessions to be accepted. If no LDP entries are configured in the ACL, the ACL will allow all LDP sessions from any source.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) IETF command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S. Default values for the **holdtime** and **interval** keywords were changed.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The discovery hold time is set to the smaller of the following: the locally proposed hold time or the hold time proposed by the neighbor. The hello interval is selected so that within the hello hold time period at least three hellos messages are sent for a link hello and at least nine hello messages are sent for a targeted hello.

When the discovery hold time elapses for a neighbor discovered on an interface or for a neighbor discovered by means of a targeted hello message, the record associating the neighbor with that interface or the targeted hello message source is discarded. If an LDP session exists with a neighbor, but a discovery record no longer exists for that neighbor, the LDP session is terminated.

Setting the hold time too high causes LDP to be slow in detecting link outages; setting the hold time too low might cause LDP to terminate sessions when a hello message is dropped during traffic bursts on a link.

The exchange of targeted hello messages between two nondirectly connected neighbors (N1 and N2) may occur in the following ways:

- N1 may initiate the transmission of targeted hello messages to N2, and N2 may send targeted hello messages in response. In this situation, N1 is considered to be active and N2 is considered to be passive.

N1 targeted hello messages carry a request that N2 send targeted hello messages in response. To respond, N2 configuration must permit it to respond to N1. The **mpls ldp discovery targeted-hello accept** command is used to configure whether N1 must respond to requests for targeted hello messages.

- Both N1 and N2 may be configured to initiate the transmission of targeted hello messages to each other. In this situation, both are active.

Both, one, or neither of N1 and N2 may be passive, depending on whether they have been configured to respond to requests for targeted hello messages from the other.

Note Normally, active transmission of targeted hello messages on a router is triggered by some configuration action, such as an **mpls ip** command on a traffic engineering tunnel interface.

Examples

The following example shows how to set the period of time to 30 seconds for which a neighbor discovered on an interface is remembered, if no hello messages are received:

```
Router# configure terminal
Router(config)# mpls ldp discovery hello holdtime 30
```

The following example shows how to configure the router to respond to requests for targeted hello messages from neighbors 209.165.200.225 and 209.165.200.234:

```
Router(config)# ip access standard TRGT-ACCEPT
Router(config-nacl)# permit 209.165.200.225
Router(config-nacl)# permit 209.165.200.234
Router(config-nacl)# exit
Router(config)# mpls ldp discovery targeted-hello from TRGT-ACCEPT
```

Related Commands

Command	Description
mpls ip	Enables MPLS forwarding of IPv4 packets along normally routed paths.
mpls ldp holdtime	Changes the time for which an LDP session is maintained in the absence of LDP messages from the session peer.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp parameters	Displays current LDP parameters.

mpls ldp discovery transport-address

To specify the transport address advertised in the Label Distribution Protocol (LDP) discovery hello messages sent on an interface, use the **mpls ldp discovery transport-address** command in interface configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp discovery transport-address {**interface***IP-address*}
no mpls ldp discovery transport-address

Syntax Description

interface	Specifies that the interface IP address should be advertised as the transport address.
IP-address	IP address advertised as the transport address.

Command Default

The default behavior when this command has not been issued for an interface depends on the interface type. Unless the interface is a label-controlled ATM (LC-ATM) interface, LDP advertises its LDP router ID as the transport address in LDP discovery hello messages sent from the interface. If the interface is an LC-ATM interface, no transport address is explicitly advertised in LDP discovery hello messages sent from the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

The establishment of an LDP session between two routers requires a session TCP connection by which label advertisements can be exchanged between the routers. To establish the session TCP connection, each router must know the transport address (IP address) of the other router.

The LDP discovery mechanism provides the means for a router to advertise the transport address for its end-of-session TCP connection. When the transport address advertisement is explicit, the transport address appears as part of the contents of discovery hello messages sent to the peer. When the transport address advertisement is implicit, the transport address is not included in the discovery hello messages, and the peer uses the source IP address of received hello messages as the peer transport address.

The mpls ldp discovery transport-address command provides the means to modify the default behavior described in the Command Default section of this document. When the **interface** keyword is specified, LDP advertises the IP address of the interface in LDP discovery hello messages sent from the interface. When the *IP-address* argument is specified, LDP advertises the specified IP address in LDP discovery hello messages sent from the interface.

Note When a router has multiple links connecting it to its peer device, the router must advertise the same transport address in the LDP discovery hello messages it sends on all such interfaces.

Examples

The following example shows how to specify the LDP transport address for interface pos2/0 should be the interface IP address; it also shows how to specify the IP address 209.165.200.225 of interface pos3/1 should be the LDP transport address:

```
Router(config#) interface pos2/0
Router(config-if)# mpls ldp discovery transport-address interface
Router(config#) interface pos3/1
Router(config-if)# mpls ldp discovery transport-address 209.165.200.225
```

Related Commands

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.

mpls ldp explicit-null

To cause a router to advertise an Explicit Null label in situations where it would normally advertise an Implicit Null label, use the **mpls ldp explicit-null** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp explicit-null [{**for** *prefix-acl* | **to** *peer-acl* | **for** *prefix-acl* **to** *peer-acl*}]
no mpls ldp explicit-null

Syntax Description

for *prefix-acl*	(Optional) Specifies prefixes for which Explicit Null should be advertised in place of Implicit Null.
to *peer-acl*	(Optional) Specifies Label Distribution Protocol (LDP) peers to which Explicit Null should be advertised in place of Implicit Null.

Command Default

Implicit Null is advertised for directly connected routes unless the command mpls ldp explicit-null has been executed.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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

Normally, LDP advertises an Implicit Null label for directly connected routes. The Implicit Null label causes the previous hop (penultimate) router to do penultimate hop popping. Situations exist where it might be desirable to prevent the penultimate router from performing penultimate hop popping and to force it to replace the incoming label with the Explicit Null label.

When you issue the **mpls ldp explicit-null** command, Explicit Null is advertised in place of Implicit Null for directly connected prefixes permitted by the *prefix-acl* argument to peers permitted by the *peer-acl* argument.

If you do not specify the *prefix-acl* argument in the command, Explicit Null is advertised in place of Implicit Null for all directly connected prefixes.

If you do not specify the *peer-acl* argument in the command, Explicit Null is advertised in place of Implicit Null to all peers.

Examples

The following command shows how to cause Explicit Null to be advertised for all directly connected routes to all LDP peers:

```
Router(config)# mpls ldp explicit-null
```

The following command sequence shows how to cause Explicit Null to be advertised for directly connected route 10.5.0.0 to all LDP peers and Implicit Null to be advertised for all other directly connected routes:

```
Router(config)# ip access-list standard adv-exp-null
Router(config-std-nacl)# permit 10.5.0.0
Router(config-std-nacl)# deny any
Router(config-std-nacl)# exit
Router(config)# mpls ldp explicit-null for adv-exp-null
```

Related Commands

Command	Description
show mpls ip binding	Displays specified information about label bindings learned by LDP.

mpls ldp graceful-restart

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Graceful Restart, use the **mpls ldp graceful-restart** command in global configuration mode. To disable LDP Graceful Restart, use the **no** form of this command.

mpls ldp graceful-restart
no mpls ldp graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Default

LDP Graceful Restart is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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

LDP Graceful Restart must be enabled before an LDP session is established.

Using the no form of the command disables the Graceful Restart functionality on all LDP sessions.

Examples

The command in the following example enables LDP Graceful Restart on a router:

```
Router(config)# mpls ldp graceful-restart
```

Related Commands

Command	Description
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS forwarding state should be preserved after the control plane restarts.
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router should hold stale label-FEC bindings after an LDP session has been reestablished.
mpls ldp graceful-restart timers neighbor-liveness	Specifies the amount of time a router should wait for an LDP session to be reestablished.

mpls ldp graceful-restart timers forwarding-holding

To specify the amount of time the Multiprotocol Label Switching (MPLS) forwarding state should be preserved after the control plane restarts, use the **mpls ldp graceful-restart timers forwarding-holding** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers forwarding-holding *secs*
no mpls ldp graceful-restart timers forwarding-holding

Syntax Description

secs	The amount of time (in seconds) that the MPLS forwarding state should be preserved after the control plane restarts. The default is 600 seconds. The range is 30 to 600 seconds.

Command Default

After the control plane on the Cisco 7500 and Cisco 10000 series router restarts, the MPLS forwarding state is preserved for 600 seconds.

Command Modes

Global configuration

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

Configuring the local forwarding-holding timer to a value less than the IOS FT Reconnect Timeout of 120 seconds may prevent a Label Distribution Protocol (LDP) session from being established. Configure the forwarding-holding timer to less than 120 seconds only if an LDP neighbor has an FT Reconnect Timeout value of less than 120 seconds.

If the timer expires, all entries that are marked stale are deleted.

Examples

In the following example, the MPLS forwarding state is preserved for 300 seconds after the control plane restarts:

```
Router(config)# mpls ldp graceful-restart timers forwarding-holding 300
```

Related Commands

Command	Description
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router should hold stale label-FEC bindings after an LDP session has been reestablished.

Command	Description
mpls ldp graceful-restart timers neighbor-aliveness	Specifies the amount of time a router should wait for an LDP session to be reestablished.

mpls ldp graceful-restart timers max-recovery

To specify the amount of time a router should hold stale label-Forwarding Equivalence Class (FEC) bindings after a Label Distribution Protocol (LDP) session has been reestablished, use the **mpls ldp graceful-restart timers max-recovery** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers max-recovery *secs*
no mpls ldp graceful-restart timers max-recovery

Syntax Description

secs	The amount of time (in seconds) that the router should hold stale label-FEC bindings after an LDP session has been reestablished. The default is 120 seconds. The range is 15 to 600 seconds.

Command Default

Stale label-FEC bindings are held for 120 seconds after an LDP session has been reestablished.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
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

After the timer expires, all stale label-FEC bindings learned from the associated LDP session are removed, which results in the removal of any forwarding table entries that are based on those bindings.

Examples

In the following example, the router should hold stale label-FEC bindings after an LDP session has been reestablished for 180 seconds:

```
Router(config)# mpls ldp graceful-restart timers max-recovery 180
```

Related Commands

Command	Description
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS forwarding state should be preserved after the control plane restarts.
mpls ldp graceful-restart timers neighbor-liveness	Specifies the amount of time a router should wait for an LDP session to be reestablished.

mpls ldp graceful-restart timers neighbor-liveness

To specify the upper bound on the amount of time a router should wait for a Label Distribution Protocol (LDP) session to be reestablished, use the **mpls ldp graceful-restart timers neighbor-liveness** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers neighbor-liveness *secs*
no mpls ldp graceful-restart timers neighbor-liveness

Syntax Description

secs	The amount of time (in seconds) that the router should wait for an LDP session to be reestablished. The default is 120 seconds. The range is 5 to 300 seconds.

Command Default

The default is a maximum of 120 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
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

The amount of time a router waits for an LDP session to be reestablished is the lesser of the following values:

- The value of the peer's fault tolerant (FT) type length value (TLV) reconnect timeout
- The value of the neighbor liveness timer

If the router cannot reestablish an LDP session with the neighbor in the time allotted, the router deletes the stale label-FEC bindings received from that neighbor.

Examples

The command in the following example sets the amount of time that the router should wait for an LDP session to be reestablished to 30 seconds:

```
Router(config)# mpls ldp graceful-restart timers neighbor-liveness 30
```

Related Commands

Command	Description
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS forwarding state should be preserved after the control plane restarts.

Command	Description
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router should hold stale label-FEC bindings after an LDP session has been reestablished.

mpls ldp holdtime

To change the time for which an Label Distribution Protocol (LDP) session is maintained in the absence of LDP messages from the session peer, use the **mpls ldp holdtime** command in global configuration mode. To disable this command, use the **no** form of the command.

mpls ldp holdtime *seconds*
no mpls ldp holdtime *seconds*

Syntax Description

seconds	Number from 15 to 65535 that defines the time, in seconds, an LDP session is maintained in the absence of LDP messages from the session peer. The default is 180.

Command Default

The default value for the *seconds* argument is 180.

Command Modes

Global configuration

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) IETF command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)s	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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

When an LDP session is established between two LSRs, the hold time used for the session is the lower of the values configured on the two LSRs.

Examples

The following example shows how to configure the hold time of LDP sessions for 30 seconds:

```
Router# mpls ldp holdtime 30
```

Related Commands

Command	Description
show mpls ldp parameters	Displays the current LDP parameter.
show mpls atm-ldp bindings	Displays specified entries from the ATM label binding database.

mpls ldp igp autoconfig

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) autoconfiguration on an interface that belongs to an Open Shortest Path First (OSPF) area, use the **mpls ldp igp autoconfig** command in interface configuration mode. To disable MPLS LDP autoconfiguration, use the **no** form of the command.

mpls ldp igp autoconfig
no mpls ldp igp autoconfig

Syntax Description

This command has no arguments or keywords.

Command Default

This command works with the **mpls ldp autoconfig** command, which enables LDP on all interfaces that belong to an OSPF area. So, by default, all interfaces are enabled for LDP.

Command Modes

Interface configuration (config-if)

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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Release 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

This command works with the **mpls ldp autoconfig** command, which enables LDP on all interfaces that belong to an OSPF area. To disable LDP on selected interfaces, use the **no mpls ldp igp autoconfig** command.

Examples

The following example shows how to disable LDP on interface POS1/0:

```
Router(config)# interface pos1/0
Router(config-if)# no mpls ldp igp autoconfig
```

Related Commands

Command	Description
mpls ldp autoconfig	Globally enables LDP on all interfaces that belong to an OSPF area.
show mpls interfaces	Displays information about interfaces configured for LDP.
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls ldp igp sync

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization on an interface that belongs to an Open Shortest Path First (OSPF) process, use the **mpls ldp igp sync** command in interface configuration mode. To disable MPLS LDP-IGP synchronization, use the **no** form of the command.

mpls ldp igp sync [**delay** *seconds*]
no mpls ldp igp sync [**delay**]

Syntax Description

delay	(Optional) Sets a delay timer for MPLS LDP-IGP synchronization.
seconds	(Optional) Delay time, in seconds. The range is 5 to 60 seconds.

Command Default

If MPLS LDP-IGP synchronization is enabled on an OSPF process, MPLS LDP-IGP synchronization is enabled by default on all interfaces configured for the process. A delay timer is not set.

Command Modes

Interface configuration (config-if)

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.
12.0(32)S	The optional **delay** *seconds* keyword and argument were added.
12.4(12)	This command was integrated into Cisco IOS Release 12.4(12).
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

This command works with the **mpls ldp sync** command, which enables MPLS LDP-IGP synchronization on all interfaces that belong to an OSPF process. To disable MPLS LDP-IGP synchronization on a selected interface, use the **no mpls ldp igp sync** command in the configuration for that interface.

Use the **mpls ldp igp sync delay** *seconds* command to configure a delay time for MPLS LDP and IGP synchronization on an interface-by-interface basis. To remove the delay timer from a specified interface, use the **no mpls ldp igp sync delay** command. This command sets the delay time to 0 seconds, but leaves MPLS LDP-IGP synchronization enabled.

When LDP is fully established and synchronized, LDP checks the delay timer:

- If you configured a delay time, LDP starts the timer. When the timer expires, LDP checks that synchronization is still valid and notifies the OSPF process.
- If the delay time is not configured, synchronization is disabled or down, or an interface is removed from an IGP process, LDP stops the timer and immediately notifies the OSPF process.

If you configure a new delay time while a timer is running, LDP saves the new delay time but does not reconfigure the running timer.

Examples

The following example shows how to disable MPLS LDP-IGP synchronization on POS interface 1/0:

```
Router(config)# interface pos1/0
Router(config-if)# no mpls ldp igp sync
```

The following example shows how to set a delay timer of 45 seconds for MPLS LDP-IGP synchronization on FastEthernet interface 0/0:

```
Router(config)# interface FastEthernet 0/0
Router(config-if)# mpls ldp igp sync delay 45
```

Related Commands

Command	Description
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process or an IS-IS process.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls ldp igp sync holddown

To specify how long an Interior Gateway Protocol (IGP) should wait for Label Distribution Protocol (LDP) synchronization to be achieved, use the **mpls ldp igp sync holddown** command in global configuration mode. To disable the hold-down timer, use the **no** form of this command.

mpls ldp igp sync holddown *milliseconds*
no mpls ldp igp sync holddown

Syntax Description

milliseconds	The number of milliseconds an IGP should wait for an LDP session to be established. The range is 1 to 2147483647.

Command Default

An IGP will wait indefinitely for LDP synchronization to be achieved.

Command Modes

Global configuration (config)

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.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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 3.6S	This command was implemented on the Cisco ASR 903 series routers.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command enables you to limit the amount of time an IGP waits for LDP synchronization to be achieved.

Examples

In the following example, the IGP is limited to 10,000 milliseconds (10 seconds):

```
Router(config)# mpls ldp igp sync holddown 10000
```

Related Commands

Command	Description
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process or an IS-IS process.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls ldp label

To enter MPLS LDP label configuration mode to specify how Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) handles local label allocation, use the **mpls ldp label** command in global configuration mode. To remove all local label allocation filters configured in MPLS LDP label configuration mode and restore LDP default behavior for local label allocation without a session reset, use the **no** form of this command.

mpls ldp label
no mpls ldp label

Syntax Description

This command has no arguments or keywords.

Command Default

LDP label configuration mode commands are not available.

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

After you enter the **mpls ldp label** command, you can specify a prefix list or host routes to filter prefixes for MPLS LDP local label allocation.

Use the **no** form of the command to remove prefix filtering for local label allocation and restore the default LDP local allocation behavior without resetting the session.

A maximum of one filter configuration is allowed for the global table.

Examples

The following example shows how to enter MPLS LDP label configuration mode, specify the prefix list named list1 to filter prefixes for MPLS LDP local label allocation, and exit MPLS LDP label configuration mode:

```
configure terminal
!
mpls ldp label
 allocate global prefix-list list1
 exit
```

The following examples shows how to remove all local label allocation filters in MPLS LDP label configuration mode and restore LDP default behavior for local label allocation:

```
configure terminal
!
no mpls ldp label
```

Related Commands

Command	Description
allocate	Configures local label allocation filters for learned routes for MPLS LDP.

mpls ldp logging neighbor-changes

To generate system error logging (syslog) messages when Label Distribution Protocol (LDP) sessions go down, use the **mpls ldp logging neighbor-changes** command in global configuration mode. To disable generating syslog messages, use the **no** form of this command.

mpls ldp logging neighbor-changes
no mpls ldp logging neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Logging is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)T	This command was integrated into Cisco IOS Release 12.2(14)T.
12.0(31)S	The log message is updated to show a VPN routing/forwarding instance (VRF) information and the reason for an LDP neighbor going down.
12.3(15)	The log message is updated to show VRF information and the reason for an LDP neighbor going down.
12.4(1)	The log message is updated to show VRF information and the reason for an LDP neighbor going down.
12.2(28)S	The log message is updated to show VRF information and the reason for an LDP neighbor going down.

Usage Guidelines

Use the **mpls ldp logging neighbor-changes** command to generate syslog messages when an LDP session goes down. The command also provides VRF information about the LDP neighbor and the reason for the LDP session going down. Some of the reasons for an LDP session going down are the following:

- An LDP was disabled globally by configuration.
- An LDP was disabled on an interface.

Examples

The following example generates syslog messages when LDP sessions go down:

```
Router(config)# mpls ldp logging neighbor-changes
```

The following output shows the log entries when an LDP session with neighbor 192.168.1.100:0 goes down and comes up. The session went down because the discovery hold timer expired. The VRF table identifier for the neighbor is 1.

```
2d00h: %LDP-5-NBRCHG: LDP Neighbor 192.168.1.100:0 (1) is DOWN (Disc hold timer expired)
2d00h: %LDP-5-NBRCHG: LDP Neighbor 192.168.1.100:0 (1) is UP
```

mpls ldp logging password configuration

To enable the display password configuration change events on an MPLS Label Switch Router (LSR), use the **mpls ldp logging password configuration** command in global configuration mode. To disable the display of password events, use the **no** form of this command.

mpls ldp logging password configuration [**rate-limit** *num*]
no mpls ldp logging password configuration

Syntax Description

rate-limit *num*	(Optional) Specifies a rate limit of 1 to 60 messages per minute.

Command Default

Logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The logging output displays events when a new password is configured or an existing password has been changed or deleted.

Related Commands

Command	Description
mpls ldp logging password rollover	Enables the display password rollover events on an MPLS LSR.
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.

Command	Description
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp logging password rollover

To enable the display password rollover events on an MPLS Label Switch Router (LSR), use the **mpls ldp logging password rollover** command in global configuration mode. To disable the display of password events, use the **no** form of this command.

mpls ldp logging password rollover [**rate-limit** *num*]
no mpls ldp logging password rollover

Syntax Description

rate-limit *num*	(Optional) Specifies a rate limit of 1 to 60 messages per minute.

Command Default

Logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The logging output displays events when a new password is used for authentication or when authentication is disabled.

Related Commands

Command	Description
mpls ldp logging password configuration	Enables the display password configuration change events on an MPLS LSR.
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp loop-detection

To enable the label distribution protocol (LDP) optional loop detection mechanism, use the **mpls ldp loop-detection** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp loop-detection
no mpls ldp loop-detection

Syntax Description

This command has no optional keywords or arguments.

Command Default

LDP loop detection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
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 LDP loop detection mechanism is intended for use in networks of devices that do not use time-to-live mechanisms (for example, ATM switches) that cannot fairly allocate device resources among traffic flows.

The LDP loop detection mechanism is used with the Downstream on Demand method of label distribution, supplementing the Downstream on Demand hop count mechanism to detect looping LSPs that might occur during routing transitions.

Examples

The following command sets the LDP loop detection mechanism on:

```
Router(config)# mpls ldp loop-detection
```

Related Commands

Command	Description
mpls ldp maxhops	Limits the number of hops permitted in an LSP established by the Downstream on Demand method of label distribution.

mpls ldp maxhops

To limit the number of hops permitted in a label switched path (LSP) established by the Downstream on Demand method of label distribution, use the **mpls ldp maxhops** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp maxhops *number*
no mpls ldp maxhops

Syntax Description

number	Number from 1 to 255, inclusive, that defines the maximum hop count. The default is 254.

Command Default

The default is 254 hops.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was updated with MPLS command syntax and terminology.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
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

When an ATM label switch router (LSR) initiates a request for a label binding, it sets the hop count value in the Label Request message to 1. Subsequent ATM-LSRs along the path to the edge of the ATM label switching region increment the hop count before forwarding the Label Request message to the next hop.

When an ATM LSR receives a Label Request message, it does not send a Label Mapping message in response, nor does it propagate the request to the destination next hop if the hop count value in the request equals or exceeds the maxhops value. Instead, the ATM LSR returns an error message that specifies that the maximum allowable hop count has been reached. This threshold is used to prevent forwarding loops in the setting up of label switch paths across an ATM region.

Examples

The following example sets the hop count limit to 10:

```
Router(config)# mpls ldp maxhops 10
```

Related Commands

Command	Description
mpls ldp router-id	Specifies a preferred interface for determining the LDP router ID.

Command	Description
show mpls atm-ldp bindings	Displays specified entries from the ATM label binding database.
show mpls ip binding	Displays specified information about label bindings learned by LDP.

mpls ldp neighbor implicit-withdraw

To configure the advertisement of a new label for a Forwarding Equivalence Class (FEC) without the withdrawal of the previously advertised label, use the **mpls ldp neighbor implicit-withdraw** command in global configuration mode. To disable this option for the specified neighbor, use the **no** form of this command.

mpls ldp neighbor [**vrf** *vpn-name*] *ip-addr* **implicit-withdraw**
no mpls ldp neighbor [**vrf** *vpn-name*] *ip-addr* [**implicit-withdraw**]

Syntax Description

vrf *vpn-name*	(Optional) VPN routing and forwarding instance for the specified neighbor.
ip-addr	Router ID (IP address) that identifies a neighbor.

Command Default

When the **vrf** keyword is not specified in this command, the label distribution protocol (LDP) neighbor is configured in the default routing domain.

If this command is not configured, when it is necessary for LDP to change the label it has advertised to a neighbor for some prefix, it will withdraw the previously advertised label before advertising the new label to the neighbor.

For the no form of the command, if the **implicit-withdraw** keyword is not specified, all configuration information for the specified neighbor reverts to the defaults and the neighbor record is deleted.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(21)ST	This command was modified to add the **implicit-withdraw** keyword.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was implemented on the Cisco 10000(PRE-1) router.
12.2(13)T	This command was implemented on the Cisco 2600 and 3600 routers.
12.2(14)S	This command was implemented on the Cisco 7200 and 7500 series routers and integrated into Cisco IOS Release 12.2(14)S.
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

By default, in Cisco IOS Release 12.0(21)ST and later, LDP withdraws the previously advertised label by using a withdraw message before advertising a new label for a FEC. In Cisco IOS releases prior to 12.0(21)ST, LDP did not withdraw a previously advertised label before advertising a new label for a FEC. In those older releases, the new label advertisement served as an implied withdraw and LDP did not send a withdraw message. To cause LDP now to operate as it did in releases before Cisco IOS release 12.0(21)ST--that is, to make LDP now advertise a new label for a FEC without first withdrawing the previously advertised label--use this command's **implicit-withdraw**keyword.

```
Router(config)# mpls ldp neighbor 10.10.10.10 implicit-withdraw
```

Using the **implicit-withdraw** keyword avoids generating the overhead from an exchange of label withdraw and label release messages.

To disable the **implicit-withdraw** option, use the **no** form of the command with the **implicit-withdraw** keyword. This returns the router to the default, which requires that LDP withdraw the previously advertised label for a FEC before advertising a new label.

```
Router(config)# no
 mpls ldp neighbor 10.10.10.10 implicit-withdraw
```

Examples

In the following example, LDP does not send a label-withdraw message to the neighbor whose router ID is 10.10.10.10 when a need exists to change the previously advertised label for a FEC:

```
Router(config)# mpls ldp neighbor 10.10.10.10 implicit-withdraw
```

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp neighbor targeted	Sets up a targeted session with the specified neighbor.

mpls ldp neighbor labels accept

To configure a label switching router (LSR) to filter label distribution protocol (LDP) inbound label bindings from a particular LDP peer, use the **mpls ldp neighbor labels accept** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp neighbor [**vrf** *vpn-name*] *nbr-address* **labels accept** *acl*
no mpls ldp neighbor [**vrf** *vpn-name*] *nbr-address* **labels accept** *acl*

Syntax Description

vrf *vpn-name*	(Optional) Specifies VPN routing and forwarding instance (*vpn-name*) for accepting labels.
nbr-address	Specifies address of the LDP peer whose advertisements are to be filtered.
labels accept *acl*	Specifies the prefixes (access control list) that are acceptable (permitted).

Command Default

If the **vrf** keyword is not specified, the specified LDP neighbor is configured in the default routing domain.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The specified ACL is used to filter label bindings advertised by the specified neighbor. If the prefix part of the label binding is permitted by the ACL, the router will accept the binding. If the prefix is denied, the router will not accept or store the binding.

This functionality is particularly useful when two different entities manage peer LSRs; that is, the recipient cannot perform filtering by altering the configuration of the sender. This is likely to occur in an Multiprotocol Label Switching (MPLS) virtual private network (VPN) that is using the LDP-based Carrier Supporting Carrier (CSC) feature. In that situation, the backbone carrier may want to restrict the set of label bindings that its provider edge (PE) router may learn from an adjacent customer edge (CE) router that a customer carrier operates.

When inbound label binding filtering is configured, certain configuration changes may require a router to retain bindings that it previously discarded. For example:

- Inbound filtering is disabled.
- An inbound filtering ACL is redefined to be less restrictive.

A router does not maintain a record of the set of bindings it previously discarded. Therefore, it cannot ask its neighbors to readvertise just those bindings. In addition, LDP (as defined by RFC 3036) does not provide a means for a router to signal its neighbors to readvertise all label bindings. Consequently, to relearn label bindings following such configuration changes, you must reset the LDP session or sessions by using the**clear mpls ldp neighbor** command.

Note The **mpls ldp neighbor labels accept** command has no effect on an LC-ATM interface. Such an interface behaves as though this command had not been executed. The **mpls ldp request-labels** ACL command, which is supported for LC-ATM, controls which label bindings are requested (accepted) from neighbors.

Examples

The following example specifies that the LSR accepts inbound label bindings from neighbor 10.19.19.19 in vrf vpn1 for prefixes permitted by the ACL named aclone:

```
Router(config)# mpls ldp neighbor vrf vpn1 10.19.19.19 label accept aclone
```

Related Commands

Command	Description
clear mpls ldp neighbor	Forcibly resets an LDP session.
mpls ldp advertise-labels	Controls the distribution of locally assigned (incoming) labels by means of LDP.
show ip access list	Displays the list of configured access lists and their definitions.
show mpls ldp neighbor	Displays the status of the LDP sessions.

mpls ldp neighbor password

To configure a password for computing message digest algorithm 5 (MD5) checksums for the session TCP connection with the specified neighbor, use the **mpls ldp neighbor password** command in global configuration mode. To disable this option for the specified neighbor, use the **no** form of this command.

mpls ldp neighbor [**vrf** *vpn-name*] *ip-address* **password** *password*
no mpls ldp neighbor [**vrf** *vpn-name*] *ip-address* [**password** *password*]

Syntax Description

vrf *vpn-name*	(Optional) VPN routing and forwarding instance for the specified neighbor.
ip-address	Router ID (IP address) that identifies a neighbor.
password	Password used for computing MD5 checksums for the session TCP connection with the specified neighbor.

Command Default

Unless the TCP MD5 Signature Option is explicitly configured with the password for session TCP connections, the option is not used. When the **vrf** name is not specified in this command, the Label Distribution Protocol (LDP) neighbor is configured in the default routing domain. For the no form of the command, if the password is not specified, all configuration information for the specified neighbor reverts to the defaults and the neighbor record is deleted.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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.
12.0(33)S	This command was integrated in Cisco IOS Release 12.0(33)S.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.

Usage Guidelines

You can invoke authentication between two LDP peers, verifying each segment sent on the TCP connection between the peers. To do so, you must configure authentication on both LDP peers using the same password; otherwise, the peer session is not established.

The authentication capability uses the MD5 algorithm. MD5, an algorithm used in conjunction with SNMP, verifies the integrity of the communication, authenticates the origin of the message, and checks for timeliness.

Invoking the **mpls ldp neighbor password** command causes the generation and checking of the MD5 digest for every segment sent on the TCP connection.

Configuring a password for an LDP neighbor causes an existing LDP session to be torn down and a new session to be established.

If a router has a password configured for a neighbor, but the neighbor router does not have a password configured, a message such as the following appears on the console while the two routers attempt to establish an LDP session:

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's IP
address]:646
```

Similarly, if the two routers have different passwords configured, a message such as the following appears on the console:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP
address]:646
```

Examples

In the following example, the password (password1) is configured as the password for use with MD5 for the neighbor whose router ID is 139.27.0.15:

```
Router(config)# mpls ldp neighbor 139.27.0.15 password password1
```

In the following example, the password (password1) is configured as the password for use with MD5 for the LDP neighbor having router ID 4.4.4.4 in the VPN routing and forwarding instance named vpn1:

```
Router(config)# mpls ldp neighbor vrf vpn1 4.4.4.4 password password1
```

Related Commands

Command	Description
mpls ldp neighbor implicit-withdraw	Configures the advertisement of a new label for a FEC without the withdrawal of the previously advertised label.
mpls ldp neighbor targeted	Sets up a targeted session with the specified neighbor.

mpls ldp neighbor targeted

To set up a targeted session with a specified neighbor, use the **mpls ldp neighbor targeted** command in global configuration mode. To disable a targeted session, use the **no** form of this command.

mpls ldp neighbor [**vrf** *vpn-name*] *ip-addr* **targeted** [{**ldp** | **tdp**}]
no mpls ldp neighbor [**vrf** *vpn-name*] *ip-addr* [**targeted** [{**ldp** | **tdp**}]]

Syntax Description

vrf *vpn-name*	(Optional) VPN routing and forwarding (VRF) instance for a specified neighbor.
ip-addr	Router ID (IP address) that identifies a neighbor.
ldp	(Optional) Specifies Label Distribution Protocol (LDP) as the label protocol for the targeted session.
tdp	(Optional) Specifies Tag Distribution Protocol (TDP) as the label protocol for the targeted session.

Command Default

When the **targeted** keyword is not specified, a targeted session is not set up with the neighbor. For the no form of the command, if the **targeted** keyword is not specified, all configuration information for the specified neighbor reverts to the defaults and the neighbor record is deleted.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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

If you do not specify the label protocol for the targeted session, the label protocol specified with the **mpls label protocol** command is used. If the **mpls label protocol** command is not configured, then LDP is used for the targeted session.

Use the **mpls ldp neighbor targeted** command when you need to set up a targeted session and other means of establishing targeted sessions do not apply, such as configuring **mpls ip** on a traffic engineering (TE) tunnel or configuring Any Transport over MPLS (AToM) virtual circuits (VCs). For example, you would use this command to set up a targeted session between directly connected MPLS label switch routers (LSRs) when MPLS label forwarding convergence time is an issue.

The **mpls ldp neighbor targeted** command can improve label convergence time for directly connected neighbor LSRs when the links directly connecting them are down. When the links between the neighbor LSRs are up, both the link and targeted Hellos maintain the LDP session. If the links between the neighbor LSRs go down, the targeted Hellos maintain the session, allowing the LSRs to retain labels learned from each other.

When a link directly connecting the LSRs comes back up, the LSRs can immediately reinstall labels for forwarding use without having to reestablish their LDP session and exchange labels.

Examples

In the following example, the router sets up a targeted session with the neighbor 10.10.10.10 using TDP as the label protocol:

```
Router(config)# mpls ldp neighbor 10.10.10.10 targeted
```

In the following example, the router sets up a targeted session with the neighbor 10.10.10.10 using LDP as the label protocol:

```
Router(config)# mpls label protocol ldp
Router(config)# mpls ldp neighbor 10.10.10.10 targeted
```

Another way to set up a targeted session using LDP without changing the default label protocol is as follows:

```
Router(config)# mpls ldp neighbor 10.10.10.10 targeted ldp
```

Related Commands

Commands	Description
mpls ldp neighbor implicit-withdraw	Configures the advertisement of a new label for a FEC without the withdrawal of the previously advertised label.
mpls ldp neighbor password	Configure a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.

mpls ldp password fallback

To configure a message digest algorithm 5 (MD5) password for Label Distribution Protocol (LDP) sessions with peers, use the **mpls ldp password fallback** command in global configuration mode. To remove the MD5 password, use the **no** form of this command.

mpls ldp [**vrf** *vrf-name*] **password fallback** {**key-chain keychain-name** | [{**0** | **7**}] **password**}
no mpls ldp [**vrf** *vrf-name*] **password fallback**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding (VRF) instance configured on the label switch router (LSR).
key-chain *keychain-name*	(Optional) Specifies the name of the key chain used to specify the MD5 key that authenticates the exchange of bidirectional LDP traffic.
0 |**7**	(Optional) Specifies whether the password that follows is encrypted: • **0** specifies an unencrypted password. • **7** specifies an encrypted password.
password	Specifies the MD5 password to be used for the LDP sessions with peers whose connections are established through a named VRF or the global routing table.

Command Default

The MD5 password for LDP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.0(33)S	The **key-chain** *keychain-name* keyword-argument pair argument was added.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command specifies the default password for the VRF routing table. The VRF routing table name is specified by the *vrf-name* argument when you configure the **vrf** keyword for the command. If you do not include the **vrf** keyword in the command, the command specifies the default password for the global routing table. The password configured by this command is the password used for sessions between peers, if neither of the following commands applies: the **mpls ldp neighbor password** command or the **mpls ldp password option** command.

If you configure a type 7 (encrypted) password, the password is saved in encrypted form.

If you configure a type 0 (clear-text) password, it can be saved in clear-text form or encrypted form, depending on the status of the **service password-encryption** command:

- If the **service password-encryption** command is enabled, then the type 0 password is converted and saved in encrypted form.
- If the **service password-encryption** command is disabled, then the type 0 password is saved in clear-text (nonencrypted) form.

When you enter a **show running-config** command, if the global **service password-encryption** command is enabled, a password saved in clear-text form is converted into encrypted form, and displayed and saved in encrypted form.

Examples

The following example shows how to configure an MD5 password for an LDP session with peers in VRF vpn1:

```
Router> enable
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mpls ldp vrf vpn1 password fallback secure
Router(config)# exit
Router#
```

The password, secure, would be encrypted. It is shown here as you would enter it on the command line.

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp password option

To configure a message digest algorithm 5 (MD5) password for Label Distribution Protocol (LDP) sessions with neighbors whose LDP router IDs are permitted by a specified access list, use the **mpls ldp password option** command in global configuration mode. To disable an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list, use the **no** form of this command.

mpls ldp[{**vrf** *vrf-name*}]**password option** *number* **for** *acl*{**key-chain** *keychain-name* | [{**0** | **7**}]}*password*
no mpls ldp [**vrf** *vrf-name*] **password option** *number*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding (VRF) instance configured on the label switch router (LSR).
number	The option number. A comparison of the *number* argument from several commands by the software sets up the order in which LDP evaluates access lists in the definition of a password for the neighbor. The valid range is from 1 to 32767.
for *acl*	Specifies the name of the access list that includes the LDP router IDs of those neighbors for which the password applies. Only standard IP access lists can be used for the *acl* argument.
key-chain *keychain-name*	Specifies the name of the key chain used to specify the MD5 key that authenticates the exchange of bidirectional LDP traffic.
0	(Optional) Specifies that the password is an unencrypted password.
7	(Optional) Specifies that the password is an encrypted password.
password	Specifies the MD5 password to be used for the specified LDP sessions.

Command Default

The MD5 password for LDP is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.0(32)SRB.
12.0(33)S	This command was modified. The **key-chain***keychain-name* keyword-argument pair was added.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Release	Modification
15.1(1)S	This command was modified. Support for a warning message to be displayed when the MD5 key from the key chain is truncated to the first 25 characters was added.

Usage Guidelines

This command specifies the *password* argument as the MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by an access list specified in the *acl* argument. This password is used if a password is not specified by the **mpls ldp password option** command.

When a configuration includes multiple **mpls ldp password option** commands, the *number* argument defines the order in which the command access lists are evaluated.

A configuration for a VRF can include zero, one, or multiple **mpls ldp password option** commands.

You can specify the passwords as unencrypted text (type 0) or in encrypted format (type 7). If you configure a type 7 password, the password is saved in encrypted form. If you configure a type 0 password, the password can be saved in unencrypted form or encrypted form, depending on the status of the **service password-encryption** command:

- If the **service password-encryption** command is enabled, the type 0 password is converted and saved in encrypted form.

When you enter a **show running-config** command, if the **service password-encryption** command is enabled, a password saved in unencrypted form is converted into encrypted form, and is then displayed and saved in encrypted form.

- If the **service password-encryption**command is disabled, the type 0 password is saved in unencrypted form.

The MD5 password and the generated key chain key are limited to 25 characters. If he password and key are more than 25 characters, the encryption is performed only on the first 25 characters and the remaining characters are truncated.

The following is an example of the message displayed when the MD5 password exceeds 25 characters:

```
Router(config)# mpls ldp password option 7 for acl1 password12345678912345678912345678 9

% Unencrypted password has been truncated to 25 characters.
```

The following is an example of the message displayed when you configure the **service password-encryption key-chain** keyword to generate a password:

```
Router(config)# mpls ldp password option 0 for acl1 key-chain MyKeyChain
```

The key chain “MyKeyChain” consists of a series of keys, each with an acceptance interval:

```
Key-chain MyKeyChain:
    key 1 -- text "first_key"
        accept lifetime (00:00:00 GMT Jan 1 2010) - (18:58:00 GMT Dec 8 2010)
        send lifetime (00:00:00 GMT Jan 1 2010) - (18:56:00 GMT Dec 8 2010)
    key 10 -- text "10_key_ten_begin"
        accept lifetime (18:52:00 GMT Dec 8 2010) - (960 seconds)
        send lifetime (18:55:00 GMT Dec 8 2010) - (600 seconds)
    key 20 -- text "20_key_20_20_20_20_20_20_20_20_20_20_20_20_"
        accept lifetime (19:02:00 GMT Dec 8 2010) - (960 seconds)
        send lifetime (19:05:00 GMT Dec 8 2010) - (600 seconds)
    key 30 -- text "30_key_30_30_30_30_30_30_30_30_30_30_30_30_"
```

```
        accept lifetime (19:12:00 GMT Dec 8 2010) - (960 seconds)
        send lifetime (19:15:00 GMT Dec 8 2010) - (600 seconds)
    key 40 -- text "key_forty_endgame"
        accept lifetime (19:12:00 GMT Dec 8 2010) - (infinite) [valid now]
        send lifetime (19:15:00 GMT Dec 8 2010) - (infinite) [valid now]
```

A [valid now] key is selected as the current MD5 password. If the selected key exceeds 25 characters, only the first 25 characters are used for the MD5 password. When you configure the **mpls ldp password option** command with the **key-chain** keyword, a notification is displayed to remind you that the MD5 password used may be shorter than the key string:

key-chain

```
% Only first 25 characters of key chain keys can be used for MD5 encryption
```

Note This notification is displayed every 15 minutes. If it has been less than 15 minutes since you last entered the **mpls ldp password option** command with the keyword, this notification is not displayed.

Whenever LDP truncates a key from a key chain for the encrypted LDP session, a notice message of the following format is also logged:

```
%LDP-5-PWDKEYTRUNC: MD5 digest uses 25 chars of longer transmit/receive key(s) for peer
<Routerid>
```

The following is an example of a log created when a key chain key exceeds 25 characters:

```
*Dec 17 02:45:31.831: %LDP-5-PWDKEYTRUNC: MD5 digest uses 25 chars of longer transmit/receive
 key(s) for peer 3.3.3.30
```

Examples

The following example shows how to configure an MD5 password for an LDP session with neighbors whose LDP router IDs are permitted by access list 10:

```
Router> enable
Router# configure terminal
Router(config)# mpls ldp password option 6 for 10
 password1
Router(config)# exit
```

The password, called password1 in the above example, is unencrypted.

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.

Command	Description
service password-encryption	Encrypts passwords.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp password required

To specify that Label Distribution Protocol (LDP) must use a password for an attempt to establish a session between LDP peers, use the **mpls ldp password required** command in global configuration mode. To remove the requirement that a password be used for a session with LDP, use the **no** form of this command.

mpls ldp [**vrf** *vrf-name*] **password required** [**for** *acl*]
no mpls ldp [**vrf** *vrf-name*] **password required** [**for** *acl*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding (VRF) instance configured on the label switch router (LSR).
for *acl*	(Optional) Access list name or number that specifies a password is mandatory only for LDP sessions with neighbors whose LDP router IDs are permitted by the list. Only standard IP access lists can be used for the *acl* argument.

Command Default

If the **vrf** keyword is not specified in the command, the command applies to the global routing table.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command specifies that LDP must always use a password for an attempt to establish a session. If LDP cannot determine the password to use for an LDP session with a neighbor, an LDP session is not established.

The **vrf** keyword is available when you have configured a VRF on the LSR. If you specify a *vrf-name* argument and a VRF with that name is not configured on the LSR, a warning message is displayed and the command is discarded. If you remove a VRF, you also delete the password configured for that VRF.

Each VRF or global routing table can have zero or one **mpls ldp password required** command.

Examples

The following example shows how to specify that LDP must use a password for an attempt to establish a session between LDP peers:

```
Router> enable
Router# configure terminal
Router(config)# mpls ldp password required
```

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions
show mpls ldp neighbor password mpls	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp password rollover duration

To configure the duration before the new password takes effect on an MPLS label switch router (LSR), use the **mpls ldp password rollover duration** command in global configuration mode. To disable duration of a password rollover, use the **no** form of this command.

mpls ldp [**vrf** *vrf-name*] **password rollover duration** *minutes*
no mpls ldp [**vrf** *vrf-name*] **password rollover duration** *minutes*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a Virtual Private Network (VPN) routing/forwarding instance (VRF) configured on the label switch router (LSR).
minutes	Specifies the time, in minutes, before password rollover occurs on this router. The range is 5 to 65535.

Command Default

The MD5 password for LDP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

A lossless password rollover takes effect after the configured duration when passwords are configured without the use of a key chain.

Examples

The following example shows how to configure the duration before the new password takes effect on an LSR so there is enough time to successfully change all the passwords on all of the routers. In this example, a duration of 10 minutes is configured before the rollover occurs.

```
mpls ldp password rollover duration 10
```

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.

Command	Description
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp path-vector maxlength

To set the maximum number of router IDs permitted in a path vector type, length, value (TLV) used to perform path vector loop detection, use the **mpls ldp path-vector maxlength** command in global configuration mode. To return the path vector maximum length to the default behavior, use the **no** form of this command.

mpls ldp path-vector maxlength *number*
no mpls ldp path-vector maxlength

Syntax Description

number	Number from 0 to 254, inclusive, that defines the maximum number of 4-octet router IDs permitted in the path vector. The default behavior configured with the **no** form of this command is to track and use the value set by the**mpls ldp maxhops** command (1 to 255). A value of 0 disables the path-vector loop detection feature.

Command Default

If you do not configure this command, the default path vector maximum length value is whatever value is configured for the **mpls ldp maxhops** command. If you reconfigure the maximum hops value, the path vector maximum length value automatically changes to the new maximum hops value. If the **mpls ldp maxhops** command is not configured, the default value is 254.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(19)	This command was introduced.
12.4(8)	This command was integrated into Cisco IOS Release 12.4(8).
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

When an ATM label switch router (LSR) initiates a request for a label binding, and path vector loop detection is enabled, the request includes a path vector TLV that contains the router ID of the requesting router. Subsequent ATM LSRs along the path to the edge of the ATM label switching region add their router IDs to the path vector before forwarding the Label Request message to the next hop.

When an ATM LSR receives a Label Request message, it does not send a Label Mapping message in response, nor does it propagate the request to the destination next hop if a loop is detected by the path vector feature. Instead, the ATM LSR returns an error message that specifies that a loop has been detected. A loop is detected if either of the following occurs:

- The path vector length in the request equals or exceeds the configured Path Vector Limit value configured by the **mpls ldp path-vector maxlength** command.
- The receiving ATM LSR finds its own router ID within the path vector list.

Like the maximum hop count, the path vector limit threshold is used to prevent forwarding loops in the setting up of label switch path (LSPs) across an ATM region.

If you configured the **mpls ldp loop-detection** command for ATM LSRs that are sending and receiving Label Request and Label Map messages, you might want to inhibit the use of the path vector for loop detection (**mpls ldp path-vector maxlength 0** command).

To return the maximum path vector length to its default value, which is whatever value is configured for the **mpls ldp maxhops** command, use the **no mpls lsp path-vector maxlength** command.

Examples

The following example shows how to set the maximum path vector length to 100 router IDs:

```
configure terminal
mpls ldp path-vector maxlength 100
exit
```

The following example shows the maximum path vector length set to 254, which is verified by you looking at the output from the **show mpls ldp parameters** command or the **show mpls ldp neighbors detail** command:

```
configure terminal
mpls ldp path-vector maxlength 254
exit
Router# show mpls ldp parameters

Protocol version: 1
Downstream label generic region: min label: 16; max label: 100000
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 90 sec; interval: 10 sec
Downstream on Demand max hop count: 4
Downstream on Demand Path Vector Limit: 254   !Verifies maximum path-vector length is 254.
!
LDP for targeted sessions
LDP initial/maximum backoff: 15/120 sec
LDP loop detection: on
Router#
Router# show mpls ldp neighbor detail
Peer LDP Ident: 10.0.3.33:1; Local LDP Ident 10.0.2.93:1
    TCP connection: 10.0.3.33.53366 - 10.0.2.93.646
    State: Oper; Msgs sent/rcvd: 132/123; Downstream on demand
    Up time: 00:24:27; UID: 5; Peer Id 0;
    LDP discovery sources:
      Switch1.1; Src IP addr: 10.0.3.33
        holdtime: 15000 ms, hello interval: 5000 ms
    Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
    Clients: TC ATM
    Path Vector Loop Detection Peer/Local: On/On
    Path Vector Limit Peer/Local: 4/254  ! Verifies the maximum path-vector length is 254.
Router#
```

Related Commands

Command	Description
mpls ldp loop-detection	Enables the LDP optional loop detection mechanism.
mpls ldp maxhops	Limits the number of hops permitted in an LSP established by the Downstream on Demand method of label distribution.
mpls ldp router-id	Specifies a preferred interface for determining the LDP router ID.
show mpls ldp neighbors	Displays the status of LDP sessions.

Command	Description
show mpls ldp parameters	Displays current LDP parameters.

mpls ldp router-id

To specify a preferred interface for the Label Distribution Protocol (LDP) router ID, use the **mpls ldp router-id** command in global configuration mode. To disable the interface from being used as the LDP router ID, use the **no** form of this command.

mpls ldp router-id [**vrf** *vrf-name*] *interface* [**force**]
no mpls ldp router-id [**vrf** *vrf-name*] [*interface* [**force**]]

Cisco CMTS Routers
mpls ldp router-id gigabitethernet *slot*/*subslot*/*port*[{**force**}]
no mpls ldp router-id gigabitethernet *slot*/*subslot*/*port*[{**force**}]

Syntax Description

vrf *vrf-name*	(Optional) Selects the interface as the LDP router ID for the named Virtual Private Network (VPN) routing and forwarding (VRF) table. The selected interface must be associated with the named VRF.
interface	The specified interface to be used as the LDP router ID, provided that the interface is operational.
gigabitethernet *slot* /*subslot*/*port*	Specifies the location of the Gigabit Ethernet interface.
force	(Optional) Alters the behavior of the **mpls ldp router-id** command, as described in the "Usage Guidelines" section.

Command Default

If the **mpls ldp router-id** command is not executed, the router determines the LDP router ID as follows:

1. The router examines the IP addresses of all operational interfaces.
2. If these IP addresses include loopback interface addresses, the router selects the largest loopback address as the LDP router ID.
3. Otherwise, the router selects the largest IP address pertaining to an operational interface as the LDP router ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	The **force** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.

Release	Modification
12.4(5)	The **vrf** *vrf-name* keyword and argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **mpls ldp router-id** command allows you to use the IP address of an interface as the LDP router ID.

The following steps describe the normal process for determining the LDP router ID:

1. The router considers all the IP addresses of all operational interfaces.
2. If these addresses include loopback interface addresses, the router selects the largest loopback address. Configuring a loopback address helps ensure a stable LDP ID for the router, because the state of loopback addresses does not change. However, configuring a loopback interface and IP address on each router is not required.

The loopback IP address does not become the router ID of the local LDP ID under the following circumstances:

- • If the loopback interface has been explicitly shut down.
  • If the **mpls ldp router-id** command specifies that a different interface should be used as the LDP router ID.

If you use a loopback interface, make sure that the IP address for the loopback interface is configured with a /32 network mask. In addition, make sure that the routing protocol in use is configured to advertise the corresponding /32 network.

1. Otherwise, the router selects the largest interface address.

The router might select a router ID that is not usable in certain situations. For example, the router might select an IP address that the routing protocol cannot advertise to a neighboring router.

The router implements the router ID the next time it is necessary to select an LDP router ID. The effect of the command is delayed until the next time it is necessary to select an LDP router ID, which is typically the next time the interface is shut down or the address is deconfigured.

If you use the **force** keyword with the **mpls ldp router-id** command, the router ID takes effect more quickly. However, implementing the router ID depends on the current state of the specified interface:

- If the interface is up (operational) and its IP address is not currently the LDP router ID, the LDP router ID is forcibly changed to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down, the LDP router ID is forcibly changed to the IP address of the interface when the interface transitions to up. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

The following behaviors apply to the default VRF as well as to VRFs that you explicitly configure with the **vrf** *vrf-name* keyword and argument pair:

- The interface you select as the router ID of the VRF must be associated with the VRF.
- If the interface is no longer associated with the VRF, the **mpls ldp router-id** command that uses the interface is removed.
- If the selected interface is deleted, the **mpls ldp router-id** command that uses the interface is removed.
- If you delete a VRF that you configured, the **mpls ldp router-id** command for the deleted VRF is removed. The default VRF cannot be deleted.

Examples

The following example shows that the POS2/0/0 interface has been specified as the preferred interface for the LDP router ID. The IP address of that interface is used as the LDP router ID.

```
Router(config)# mpls ldp router-id pos2/0/0
```

The following example shows that the Ethernet 1/0 interface, which is associated with the VRF vpn-1, is the preferred interface. The IP address of the interface is used as the LDP router ID.

```
Router(config)# mpls ldp router-id vrf vpn-1 eth1/0
```

Related Commands

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls ldp session protection

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) autoconfiguration for existing LDP sessions or when new sessions are established, use the **mpls ldp session protection** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp session protection [**vrf** *vpn-name*] [**for** *acl*] [**duration** {**infinite***seconds*}]
no mpls ldp session protection [**vrf** *vpn-name*] [**for** *acl*] [**duration** {**infinite***seconds*}]

Syntax Description

vrf *vpn-name*	(Optional) Specifies a VPN routing and forwarding instance (*vpn-nam* e) for accepting labels. This keyword is available when the router has at least one VRF configured.
for *acl*	(Optional) Specifies a standard IP access control list that contains the prefixes that are to be protected.
duration	(Optional) Specifies the time that the LDP Targeted Hello Adjacency should be retained after a link is lost. **Note** If you use this keyword, you must select either the **infinite** keyword or the *seconds* argument.
infinite	Specifies that the LDP Targeted Hello Adjacency should be retained forever after a link is lost.
seconds	Specifies the time in seconds that the LDP Targeted Hello Adjacency should be retained after a link is lost. The valid range of values is 30 to 2,147,483 seconds.

Command Default

LDP sessions are not established.

Command Modes

Global configuration (config)

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.
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.

Usage Guidelines

This command is not supported under the following circumstances:

- With TDP sessions
- With extended access lists
- With LC-ATM routers

If you issue the **mpls ldp session protection** command without the **duration** keyword, then session protection is enabled for 86400 seconds (24 hours) meaning that the LDP Targeted Hello Adjacency is retained for 24 hours after a link is lost. This is the default timeout.

If you issue the **mpls ldp session protection duration infinite** command, then session protection is enabled forever meaning that the LDP Targeted Hello Adjacency is retained forever after a link is lost.

If you issue the **mpls ldp session protection duration** *seconds* command, then session protection is enabled for the number of seconds indicated meaning that the LDP Targeted Hello Adjacency is retained for that amount of time. For example, if you issued **mpls ldp session protection duration 100**, then the LDP Targeted Hello Adjacency is retained for 100 seconds after a link is lost.

Examples

In the following example, MPLS LDP Autoconfiguration is enabled for LDP sessions for peers whose router IDs are listed in access control list rtr4:

```
Router(config)# mpls ldp session protection for rtr4
```

Related Commands

Command	Description
clear mpls ldp neighbor	Forcibly resets an LDP session.
show mpls ldp neighbor	Displays the contents of the LDP.

mpls ldp sync

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization on interfaces for an Open Shortest Path First (OSPF) process or an Intermediate System-to-Intermediate System (IS-IS) process, use the **mpls ldp sync** command in router configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp sync
no mpls ldp sync

Syntax Description

This command has no arguments or keywords.

Command Default

MPLS LDP-IGP synchronization is not enabled on interfaces belonging to the OSPF or IS-IS processes.

Command Modes

Router configuration (config-router)

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.
12.0(32)SY	This command is supported on interfaces running IS-IS processes in Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

If the **mpls ldp sync** command is configured, you cannot enter the global **no mpls ip** command. If you want to disable LDP synchronization, you must enter the **no mpls ldp igp sync** command first.

The **mpls ldp sync** command is supported with OSPF or IS-IS. Other IGPs are not supported.

Examples

In the following example, MPLS LDP-IGP synchronization is enabled for an OSPF process or an IS-IS process:

```
Router(config-router)# mpls ldp sync
```

Related Commands

Command	Description
mpls ldp igp sync	Enables MPLS LDP-IGP synchronization on an interface that belongs to an OSPF process.

Command	Description
no mpls ip	Disables hop-by-hop forwarding.
show isis mpls ldp	Displays synchronization and autoconfiguration information about interfaces belonging to IS-IS processes.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls ldp tcp pak-priority

To give high priority to Label Distribution Protocol (LDP) messages sent by a router locally using Transmission Control Protocol (TCP) connections, use the **mpls ldp tcp pak-priority** command in global configuration mode. To keep LDP messages at normal priority, use the **no** form of this command.

mpls ldp tcp pak-priority
no mpls ldp tcp pak-priority

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

This command allows you to set high priority for LDP messages sent by a router locally using TCP connections.

During heavy network traffic, LDP session keepalive messages can be dropped from the outgoing interface output queue. As a result, keepalives can timeout causing LDP sessions to go down.

First, to avoid session loss due to keepalive timeouts, configure the quality of service (QoS) and differentiated services code point (DSCP) for packets with type of service (ToS) bits set to 6. This configuration guarantees that packets with a ToS bit precedence value of 6 receive a specified percentage of the bandwidth of the designated outgoing links. Second, if you still experience a problem, use the **mpls ldp tcp pak-priority** command.

Note Previously established LDP sessions are not affected when you issue the **no mpls ldp tcp pak-priority** or the**mpls ldp tcp pak-priority**command.

Examples

The following example gives LDP session messages sent by a router high priority locally:

```
Router(config)# mpls ldp tcp pak-priority
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
debug mpls ldp transport connections	Displays information about the TCP connections used to support LDP sessions.
match ip precedence	Identifies IP precedence values as match criteria.

Command	Description
match mpls experimental	Configures a class map to use the specified value of the EXP field as a match criterion.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

mpls load-balance per-label

To enable the load balancing for the tag-to-tag traffic, use the **mpls load-balance per-label** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mpls load-balance per-label
no mpls load-balance per-label

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

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.

Usage Guidelines

When you enable load balancing for the tag-to-tag traffic, the traffic is balanced based on the incoming label (per prefix) among Multiprotocol Label Switching (MPLS) interfaces. Each MPLS interface supports an equal number of incoming labels.

You can use the **show mpls ttfib** command to display the incoming label (indicated by an asterisk) that is included in the load balancer.

Examples

This example shows how to enable the load balancing for the tag-to-tag traffic:

```
Router(config)# mpls load-balance per-label
Router(config)#
```

This example shows how to disable the load balancing for the tag-to-tag traffic:

```
Router(config)# no mpls load-balance per-label
Router(config)#
```

Related Commands

Command	Description
show mpls ttfib	Displays information about the MPLS TTFIB table.

mpls mtu

To set the per-interface Multiprotocol Label Switching (MPLS) maximum transmission unit (MTU) for labeled packets, or to set the maximum MTU on the L3VPN profile, use the **mpls mtu** command in interface configuration mode or L3VPN encapsulation configuration mode respectively. To restore the MPLS MTU to the default value, use the**no** form of this command.

Interface Configuration Mode
mpls mtu [**override**] *bytes*
no mpls mtu

L3VPN Encapsulation Configuration Mode
mpls mtu max
no mpls mtu max

Syntax Description

override	(Optional) Allows you to set the MPLS MTU to a value higher than the interface MTU value on interfaces (such as Ethernet) that have a default interface MTU value of 1580 or less. The **override** keyword is not available for interface types that do not have a default MTU value of 1580 or less.
bytes	The MTU in bytes includes the label stack in the value.
max	Sets the MPLS MTU value to the maximum value in Generic Router Encapsulation (GRE) tunnels and L3VPN profiles.

Command Default

The default MPLS MTU is the MTU that is configured for the interface.

Command Modes

Interface configuration (config-if)
L3VPN encapsulation configuration (config-l3vpn-encap-ip)

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was modified to incorporate the new MPLS terminology.
12.2(25)S	This command was modified. The maximum allowable MPLS MTU values were changed. See the “Usage Guidelines for Cisco IOS Release 12.2(25)S” section for more information.
12.2(27)SBC	This command was modified. The MPLS MTU value cannot be set larger than the interface MTU value. The **override** keyword was added. See the “Usage Guidelines for Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and Later Releases” section for more information.
12.(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.

Release	Modification
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
Cisco IOS XE Release 2.6.0	This command was modified. The **maximum** keyword was added.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(2)S	This command was modified. This command was made available in L3VPN encapsulation configuration mode. The **maximum** keyword was replaced with the **max** keyword.

Usage Guidelines

Usage Guidelines for Cisco IOS Release 12.2(25)S

Caution Although you can set the MPLS MTU to a value greater than the interface MTU, you can set the MPLS MTU to less than or equal to the interface MTU to prevent data corruption, dropped packets, and high CPU conditions. A best practice is to set the interface MTU of the core-facing interface to a value greater than either the IP MTU or the interface MTU of the edge-facing interface.

If the interface MTU is less than 1524 bytes, you can set the maximum MPLS MTU to 24 bytes more than the interface MTU. For example, if the interface MTU is set to 1510 bytes, then you can set the maximum MPLS MTU to 1534 bytes (1510 + 24).

If the interface MTU is greater than or equal to 1524 bytes, then you can set the maximum MPLS MTU as high as the interface MTU. For example, if the interface MTU is set to 1600 bytes, then you can set the MPLS MTU to a maximum of 1600 bytes. If you set the MPLS MTU to a value higher than the interface MTU, traffic is dropped.

For interfaces that do not allow you to configure the interface MTU value and for interfaces where the MTU is 1500 bytes, the MPLS MTU range is from 64 to 1524 bytes.

If you upgrade to Cisco IOS Release 12.2(25)S from an earlier release and you have an MPLS MTU setting that does not conform to these guidelines, the system will not accept the MPLS MTU setting. You must reconfigure the MPLS MTU setting to conform to the guidelines.

Usage Guidelines for Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and Later Releases

In Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and later releases, you cannot set the MPLS MTU to a value larger than the interface MTU value. This is to prevent conditions such as dropped packets, data corruption, and high CPU rates.

- If you attempt to set the MPLS MTU to a value higher than the interface MTU value, the software displays the following error, which prompts you to set the interface MTU to a higher value before you set the MPLS MTU value:

```
% Please increase interface mtu to xxxx and then set mpls mtu
```

- If you have an interface with a default interface MTU value of 1580 or less (such as an Ethernet interface), the **mpls mtu** command provides the **override** keyword, which allows you to set the MPLS MTU to a value higher than the interface MTU value. The **override** keyword is not available for interface types that do not have a default interface MTU value of 1580 or less.

Note The **override** keyword is supported in 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and later releases.

- If you have configuration files with MPLS MTU values that are larger than the interface MTU values and you upgrade to Cisco IOS Release 2.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, or a later release, the software does not change the MPLS MTU value. When you reboot the router, the software accepts whatever values are set for the MPLS MTU and the interface MTU. The following error message is displayed during system initialization:

```
Setting the mpls mtu to xxxx on interface x/x, which is higher than the interface MTU xxxx.
 This could lead to packet forwarding problems including packet drops.
Set the MPLS MTU values lower than the interface MTU values.
```

Caution If you do not set the MPLS MTU to a value less than or equal to the interface MTU, data corruption, dropped packets, and high CPU conditions can occur.

- Changing the interface MTU can also modify the IP MTU, Connectionless Network Service (CLNS) MTU, and other MTU values, if they depend on the value of the interface MTU. The Open Shortest Path First (OSPF) routing protocol requires that the IP MTU values match on both ends of the link. Similarly, the Intermediate System-to-Intermediate System (IS-IS) routing protocol requires that the CLNS MTU values match on both ends of the link. If the values on both ends of the link do not match, IS-IS or OSPF cannot complete its initialization.

Usage Guidelines for Cisco IOS XE Release 2.6.0 and Cisco IOS Release 15.1(1)T

- You can set the MPLS MTU value for a GRE tunnel interface to either the default value or the maximum value that is supported by the platform for the interface.
- The **mpls mtu max** command allows previously dropped packets to pass through the GRE tunnel by fragmentation on the underlying physical interface.
- The MPLS MTU value cannot be greater than the interface MTU value for non-GRE tunnels.
- This command was enabled from Cisco IOS XE Release 3.11S onwards.

Usage Guidelines for Cisco IOS Release 15.1(2)S

- You can use the **mpls mtu max** command in L3VPN encapsulation configuration mode to set the MPLS MTU to the maximum value on L3VPN profiles.
- The **no** form of this command restores the MPLS MTU to the default value.

General Usage Guidelines

- ATM interfaces cannot accommodate packets that exceed the Segmentation and Reassembly (SAR) buffer size because labels are added to the packet. The *bytes* argument refers to the number of bytes in

the packet before the addition of any labels. If each label is 4 bytes, the maximum value of bytes on an ATM interface is the physical MTU minus 4*x bytes, where x is the number of labels expected in the received packet.

- If a labeled IPv4 packet exceeds the MPLS MTU size for the interface, the Cisco IOS software fragments the packet. If a labeled non-IPv4 packet exceeds the MPLS MTU size, the packet is dropped.
- All devices on a physical medium must have the same MPLS MTU value in order for MPLS to interoperate.
- The MTU for labeled packets on an interface is determined as follows:
  - If the **mpls mtu** *bytes* command has been used to configure an MPLS MTU, the MTU for labeled packets is the *bytes* value.
  - Otherwise, the MTU for labeled packets is the default MTU for the interface.
- Because labeling a packet makes it large due to the label stack, you may want the MPLS MTU to be larger than the interface MTU or IP MTU in order to prevent the fragmentation of the labeled packets, which would not be fragmented if they were unlabeled. In Cisco IOS Release 12.2(25)S and later releases, the MPLS MTU cannot be larger than the interface MTU.
- Changing the interface MTU value (using the **mtu** command) can affect the MPLS MTU of the interface. If the MPLS MTU value is the same as the interface MTU value (this is the default value), and you change the interface MTU value, the MPLS MTU value will automatically be set to this new MTU. However, the reverse is not true; changing the MPLS MTU value has no effect on the interface MTU.

Examples

The following example shows how to set the MPLS MTU value:

```
Router(config-if)# mpls mtu 1520
The following example shows the MPLS MTU value for a serial interface:
Router (config)# interface Serial4/0
Router (config-if)# mtu 1520
Router (config-if)# ip unnumbered Loopback0
Router (config-if)# mpls mtu 1510
Router (config-if)# mpls traffic-eng tunnels
Router (config-if)# mpls ip
Router (config-if)# serial restart-delay 0
Router (config-if)# ip rsvp bandwidth 2000 2000
```

The following example displays the maximum labeled packet size for the Fast Ethernet interface, which is common in an MPLS core carrying MPLS Virtual Private Network (VPN) traffic:

```
Router (config)# interface Fastethernet0
Router (config-if)# mpls mtu override 1508
The following example shows how to set the MPLS MTU value to the maximum MTU on L3VPN
profiles:
Router(config)# l3vpn encapsulation ip profile
Router(config-l3vpn-encap-ip)# mpls mtu max
```

Related Commands

Command	Description
mtu	Sets the MTU size for the interface.
show mpls interfaces detail	Displays detailed information about the interfaces that are configured for label switching.

mpls netflow egress

To enable Multiprotocol Label Switching (MPLS) egress NetFlow accounting on an interface, use the **mpls netflow egress** command in interface configuration mode. To disable MPLS egress NetFlow accounting, use the **no** form of this command.

mpls netflow egress
no mpls netflow egress

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
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)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

Use this command to configure the provider edge (PE) to customer edge (CE) interface of a PE router.

Examples

The following example shows how to enable MPLS egress NetFlow accounting on the egress PE interface that connects to the CE interface at the destination Virtual Private Network (VPN) site:

```
Router(config-if)# mpls netflow egress
```

Related Commands

Command	Description
debug mpls netflow	Enables debugging of MPLS egress NetFlow accounting.
show mpls forwarding-table	Displays a message that the quick flag is set for all prefixes learned from the MPLS egress NetFlow accounting enabled interface.
show mpls interfaces	Displays the value of the output_feature_state.

mpls oam

To enter MPLS OAM configuration mode for customizing the default behavior of echo packets, use the **mpls oam** command in global configuration mode. To disable MPLS OAM functionality, use the **no** format of this command.

mpls oam
no mpls oam

Syntax Description

This command has no arguments or keywords.

Command Default

Customizing the default behavior of echo packets is enabled.

Command Modes

Global configuration (config)

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	The **no** and **default** keywords were removed.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

After you enter the **mpls oam** command, you can enter the **echo** command in MPLS OAM configuration mode to specify the revision number of the echo packet's default values or to send the vendor's extension type, length, values (TLVs) with the echo packet.

Examples

The following example enters MPLS OAM configuration mode for customizing the default behavior of echo packets:

```
mpls oam
```

Related Commands

Command	Description
echo	Customizes the default behavior of echo packets.
ping mpls	Checks MPLS LSP connectivity.
trace mpls	Discovers MPLS LSP routes that packets will actually take when traveling to their destinations.

mpls prefix-map

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

To configure a router to use a specified quality of service (QoS) map when a label destination prefix matches the specified access list, use the **mpls prefix-map** command in ATM subinterface submode.

mpls prefix-map *prefix-map* **access-list** *access-list* **cos-map** *cos-map*

Syntax Description

prefix-map	Unique number for a prefix map.
access-list *access-list*	Unique number for a simple IP access list.
cos-map *cos-map*	Unique number for a QoS map.

Command Default

No access list is linked to a QoS map.

Command Modes

ATM subinterface submode (config-subif)

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.
12.4(20)T	This command was removed.

Usage Guidelines

This **mpls prefix-map** command links an access list to a QoS map when a label distribution prefix matches the specified access list.

Examples

The following example shows how to link an access list to a QoS map:

```
Router(config-subif)# mpls prefix-map 55 access-list 55 cos-map 55
```

Related Commands

Command	Description
show mpls prefix-map	Displays the prefix map used to assign a QoS map to network prefixes that match a standard IP access list.

mpls request-labels for

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls request-labels for** command is not available in Cisco IOS software.

To restrict the creation of label switched paths (LSPs) through the use of access lists on the label switch controller (LSC) or label edge router (LER), use the **mpls request-labels for** command in global configuration mode. To restrict the creation of LSPs through the use of access lists on the LSC or LER, use the **no** form of this command.

mpls request-labels for *access-list*
no mpls request-labels for

Syntax Description

access-list	A named or numbered standard IP access list.

Command Default

No LSPs are created using access lists on the LCS or LER.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) terminology.
12.4(20)T	This command was removed.

Usage Guidelines

The command includes the following usage guidelines:

- You can specify either an access list number or name.
- When you create an access list, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.
- If you omit the mask from an IP host address access list specification, 0.0.0.0 is assumed to be the mask.

Examples

The following example shows how to prevent headend label switched controlled virtual circuits (LVCs) from being established from the LSC to all 192.168.x.x destinations. The following commands are added to the LSC configuration:

```
Router(config)# mpls request-labels for 1
Router(config)# access-list 1 deny 192.168.0.0 0.255.255.255
Router(config)# access-list 1 permit any
```

Related Commands

Command	Description
access-list	Creates access lists.
ip access-list	Permits or denies access to IP addresses.

mpls static binding ipv4

To bind a prefix to a local or remote label, use the **mpls static binding ipv4** command in global configuration mode. To remove the binding between the prefix and label, use the **no** form of this command.

mpls static binding ipv4 *prefix mask* {*label* | **input** *label* | **output** *nexthop* {**explicit-null** | **implicit-null***label*}}
no mpls static binding ipv4 *prefix mask* {*label* | **input** *label* | **output** *nexthop* {**explicit-null** | **implicit-null***label*}}

Syntax Description

prefix mask	Specifies the prefix and mask to bind to a label. (When you do not use the **input** or **output** keyword, the specified label is an incoming label.) **Note** Without the arguments, the **no** form of the command removes all static bindings.
label	Binds a prefix or a mask to a local (incoming) label. (When you do not use the **input** or **output** keyword, the specified label is an incoming label.)
input *label*	Binds the specified label to the prefix and mask as a local (incoming) label.
output *nexthop* **explicit-null**	Binds the Internet Engineering Task Force (IETF) Multiprotocol Label Switching (MPLS) IPv4 explicit null label (0) as a remote (outgoing) label.
output *nexthop* **implicit-null**	Binds the IETF MPLS implicit null label (3) as a remote (outgoing) label.
output *nexthop label*	Binds the specified label to the prefix/mask as a remote (outgoing) label.

Command Default

Prefixes are not bound to local or remote labels.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
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 2.2	This command was integrated into Cisco IOS XE Release 2.2. The command output changed.
Cisco IOS XE Release 3.5S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

The mpls static binding ipv4 command pushes bindings into Label Distribution Protocol (LDP). LDP then needs to match the binding with a route in the Routing Information Base (RIB) or Forwarding Information Base (FIB) before installing forwarding information.

The mpls static binding ipv4 command installs the specified bindings into the LDP Label Information Base (LIB). LDP will install the binding labels for forwarding use if or when the binding prefix or mask matches a known route.

Static label bindings are not supported for local prefixes, which are connected networks, summarized routes, default routes, and supernets. These prefixes use implicit-null or explicit-null as the local label.

If you do not specify the **input** or the **output** keyword, input (local label) is assumed.

For the **no** form of the command:

- If you specify the command name without any keywords or arguments, all static bindings are removed.
- Specifying the prefix and mask but no label parameters removes all static bindings for that prefix or mask.

Examples

In the following example, the **mpls static binding ipv4** command configures a static prefix and label binding before the label range is reconfigured to define a range for static assignment. The output of the command indicates that the binding has been accepted, but cannot be used for MPLS forwarding until you configure a range of labels for static assignment that includes that label.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55
 % Specified label 55 for 10.0.0.0/8 out of configured
 % range for static labels.  Cannot be used for forwarding until
 % range is extended.
Router(config)# end
```

The following **mpls static binding ipv4** commands configure input and output labels for several prefixes:

```
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 output 10.0.0.66 2607
Router(config)# mpls static binding ipv4 10.66.0.0 255.255.0.0 input 17
Router(config)# mpls static binding ipv4 10.66.0.0 255.255.0.0 output 10.13.0.8 explicit-null
Router(config)# end
```

The following **show mpls static binding ipv4** command displays the configured bindings:

```
Router# show mpls static binding ipv4

10.0.0.0/8: Incoming label: 55
  Outgoing labels:
    10.0.0.66   2607
10.66.0.0/24: Incoming label: 17
  Outgoing labels:
    10.13.0.8    explicit-null
```

Related Commands

Command	Description
show mpls forwarding-table	Displays labels currently being used for MPLS forwarding.

Command	Description
show mpls label range	Displays statically configured label bindings.

mpls static binding ipv4 vrf through mpls traffic-eng logging tunnel

mpls static binding ipv4 vrf

To bind a prefix to a local label, use the **mpls static binding ipv4 vrf** command in global configuration mode. To remove static binding between the prefix and label, use the **no** form of this command.

mpls static binding ipv4 vrf *vpn-name prefix mask* {**input** *labellabel*}
no mpls static binding ipv4 vrf *vpn-name prefix mask* [{**input** *labellabel*}]

Syntax Description

vpn-name	The VPN routing and forwarding (VRF) instance.
prefix mask	The destination prefix and mask.
input *label*	A local (incoming) label. This argument is optional for the **no** form of the command.
label	A local label. This argument is optional for the **no** form of the command.

Command Default

Label bindings are dynamically assigned.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(26)S	This command was introduced.
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

The **mpls static binding ipv4 vrf** command is used only when you configure input labels.

Depending on how you configure the MPLS LDP VRF-Aware Static Labels feature, static labels are advertised one of the following ways:

- By Label Distribution Protocol (LDP) between provider edge (PE) and customer edge (CE) routers within a VRF instance.
- In VPNv4 Border Gateway Protocol (BGP) in the service provider's backbone.

If you do not specify the **input** keyword, an input (local) label is assumed.

The **no** form of the command functions as follows:

- Omitting the prefix and the subsequent parameters removes all static bindings.
- Specifying the prefix and mask but no label parameters removes all static bindings for that prefix or mask.

Examples

The following example binds a prefix to local label 17:

```
Router(config)# mpls static binding ipv4 vrf vpn100 10.66.0.0 255.255.0.0 input 17
```

Related Commands

Command	Description
show mpls static binding ipv4 vrf	Displays configured static bindings.

mpls static crossconnect

To configure a Label Forwarding Information Base (LFIB) entry for the specified incoming label and outgoing interface, use the **mpls static crossconnect** command in global configuration mode. To remove the LFIB entry, use the **no** form of this command.

mpls static crossconnect *inlabel out-interface nexthop* {*outlabel* | **explicit-null** | **implicit-null**}
no mpls static crossconnect *inlabel out-interface nexthop* {*outlabel* | **explicit-null** | **implicit-null**}

Syntax Description

inlabel	The incoming label.
out-interface	The outgoing interface.
nexthop	The destination next hop router. (Use for multiaccess interfaces only.)
outlabel	The outgoing label.
explicit-null	Specifies the Internet Engineering Task Force (IETF) Multiprotocol Label Switching (MPLS) IPv4 explicit null label (0).
implicit-null	Specifies the IETF MPLS implicit null label (3).

Command Default

Cross connects are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
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.

Usage Guidelines

You must specify the next hop address for multiaccess interfaces.

Examples

In the following example, the **mpls static crossconnect** command configures a cross connect from incoming label 45 to outgoing label 46 through POS interface POS5/0:

```
Router(config)# mpls static crossconnect 45 pos5/0 46
```

Related Commands

Command	Description
show mpls static crossconect	Displays statically configured LFIB entries.

mpls tp

To configure Multiprotocol Label Switching (MPLS)-Transport Profile (TP) parameters and enter MPLS-TP configuration mode, use the **mpls tp** command in global configuration mode. To remove all MPLS-TP forwarding, use the **no** form of this command.

mpls tp
no mpls tp

Syntax Description

This command has no arguments or keywords.

Command Default

No MPLS-TP parameters are configured.

Command Modes

Global configuration (config)

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.

Usage Guidelines

Use this command to enter MPLS-TP configuration mode. From that mode, you can configure the parameters listed in the table below.

Table 5: Parameters for mpls tp Command

Command	Parameter
fault-oam refresh-timer *secs*	(Optional) Specifies the maximum time between successive fault Operation, Administration, and Maintenance (OAM) messages, specified in seconds. The range is from 1 to 20. The default is 5.
global-id *num*	(Optional) Specifies the default global ID used for all endpoints and midpoints. The range is from 0 to 2147483647. The default is 0. This command makes the router ID globally unique in a multiprovider tunnel. Otherwise, the router ID is only locally meaningful. The global ID is an autonomous system number, which is a controlled number space by which providers can identify each other.

Command	Parameter
protection trigger [**ais** | **ldi** | **lkr**]	(Optional) Specifies protection triggers for alarm indication signal (AIS), link down indication (LDI), lock report (LKR) messages. These triggers should be used in rare cases. They allow you to change the default protection-switching behavior for fault notifications on all tunnels. The default for these global settings is to trigger protection on receipt of LDI and LKR, but not AIS. (AIS is a nonfatal indication of potential issues, which turns into LDI when it is known to be fatal.) This command is useful when other devices send AIS or LDI in unexpected ways. For example, you can configure the **protection trigger ais** command to interoperate with another vendor whose devices send AIS when there are link failures and never send AIS with the LDI flag. Another example is if a device sends LDI when there is no actual failure, but there is a possible failure, and you want bidirectional forwarding detection (BFD) to detect the actual failure and cause protection switching, you can configure the **no protection trigger ldi** command. To undo these configuration settings and revert to the default settings, use the **default protection trigger** [**ais** | **ldi** | **lkr**] command.
router-id*router-id*	(Required) Specifies the default MPLS-TP router ID, which is used as the source node ID for all MPLS-TP tunnels configured on the router. This is required for MPLS-TP forwarding. This router ID is used in fault OAM messaging to identify the source of a fault on a midpoint router.
wtr-timer	Specifies the wait-to-restore (WTR) timer. This timer controls the length of time to wait before reversion following the repair of a fault on the original working path.

Examples

The following example shows how to enter MPLS-TP configuration mode and set the default router ID:

```
Router(config)# mpls tp

Router(config-mpls-tp)# router-id 10.10.10.10
Router(config-mpls-tp)# exit
```

Related Commands

Command	Description
interface tunnel-tp	Specifies the parameters for a MPLS tunnel.
mpls tp lsp	Specifies parameters for two ends of the MPLS-TP tunnel from a tunnel midpoint.
psc	Enables PSC.
working-lsp	Enters working LSP mode on a TP tunnel interface.

mpls tp link

To configure Multiprotocol Label Switching (MPLS) transport profile (TP) link parameters, use the **mpls tp link** command in interface configuration mode.

mpls tp link *link-num* {**ipv4** *ip-address* | **tx-mac** *mac-address*} **rx-mac** *mac-address*
no mpls tp link *link-num*

Syntax Description

link-num	Number assigned to the link. It must be unique on the device. Only one link number can be assigned per interface. Range: 1 to 2147483647.
ipv4 *ip-address*	The next-hop address that Address Resolution Protocol (ARP) uses to discover the destination MAC address.
tx-mac *mac-address*	Specifies a per-interface transmit multicast MAC address. This keyword is available on point-to-point Ethernet interfaces and non point-to-point interfaces where the MAC address is a unicast address. It is not available on serial interfaces.
rx-mac *mac-address*	Specifies a per-interface receive multicast MAC address. This keyword is available only when the **tx-mac** keyword is used. It is not available on serial interfaces.

Command Default

No MPLS-TP link parameters are configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Usage Guidelines

The link number must be unique on the device. Only one link number can be assigned per interface.

MPLS-TP link numbers may be assigned to physical interfaces only. Bundled interfaces and virtual interfaces are not supported for MPLS-TP link numbers.

When an MPLS-TP link is configured without an IP address on an Ethernet interface, Cisco uses an IEEE Bridge Group MAC address (0180.c200.0000) for communication by default.

Examples

This example creates an MPLS-TP link without an IP address:

```
interface e0/0
 medium p2p
 mpls tp link 1
```

This example configures the unicast MAC address of the next-hop device:

```
interface e0/0
 medium p2p
 mpls tp link 1 tx-mac 0000.0c00.1234
```

This example configures transmit and receive parameters for a different multicast address:

```
interface e0/0
 medium p2p
 mpls tp link 1 tx-mac 0100.0c99.8877 rx-mac 0100.0c99.8877
```

This example configures a link with an IP adress:

```
interface e0/0
      ip address 10.0.0.1 255.255.255.0
      mpls tp link 1 ipv4 10.0.0.2
```

Related Commands

Command	Description
mpls tp lsp	Specifies the parameters for forwarding of a MPLS-TP LSP at the tunnel midpoint.
interface tunnel-tp	Specifies the parameters for the MPLS tunnel.

mpls tp lsp

To configure Multiprotocol Label Switching (MPLS) transport profile (TP) midpoint connectivity, use the **mpls tp lsp** command in global configuration mode.

mpls tp lsp source *node-id* [**global-id** *num*] **tunnel-tp** *num* **lsp** {*lsp-num* | **protect** | **working**} **destination** *node-id* [**global-id** *num*] **tunnel-tp** *num*

Syntax Description

source *node-id*	Specifies the source node ID of the MPLS-TP tunnel.
global-id *num*	(Optional) Specifies the global ID of the tunnel source.
tunnel-tp *num*	Specifies the tunnel-TP number of MPLS-TP tunnel source.
lsp {*lsp-num* | **protect** | **working**}	Specifies the label switched path (LSP) within the MPLS-TP tunnel. • *lsp-num*— the number of the LSP. • **protect—** Indicates that the LSP is a backup for the primary, or working, LSP. When you specify the **protect** keyword, the LSP number is 1. • working**—**Indicates that the LSP is the primary LSP. When you specify the **working** keyword, the LSP number is 0. A protect LSP is a backup for a working LSP. When the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time forwarding reverts back to the working LSP.
destination *node-id*	Specifies the destination node ID of the MPLS-TP tunnel.
global-id *num*	(Optional) Specifies the global ID of the tunnel destination. Range: 0 to 2147483647 Default: 0.
tunnel-tp *num*	Specifies the tunnel number of MPLS-TP tunnel destination.

Command Default

No MPLS-TP parameters are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Usage Guidelines

Use this command on midpoint routers to specify the source and destination parameters of the MPLS-TP tunnel. You can use the **mpls trace** command from the MPLS-TP endpoint to validate that traffic is traversing the correct tunnel at each midpoint.

This command also enters MPLS-TP LSP configuration mode (config-mpls-tp-lsp). From that mode, you can configure the following parameters:

Command	Parameter
forward-lsp	Enters MPLS-TP LSP forward LSP configuration mode (config-mpls-tp-lsp-forw). From this mode, you can configure the following parameters: • Bandwidth (**bandwidth**) • Incoming label (**in-label**) and outgoing label and link numbers (**out-label out-link**)
reverse-lsp	Enters MPLS-TP LSP reverse LSP configuration mode (config-mpls-tp-lsp-rev). From this mode, you can configure the following parameters: • Bandwidth (**bandwidth**) • Incoming label (**in-label**) and outgoing label and link numbers (**out-label out-link**)
tunnel-name *name*	Specifies the name of the MPLS-TP tunnel.

Examples

The following examples show the configuration of an MPLS-TP LSP midpoint.

The following example configures a midpoint LSP carrying the working LSP of an MPLS-TP tunnel between node 10.10.10.10, tunnel-number 1 and 10.11.11.11, tunnel-number 2, using 1000 kbits/sec bandwidth in both directions:

```
Router(config)# mpls tp lsp source 10.10.10.10 tunnel-tp 1 lsp working destination 10.11.11.11
 tunnel-tp 2
Router(config-mpls-tp-lsp)# forward-lsp
Router(config-mpls-tp-lsp-forw)# bandwidth 1000
Router(config-mpls-tp-lsp-forw)# in-label 20 out-label 40 out-link 10
Router(config-mpls-tp-lsp-forw)# exit
Router(config-mpls-tp-lsp)# reverse-lsp
Router(config-mpls-tp-lsp-rev)# bandwidth 1000
Router(config-mpls-tp-lsp-rev)# in-label 21 out-label 50 out-link 11
```

The following example configures a midpoint LSP on the protect LSP between node 10.10.10.10, tunnel 4 and 10.11.11.11, tunnel 12. No bandwidth is reserved:

```
Router(config)# mpls tp lsp source 10.10.10.10 global-id 2 tunnel-tp 4 lsp protect destination
 10.11.11.11 global-id 14 tunnel-tp 12
Router(config-mpls-tp-lsp)# forward-lsp
Router(config-mpls-tp-lsp-forw)# in-label 30 out-label 100 out-link 27
Router(config-mpls-tp-lsp-forw)# exit
Router(config-mpls-tp-lsp)# reverse-lsp
Router(config-mpls-tp-lsp-rev)# in-label 31 out-label 633 out-link 30
```

Related Commands

Command	Description
interface tunnel-tp	Specifies the parameters for the MPLS-TP tunnel.

Command	Description
mpls tp	Specifies the parameters for the MPLS-TP tunnel and enters MPLS-TP configuration mode.
mpls tp link	Specifies MPLS-TP link parameters.

mpls traffic-eng

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

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

Syntax Description

level-1	Floods MPLS TE link information into IS-IS level 1.
level-2	Floods MPLS TE link information into IS-IS level 2.

Command Default

Flooding is disabled.

Command Modes

Router configuration (config-router)

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.
12.2SX	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)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command, which is part of the routing protocol tree, causes link resource information (such as available bandwidth) for appropriately configured links to be flooded in the IS-IS link-state database.

Examples

The following example shows how to configure MPLS TE link information flooding for IS-IS level 1:

```
Router(config-router)# mpls traffic-eng level-1
```

Related Commands

Command	Description
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.

mpls traffic-eng administrative-weight

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

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

Syntax Description

weight	Cost of the link.

Command Default

None

Command Modes

Interface configuration (config-if)

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)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Examples

The following example shows how to override the IGP cost of the link and set the cost to 20:

```
Router(config-if)# mpls traffic-eng administrative-weight 20
```

Related Commands

Command	Description
mpls traffic-eng attribute-flags	Sets the user-specified attribute flags for an interface.

mpls traffic-eng area

To configure a router running Open Shortest Path First (OSPF) Multiprotocol Label Switching (MPLS) so that it floods traffic engineering for the indicated OSPF area, use the **mpls traffic-eng area** command in router configuration mode. To disable flooding of traffic engineering for the indicated OSPF area, use the **no** form of this command.

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

Syntax Description

number	The OSPF area on which MPLS traffic engineering is enabled.

Command Default

Flooding is disabled.

Command Modes

Router configuration (config-router)

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 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

This command is in the routing protocol configuration tree and is supported for both OSPF and IS-IS. The command affects the operation of MPLS traffic engineering only if MPLS traffic engineering is enabled for that routing protocol instance. Currently, only a single level can be enabled for traffic engineering.

Examples

The following example shows how to configure a router running OSPF MPLS to flood traffic engineering for OSPF 0:

```
Router(config-router)# mpls traffic-eng area 0
```

Related Commands

Command	Description
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

Command	Description
router ospf	Configures an OSPF routing process on a router.

mpls traffic-eng atm cos global-pool

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls traffic-eng atm cos global-pool** command is not available in Cisco IOS software.

To specify the class of service for all global pools in traffic engineering tunnels traversing XTagATM interfaces on an ATM-label switch router (LSR), use the **mpls traffic-eng atm cos global-pool** command in global configuration mode.

mpls traffic-eng atm cos global-pool [{**available** | **standard** | **premium** | **control**}]

Syntax Description

available | **standard**| **pr e mium**| **control**	(Optional) Four classes of service, ordered from lowest priority (**available**) to highest priority (**control**). The default is **available**.

Command Default

The default class is the lowest, **available**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

Because this command works at the global rather than at the interface level, it sets the same class of service for global pool traffic engineering (TE) tunnel traffic on *all* XTagATM interfaces of the device.

Examples

The following example shows how to specify the second-lowest possible priority class of service for the global pool traffic:

```
Router(config)# mpls traffic-eng atm cos global-pool standard
```

Related Commands

Command	Description
mpls traffic-eng atm cos sub-pool	Specifies class of service for subpool traffic traversing XtagATM interfaces.

mpls traffic-eng atm cos sub-pool

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls traffic-eng atm cos sub-pool** command is not available in Cisco IOS software.

To specify the class of service for all subpools in traffic engineering tunnels traversing XTagATM interfaces on an ATM-label switch router (LSR), use the **mpls traffic-eng atm cos sub-pool** command in global configuration mode.

mpls traffic-eng atm cos sub-pool [{**available** | **standard** | **premium** | **control**}]

Syntax Description

available | **standard** | **premium** | **control**	Four classes of service, ordered from lowest priority (**available**) to highest priority (**control**). The default is **control**.

Command Default

The default class is the highest, **control**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

Because this command works at the global rather than at the interface level, it sets the same class of service for subpool traffic engineering (TE) tunnel traffic on *all* XTagATM interfaces of the device.

Examples

The following example shows how to specify the second-highest possible priority class of service for the subpool traffic:

```
Router(config)# mpls traffic-eng atm cos sub-pool premium
```

Related Commands

Command	Description
mpls traffic-eng atm cos global-pool	Specifies class of service for global-pool traffic traversing XTagATM interfaces.

mpls traffic-eng attribute-flags

To set the user-specified attribute flags for the interface, use the **mpls traffic-eng attribute-flags** command in interface configuration mode. To disable the user-specified attribute flags for the interface, use the **no** form of this command.

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

Syntax Description

attributes	Attributes that will be compared to a tunnel's affinity bits during selection of a path. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits) where the value of an attribute is 0 or 1.

Command Default

None

Command Modes

Interface configuration (config-if)

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)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

This command assigns attributes to a link so that tunnels with matching attributes (represented by their affinity bits) prefer this link to others that do not match.

The interface is flooded globally so that it can be used as a tunnel head-end path selection criterion.

Examples

The following example shows how to set the attribute flags to 0x0101:

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

Related Commands

Command	Description
mpls traffic-eng administrative-weight	Overrides the IGP administrative weight of the link.
tunnel mpls traffic-eng affinity	Configures affinity (the properties that the tunnel requires in its links) for an MPLS traffic engineering tunnel.

mpls traffic-eng auto-bw timers

To enable automatic bandwidth adjustment for a platform and to start output rate sampling for tunnels configured for automatic bandwidth adjustment, use the **mpls traffic-eng auto-bw timers** command in global configuration mode. To disable automatic bandwidth adjustment for the platform, use the **no** form of this command.

mpls traffic-eng auto-bw timers [**frequency** *seconds*]
no mpls traffic-eng auto-bw timers

Syntax Description

frequency *seconds*	(Optional) Interval, in seconds, for sampling the output rate of each tunnel configured for automatic bandwidth. The range is 1 to 604800. The recommended value is 300.

Command Default

When the optional **frequency** keyword is not specified, the sampling interval is 300 seconds (5 minutes).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)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.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **mpls traffic-eng auto-bw timers** command enables automatic bandwidth adjustment on a platform by causing traffic engineering to periodically sample the output rate for each tunnel configured for bandwidth adjustment.

The **no mpls traffic-eng auto-bw timers** command disables automatic bandwidth adjustment for a platform by terminating the output rate sampling and bandwidth adjustment for tunnels configured for adjustment. In addition, the **no** form of the command restores the configured bandwidth for each tunnel where “configured bandwidth” is determined as follows:

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

Examples

The following example shows how to designate that for each Multiprotocol Label Switching (MPLS) traffic engineering tunnel, the output rate is sampled once every 10 minutes (every 600 seconds):

```
Router(config)# mpls traffic-eng auto-bw timers frequency 600
```

Related Commands

Command	Description
tunnel mpls traffic-eng auto-bw	Enables automatic bandwidth adjustment for a tunnel, specifies the frequency with which tunnel bandwidth can be automatically adjusted, and designates the allowable range of bandwidth adjustments.
tunnel mpls traffic-eng bandwidth	Configures bandwidth required for an MPLS traffic engineering tunnel.

mpls traffic-eng auto-tunnel backup

To automatically build next-hop (NHOP) and next-next hop (NNHOP) backup tunnels, use the **mpls traffic-eng auto-tunnel backup** command in global configuration mode. To delete the NHOP and NNHOP backup tunnels, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup
no mpls traffic-eng auto-tunnel backup

Syntax Description

This command has no arguments or keywords.

Command Default

No backup tunnels exist.

Command Modes

Global configuration (config)

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.
15.2(2)S	This command was modified. The usage guidelines changed on hardware that supports dual Route Processors (RPs).
Cisco IOS XE Release 3.6S	This command was modified. The usage guidelines changed on hardware that supports dual RPs.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **no** form of this command deletes both NHOP and NNHOP backup tunnels that were configured using either the **mpls traffic-eng auto-tunnel backup** command or the **mpls traffic-eng auto-tunnel backup nhop-only** command.

On hardware that supports dual RPs, once this command is enabled, the tunnel is created on both the active and the standby RPs. When the **no** form of the command is executed, the tunnel is deleted on both the active and the standby RPs.

Examples

The following example automatically builds NHOP and NNHOP backup tunnels:

```
Router(config)# mpls traffic-eng auto-tunnel backup
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel backup nhop-only	Enables the creation of only dynamic next-hop backup tunnels.
mpls traffic-eng auto-tunnel backup timers	Configures how frequently a timer will scan backup autotunnels and remove tunnels that are not being used.
mpls traffic-eng auto-tunnel backup tunnel-num	Configures the range of tunnel interface numbers for backup autotunnels.

mpls traffic-eng auto-tunnel backup config

To configure a specific unnumbered interface for all backup auto-tunnels, use the **mpls traffic-eng auto-tunnel backup config** command in global configuration mode. To remove the specific interface and resume the default interface for all backup auto-tunnels, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup config unnumbered-interface *interface*
no mpls traffic-eng auto-tunnel backup config unnumbered-interface

Syntax Description

unnumbered-interface *interface*	Interface for all backup auto-tunnels. Default: Loopback0.

Command Default

Loopback0

Command Modes

Global configuration (config)

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.
15.1(1)S	This command was modified. In Cisco IOS Release 15.1(1)S, this command changed so that you do not need to specific the interface name when you specify the **no** form of this command. In releases prior to 15.1(1)S, you had to specify the interface name as part of the **no** form of the command.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

In Cisco IOS Release 15.1(1)S, this command changed so that you do not need to specific the interface name when you specify the **no** form of this command. In release prior to 15.1(1)S, you had to specify the interface name as part of the **no** form of the command. If you upgrade to Cisco IOS Release 15.1(1)S, check that your configuration does not contain the interface name as part of the **mpls traffic-eng auto-tunnel backup config** command.

Examples

The following example assigns interface Ethernet 1/0 to all backup auto-tunnels:

```
Router# mpls traffic-eng auto-tunnel backup config unnumbered-interface ethernet1/0
```

The following example assigns the default interface of loopback0 to all backup auto-tunnels:

```
Router# no
mpls traffic-eng auto-tunnel backup config unnumbered-interface
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup	Automatically builds NHOP and NNHOP backup tunnels.
mpls traffic-eng auto-tunnel backup nhop-only	Enables the creation of only dynamic next-hop backup tunnels.
mpls traffic-eng auto-tunnel backup timers	Configures how frequently a timer will scan backup autotunnels and remove tunnels that are not currently being used.
mpls traffic-eng auto-tunnel backup tunnel-num	Configures the range of tunnel interface numbers for backup autotunnels.

mpls traffic-eng auto-tunnel backup config affinity

To specify an affinity on dynamically created Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) backup tunnels, use the **mpls traffic-eng auto-tunnel backup config affinity** command in global configuration mode. To return to the default values, use the **no** form of the command.

mpls traffic-eng auto-tunnel backup config affinity *affinity-value* [**mask** *mask-value*]
no mpls traffic-eng auto-tunnel backup config affinity

Syntax Description

affinity-value	Values that will be compared to the link attributes during selection of a path. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits) where the value of an attribute is 0 or 1.
mask *mask-value*	(Optional) Affinity value flag. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of the affinity bit is 0 or 1. A value of 0 means ignore the corresponding affinity bit.

Command Default

Affinity: 0x0 mask: 0xFFFF

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

This command is used with the **mpls traffic-eng attribute-flags** command, which specifies attributes for a link so that tunnels with matching affinity bits will use that link.

With the autotunnel backup feature, you can use the **mpls traffic-eng attribute-flags** and **mpls traffic-eng auto-tunnel backup config affinity** commands to include or exclude links when calculating a path for a dynamically created backup tunnel.

The affinity determines the attributes of the links that this tunnel will use (that is, the attributes for which the tunnel has an affinity). The attribute mask determines which link attribute the router should check. If a bit in the mask is 0, an attribute value of a link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of a link and the required affinity of the tunnel for that bit must match.

A tunnel can use a link if:

```
tunnel affinity = the link attributes && the tunnel affinity mask
```

Any properties set to 1 in the affinity should also be 1 in the mask.

Examples

The following example configures all dynamically created backup with affinity 0x22, mask 0x22:

```
Router (config)# mpls traffic-eng auto-tunnel backup config affinity 0x22 mask 0x22
```

Related Commands

Command	Description
mpls traffic-eng attribute-flags	Specifies attributes for a link so that tunnels with matching affinity bits will use that link.
mpls traffic-eng auto-tunnel backup	Automatically builds NHOP and NNHOP backup tunnels.
show mpls traffic-eng auto-tunnel backup	Displays information about dynamically created backup tunnels.
tunnel mpls traffic-eng affinity	Configure an affinity for the interface.

mpls traffic-eng auto-tunnel backup nhop-only

To automatically build next-hop (NHOP) backup tunnels, use the **mpls traffic-eng auto-tunnel backup nhop-only** command in global configuration mode. To delete the NHOP backup tunnels, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup nhop-only
no mpls traffic-eng auto-tunnel backup nhop-only

Syntax Description

This command has no arguments or keywords.

Command Default

The dynamically created backup tunnel uses Loopback0.

Command Modes

Global configuration (config)

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.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command permits the creation of only NHOP backup tunnels; next-next hop (NNHOP) backup tunnels are not created. The **no** form of this command deletes only the NHOP backup tunnels; NNHOP backup tunnels are not deleted.

Examples

The following example enables the creation of only dynamic NHOP backup tunnels:

```
Router# mpls traffic-eng auto-tunnel backup nhop-only
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup	Automatically builds NHOP and NNHOP backup tunnels.
mpls traffic-eng auto-tunnel backup config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel backup timers	Configures how frequently a timer will scan backup autotunnels and remove tunnels that are not being used.
mpls traffic-eng auto-tunnel backup tunnel-num	Configures the range of tunnel interface numbers for backup autotunnels.

mpls traffic-eng auto-tunnel backup srlg exclude

To specify that autocreated backup tunnels should avoid Shared Risk Link Groups (SRLGs) of the protected interface, use the **mpls traffic-eng auto-tunnel backup srlg exclude** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup srlg exclude {**force** | **preferred**}
no mpls traffic-eng auto-tunnel backup srlg exclude

Syntax Description

force	Forces the backup tunnel to avoid SRLGs of its protected interfaces.
preferred	Causes the backup tunnel to *try* to avoid SRLGs of its protected interfaces, but the backup tunnel can be created if SRLGs cannot be avoided.

Command Default

Autocreated backup tunnels are created without regard to SRLGs.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(28)S	This command was introduced.
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

If you enter the command with either the **force** or the **preferred** keyword and then reenter the command with the other keyword, only the last command entered is effective.

Examples

In the following example, backup tunnels must avoid SRLGs of the protected interface:

```
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force
```

In the following example, backup tunnels should *try* to avoid SRLGs of the protected interface:

```
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude preferred
```

Related Commands

Command	Description
mpls traffic-eng srlg	Configures the SRLG membership of a link (interface).

mpls traffic-eng auto-tunnel backup timers

To configure how frequently a timer will scan backup autotunnels and remove tunnels that are not being used, use the **mpls traffic-eng auto-tunnel backup timers** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup timers removal unused [*sec*]
no mpls traffic-eng auto-tunnel backup timers removal unused [*sec*]

Syntax Description

removal unused [*sec*]	Configures how frequently (in seconds) a timer will scan the backup autotunnels and remove tunnels that are not being used. The range is 0 to 604,800.

Command Default

The timer scans backup autotunnels and removes tunnels that are not being used every 3600 seconds (60 minutes).

Command Modes

Global configuration (config)

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.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example shows that a timer scans backup autotunnels every 80 seconds and remove tunnels that are not being used:

```
Router(config)# mpls traffic-eng auto-tunnel backup timers removal unused 80
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup	Automatically builds NHOP and NNHOP backup tunnels.
mpls traffic-eng auto-tunnel backup config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel backup nhop-only	Enables the creation of only dynamic next-hop backup tunnels.
mpls traffic-eng auto-tunnel backup tunnel-num	Configures the range of tunnel interface numbers for backup autotunnels.

mpls traffic-eng auto-tunnel backup tunnel-num

To configure the range of tunnel interface numbers for backup autotunnels, use the **mpls traffic-eng auto-tunnel backup tunnel-num** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup tunnel-num [**min** *num*] [**max** *num*]
no mpls traffic-eng auto-tunnel backup tunnel-num [**min** *num*] [**max** *num*]

Syntax Description

min *num*	(Optional) Minimum number of the backup tunnels. The range is 0 to 65535. Default: 65436.
max *num*	(Optional) Maximum number of the backup tunnels. The range is 0 to 65535. Default: 65535.

Command Default

None

Command Modes

Global configuration (config)

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.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example configures the range of backup autotunnel numbers to be between 1000 and 1100:

```
Router(config)# mpls traffic-eng auto-tunnel backup tunnel-num min 1000 max 1100
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup	Automatically builds NHOP and NNHOP backup tunnels.
mpls traffic-eng auto-tunnel backup config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel backup nhop-only	Enables the creation of only dynamic next-hop backup tunnels.
mpls traffic-eng auto-tunnel backup timers	Configures how frequently a timer will scan backup autotunnels and remove tunnels that are not being used.

mpls traffic-eng auto-tunnel mesh

To enable autotunnel mesh groups globally, use the **mpls traffic-eng auto-tunnel mesh** command in global configuration mode. To disable autotunnel mesh groups globally, use the **no** form of this command.

mpls traffic-eng auto-tunnel mesh
no mpls traffic-eng auto-tunnel mesh

Syntax Description

This command has no arguments or keywords.

Command Default

Autotunnel mesh groups are not enabled globally.

Command Modes

Global configuration (config)

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.
15.2(2)S	This command was modified. The usage guidelines changed on hardware that supports dual Route Processors (RPs).
Cisco IOS XE Release 3.6S	This command was modified. The usage guidelines changed on hardware that supports dual RPs.

Usage Guidelines

On hardware that supports dual processors, once this command is enabled, the tunnel is created on both the active and the standby RPs. When the **no** form of the command is executed, the tunnel is disabled on both the active and the standby RPs.

Examples

The following example shows how to enable autotunnel mesh groups globally:

```
Router(config)# mpls traffic-eng auto-tunnel mesh
```

Related Commands

Command	Description
interface auto-template	Creates the template interface.

mpls traffic-eng auto-tunnel mesh tunnel-num

To configure a range of mesh tunnel interface numbers, use the **mpls traffic-eng auto-tunnel mesh tunnel-num** command in global configuration mode. To use the default values, use the **no** form of this command.

mpls traffic-eng auto-tunnel mesh tunnel-num min *num* **max** *num*
no mpls traffic-eng auto-tunnel mesh tunnel-num

Syntax Description

min *num*	Specifies the beginning number of the range of mesh tunnel interface numbers. The range is 1 to 65535. The default value is 64336.
max *num*	Specifies the ending number of the range of mesh tunnel interface numbers. The range is 1 to 65535. The default value is 65335.

Command Default

The **min** default is 64336. The **max** default is 65335.

Command Modes

Global configuration (config)

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.

Usage Guidelines

If you change an access control list (ACL) and tunnels are deleted because they no longer match the ACL, tunnels that are re-created might not be numbered sequentially; that is, the range of tunnel numbers might not be sequential.

Examples

The following example shows how to specify 1000 as the beginning number of the mesh tunnel interface and 2000 as the ending number:

```
Router(config)# mpls traffic-eng auto-tunnel mesh tunnel-num min 1000 max 2000
```

Related Commands

Command	Description
show mpls traffic-eng auto-tunnel mesh	Displays the cloned mesh tunnel interfaces of each autotemplate interface and the current range of mesh tunnel interface numbers.

mpls traffic-eng auto-tunnel primary config

To enable IP processing without an explicit address, use the **mpls traffic-eng auto-tunnel primary config** command in global configuration mode. To disable this capability, use the **no** form of this command.

mpls traffic-eng auto-tunnel primary config unnumbered *interface*
no mpls traffic-eng auto-tunnel primary config unnumbered *interface*

Syntax Description

unnumbered *interface*	Interface on which IP processing will be enabled without an explicit address.

Command Default

Loopback0

Command Modes

Global configuration (config)

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.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example enables IP processing on an Ethernet interface:

```
Router# mpls traffic-eng auto-tunnel primary config unnumbered ethernet1/0
```

Related Commands

Command	Description
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 primary autotunnels are removed.
mpls traffic-eng auto-tunnel primary tunnel-num	Configures the range of tunnel interface numbers for primary autotunnels.
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

mpls traffic-eng auto-tunnel primary config mpls ip

To enable Label Distribution Protocol (LDP) on primary autotunnels, use the **mpls traffic-eng auto-tunnel primary config mpls ip** command in global configuration mode. To disable LDP on primary autotunnels, use the **no** form of this command.

mpls traffic-eng auto-tunnel primary config mpls ip
no mpls traffic-eng auto-tunnel primary config mpls ip

Syntax Description

This command has no arguments or keywords.

Command Default

LDP is not enabled.

Command Modes

Global configuration (config)

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.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example enables LDP on primary autotunnels:

```
Router(config)# mpls traffic-eng auto-tunnel primary config mpls ip
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel primary config	Enables IP processing without an explicit address.
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 primary autotunnels are removed.
mpls traffic-eng auto-tunnel primary tunnel-num	Configures the range of tunnel interface numbers for primary autotunnels.
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

mpls traffic-eng auto-tunnel primary onehop

To automatically create primary tunnels to all next hops, use the **mpls traffic-eng auto-tunnel primary onehop** command in global configuration mode. To disable the automatic creation of primary tunnels to all next hops, use the **no** form of this command.

mpls traffic-eng auto-tunnel primary onehop
no mpls traffic-eng auto-tunnel primary onehop

Syntax Description

This command has no arguments or keywords.

Command Default

The dynamically created one-hop tunnels use Loopback0.

Command Modes

Global configuration (config)

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.
15.2(2)S	This command was modified. The usage guidelines changed on hardware that supports dual Route Processors (RPs).
Cisco IOS XE Release 3.6S	This command was modified. The usage guidelines changed on hardware that supports dual RPs.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

On hardware that supports dual processors, once this command is enabled, the tunnel is created on both the active and the standby RPs. When the **no** form of the command is executed, the tunnel is disabled on both the active and the standby RPs.

Examples

The following example automatically creates primary tunnels to all next hops:

```
Router(config)# mpls traffic-eng auto-tunnel primary onehop
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel primary config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel primary onehop	Enables LDP on primary autotunnels.

Command	Description
mpls traffic-eng auto-tunnel primary timers	Configures how many seconds after a failure primary autotunnels are removed.
mpls traffic-eng auto-tunnel primary tunnel-num	Configures the range of tunnel interface numbers for primary autotunnels.
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

mpls traffic-eng auto-tunnel primary timers

To configure how many seconds after a failure primary autotunnels are removed, use the **mpls traffic-eng auto-tunnel primary timers** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls traffic-eng auto-tunnel primary timers removal rerouted *sec*
no mpls traffic-eng auto-tunnel primary timers removal rerouted *sec*

Syntax Description

removal rerouted *sec*	Number of seconds after a failure that primary autotunnels are removed. The range is 30 to 604,800. Default: 0.

Command Default

None

Command Modes

Global configuration (config)

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.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example shows that primary autotunnels are removed 100 seconds after a failure:

```
Router(config)# mpls traffic-eng auto-tunnel primary timers removal rerouted 100
```

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 tunnel-num	Configures the range of tunnel interface numbers for primary autotunnels.
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

mpls traffic-eng auto-tunnel primary tunnel-num

To configure the range of tunnel interface numbers for primary autotunnels, use the **mpls traffic-eng auto-tunnel primary tunnel-num** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls traffic-eng auto-tunnel primary tunnel-num [**min** *num*] [**max** *num*]
no mpls traffic-eng auto-tunnel primary tunnel-num [**min** *num*] [**max** *num*]

Syntax Description

min *num*	(Optional) Minimum number of the primary tunnels. The range is 0 to 65535. Default: 65436.
max *num*	(Optional) Maximum number of the primary tunnels. The **max** number is the minimum number plus 99. The range is 0 to 65535.

Command Default

None

Command Modes

Global configuration (config)

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.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example shows that the primary tunnel numbers can be between 2000 and 2100:

```
Router(config)# mpls traffic-eng auto-tunnel primary tunnel-num min 2000 max 2100
```

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 primary autotunnels are removed.

Command	Description
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

mpls traffic-eng autoroute-exclude prefix list

To configure or to allow specific destinations or prefixes to avoid routing through traffic engineering (TE) tunnels, use the **mpls traffic-eng autoroute-exclude prefix list** command in router configuration mode. To allow the specified destinations to route through TE tunnels, use the**no** form of this command.

mpls traffic-eng autoroute-exclude prefix list *prefix-list-name*
no mpls traffic-eng autoroute-exclude prefix list *prefix-list-name*

Syntax Description

autoroute-exclude	MPLS TE auto route that is excluded from the prefix list.
prefix list *prefix-list-name*	Filter prefixes that are not routed through the TE tunnels.

Command Default

IP routes are sent over all MPLS/TE IP tunnels.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE 3.13S	This command was introduced.

Usage Guidelines

The **mpls traffic-eng autoroute-exclude prefix list** command allows specific destinations or prefixes to avoid TE tunnels. However, other prefixes can still be configured to use TE tunnels. Autoroute exclude is configured using a prefix list. IP addresses and prefixes that are members of this prefix list are excluded from TE tunnels, even when autoroute is enabled on them. If the IP addresses or prefixes are added to the prefix list, they are dynamically routed without passing through the TE tunnel. If the IP addresses or prefixes are removed from the prefix list, they are dynamically rerouted back on the TE tunnel path.

Examples

The following example shows how to configure specific destinations without routing through TE tunnels:

```
Router(config-router)# mpls traffic-eng autoroute-exclude prefix-list XX
```

Related Commands

Command	Description
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
router ospf	Configures an OSPF routing process on a router.

mpls traffic-eng backup-path

To assign one or more backup tunnels to a protected interface, use the **mpls traffic-eng backup-path** command in interface configuration mode.

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

Syntax Description

tunnel *tunnel-id*	Tunnel ID of the backup tunnel that can be used in case of a failure.

Command Default

No backup tunnels are used if this interface goes down.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(16)ST	With Link Protection, this command selected the one-and-only backup tunnel for a given protected interface. If you enter the command twice, the second occurrence overwrites the first occurrence.
12.0(22)S	You can now enter this command multiple times to select multiple backup tunnels for a given protected interface. This can be done for both Link and Node Protection. 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(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.

Usage Guidelines

Enter this command on the interface to be protected (Link Protection), or on the interface whose downstream node is being protected (Node Protection). You can enter this command multiple times to select multiple backup tunnels for a given protected interface. An unlimited number of backup tunnels can be assigned to protect an interface. The only limitation is memory. By entering this command on a physical interface, LSPs using this interface (sending data *out of* this interface) can use the indicated backup tunnels if there is a link or node failure.

Examples

The following example assigns backup tunnel 34 to interface POS5/0:

```
Router(config)# interface pos5/0
Router(config-if)# mpls traffic-eng backup-path tunnel34
```

Related Commands

Command	Description
tunnel mpls traffic-eng fast-reroute	Enables an MPLS traffic engineering tunnel to use a backup tunnel if there is a link or node failure (provided that a backup tunnel exists).

mpls traffic-eng backup-path tunnel

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

mpls traffic-eng backup-path tunnel *interface*

Syntax Description

interface	String that identifies the tunnel interface being created and configured.

Command Default

This command is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(8)ST	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was 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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example specifies the traffic engineering backup tunnel with the identifier 1000:

```
Router(config-if)# mpls traffic-eng backup-path Tunnel 1000
```

Related Commands

Command	Description
show mpls traffic-eng fast-reroute database	Displays information about existing Fast Reroute configurations.
tunnel mpls traffic-eng fast-reroute	Enables an MPLS traffic engineering tunnel to use a backup tunnel in the event of a link failure (assuming a backup tunnel exists).

mpls traffic-eng ds-te bc-model

To enable a Bandwidth Constraints Model to be used by a router in DiffServ-aware Traffic Engineering, use the **mpls traffic-eng ds-te bc-model** global configuration command. (Using the **no** form of this command selects the default model, which is the Russian Dolls Model.)

mpls traffic-eng ds-te bc-model [{**rdm** | **mam**}]
no mpls traffic-eng ds-te bc-model [{**rdm** | **mam**}]

Syntax Description

rdm	Russian Dolls Model. (Described in IETF RFC 4127).
mam	Maximum Allocation Model. (Described in IETF RFC 4125).

Command Default

Russian Dolls Model is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

1. The Maximum Allocation Model should be selected when the network administrator needs to ensure isolation across all Class Types without having to use pre-emption, and can afford to risk some QoS degradation of Class Types other than the Premium Class.
2. The Russian Dolls Model should be selected when the network administrator needs to prevent QoS degradation of all Class Types and can impose pre-emption.

Examples

In the following example, the Maximum Allocation Model is being selected:

```
Router(config)# mpls traffic-eng ds-te bc-model mam
```

mpls traffic-eng ds-te mode

To configure a router to enter DiffServ-aware Traffic Engineering modes which incorporate degrees of the IETF Standard, use the **mpls traffic-eng ds-te mode** global configuration command. To return the router to the pre-IETF-Standard mode, use the **no** form of this command.

mpls traffic-eng ds-te mode [{**migration** | **ietf**}]
no mpls traffic-eng ds-te mode [{**migration** | **ietf**}]

Syntax Description

migration	A mode by which the router generates IGP and tunnel signaling according to the pre-IETF standard, but adds TE-class mapping and accepts advertisement in both the pre-IETF and the IETF-Standard formats.
ietf	The "Liberal" IETF mode, by which the router generates IGP advertisement and tunnel signaling according to the IETF Standard and responds to TE-class mapping, yet also accepts advertisement in both the pre-IETF-Standard and IETF-Standard formats.

Command Default

Pre-IETF-Standard mode is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

1. Place the router into Migration Mode only if it is still in the pre-IETF Standard ("Traditional") mode, and you want to begin upgrading its network to operate the IETF-Standard form of DS-TE.
2. Place the router into Liberal-IETF Mode only if its network is already in the Migration Mode, and you want to complete the upgrade of that network so it will operate the IETF-Standard form of DS-TE.

Examples

In the following example, the router is configured to operate in Migration Mode:

```
Router(config)# mpls traffic-eng ds-te migration
```

mpls traffic-eng fast-reroute backup-prot-preemption

To change the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted, use the **mpls traffic-eng fast-reroute backup-prot-preemption** command in global configuration mode. To use the default algorithm of minimizing the number of label-switched paths (LSPs) that are demoted, use the **no** form of this command.

mpls traffic-eng fast-reroute backup-prot-preemption [**optimize-bw**]
no mpls traffic-eng fast-reroute backup-prot-preemption

Syntax Description

optimize-bw	(Optional) Minimizes the amount of bandwidth wasted.

Command Default

A minimum number of LSPs are preempted.

Command Modes

Global configuration (config)

Command History

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

The **mpls traffic-eng fast-reroute backup-prot-preemption** command allows you to determine the criteria the router will use when selecting the LSPs that will be preempted.

If you enter the command with the **optimize-bw** keyword, the router chooses LSPs that will waste the least amount of bandwidth.

If you do not enter the **mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw** command, the router preempts as few LSPs as possible.

Each router in the network does not have to use the same algorithm; that is, you can specify **optimize-bw** for some routers in the network but not for others.

You can enter the **mpls traffic-eng fast-reroute backup-prot-preemption** command at any time. If you change the algorithm, it does not affect LSPs that already are protected. It only affects the placement of new LSPs signaled after you enter this command. The command can affect LSPs during the next periodic promotion cycle.

Examples

In the following examples, a next-next hop (NNHOP) backup tunnel has the following characteristics:

- Total backup capacity: 240 units
- Used backup bandwidth: 220 units
- Available backup bandwidth: 20 units

The backup tunnel currently is protecting LSP1 through LSP5, which have the following bandwidth, and do not have backup bandwidth protection (that is, the "bandwidth protection desired" bit was not set via the **tunnel mpls traffic-eng fast-reroute** command):

- LSP1: 10 units
- LSP2: 20 units
- LSP3: 30 units
- LSP4: 60 units
- LSP5: 100 units

As shown, LSP1 through LSP5 use 220 units of bandwidth.

LSP6 has backup bandwidth protection and needs 95 units of bandwidth. Twenty units of bandwidth are available, so 75 more units of bandwidth are needed.

In the following example, backup bandwidth protection is enabled and the amount of wasted bandwidth is minimized:

```
Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw
```

LSP2 and LS4 are preempted so that the least amount of bandwidth is wasted.

In the following example, backup protection preemption is enabled and the number of preempted LSPs is minimized:

```
Router(config)# no mpls traffic-eng fast-reroute backup-prot-preemption
```

The router selects the LSP whose bandwidth is next-greater than the required bandwidth. Therefore, the router picks LSP5 because it has the next larger amount of bandwidth over 75. One LSP is demoted. and 25 units of bandwidth are wasted.

Related Commands

Command	Description
show ip rsvp fast bw-protect	Displays information about whether backup bandwidth protection is enabled and the status of backup tunnels that may be used to provide that protection.

mpls traffic-eng fast-reroute promote

To configure the router to assign new or more efficient backup Multiprotocol Label Switching traffic engineering (MPLS-TE) tunnels to protect MPLS-TE tunnels, use the **mpls traffic-eng fast-reroute promote** command in privileged EXEC mode.

mpls traffic-eng fast-reroute promote

Syntax Description

This command has no arguments or keywords.

Command Default

No MPLS-TE backup tunnels are assigned.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use the **mpls traffic-eng fast-reroute promote** command, you must be in a user group associated with a task group.

Examples

The following example shows how to initiate backup tunnel promote and assignment:

```
Router# mpls traffic-eng fast-reroute promote
```

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.
mpls traffic-eng fast-reroute timers	Specifies how often the router considers switching an LSP to a new (better) backup tunnel if additional backup bandwidth becomes available.

mpls traffic-eng fast-reroute timers

To specify how often the router considers switching a label switched path (LSP) to a new (better) backup tunnel if additional backup bandwidth becomes available, use the **mpls traffic-eng fast-reroute timers** command in global configuration mode. To disable this timer, set the seconds value to zero or use the **no** form of this command.

mpls traffic-eng fast-reroute timers [**promotion** *seconds*]
no mpls traffic-eng fast-reroute timers

Syntax Description

promotion *seconds*	(Optional) Sets the interval, in seconds, between scans to determine if an LSP should use a new, better backup tunnel. The range is 0 to 604800. A value of 0 disables promotions to a better LSP.

Command Default

The timer is running and is set to a frequency of every 300 seconds (5 minutes). If you enter the **no mpls traffic-eng fast-reroute timers** command, the router returns to this default behavior.

Command Modes

Global configuration (config)

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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

In the following example, LSPs are scanned every 2 minutes (120 seconds). The router uses this information to consider if the LSPs should be promoted to a better backup tunnel:

```
Router(config)# mpls traffic-eng fast-reroute timers promotion 120
```

mpls traffic-eng flooding thresholds

To set a reserved bandwidth thresholds for a link, use the **mpls traffic-eng flooding thresholds** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

mpls traffic-eng flooding thresholds {**down** | **up**} *percent* [*percent* . . .]
no mpls traffic-eng flooding thresholds {**down** | **up**}

Syntax Description

down	Sets the thresholds for decreased reserved bandwidth.
up	Sets the thresholds for increased reserved bandwidth.
percent [*percent*]	Bandwidth threshold level. For the **down** keyword, the range is 0 through 99. For the **up** keyword, the range is 1 through 100.

Command Default

None

Command Modes

Interface configuration (config-if)

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)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

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

Examples

The following example shows how to set the reserved bandwidth of the link for decreased (down) and for increased (up) thresholds:

```
Router(config-if)# mpls traffic-eng flooding thresholds down 100 75 25
Router(config-if)# mpls traffic-eng flooding thresholds up 25 50 100
```

Related Commands

Command	Description
mpls traffic-eng link timers periodic-flooding	Sets the length of the interval used for periodic flooding.

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.

mpls traffic-eng interface

To enable Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) link-state advertisement (LSA) for an interface to be advertised into the Open Shortest Path First (OSPF) area 0, use the **mpls traffic-eng interface** command in router configuration mode. To restore the setting of the MPLS TE LSA to the same area as the router LSA, use the **no** form of this command.

mpls traffic-eng interface interface area 0
no mpls traffic-eng interface interface area 0

Syntax Description

interface	The interface to be advertised with an MPLS TE LSA into OSPF area 0. The interface may be one or two words.

Command Default

The default is to advertise the area assigned to the interface by the OSPF network configuration.

Command Modes

Router configuration

Command History

Release	Modification
12.0(12)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
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

Usually, the MPLS TE LSA is advertised into the same area as the router LSA. If a link between two Area Border Routers (ABRs) is in an OSPF area besides area 0, you can advertise the link between ABRs into area 0. This solves for TE the same problem that virtual links solve for IP routing. This command is valid only for OSPF. Issue the command on both ABRs for the interfaces at both ends of the link.

Examples

In the following example, OSPF advertises the MPLS TE LSA for interface pos2/0 to area 0:

```
Router(config)# router ospf 1
Router(config-router)# mpls traffic-eng interface pos2/0 area 0
```

Related Commands

Command	Description
mpls traffic-eng multicast-intact	Enables multicast-intact support from the OSPF routing protocol to maintain and publish the native IP nexthops (paths) for every OSPF route.

mpls traffic-eng link timers bandwidth-hold

To set the length of time that bandwidth is held for a Resource Reservation Protocol (RSVP) PATH (Set Up) message while waiting for the corresponding RSVP RESV message to come back, use the **mpls traffic-eng link timers bandwidth-hold** command in global configuration mode.

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

Syntax Description

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

Command Default

15 seconds

Command Modes

Global configuration (config)

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.

Examples

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

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

Related Commands

Command	Description
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information.

mpls traffic-eng link timers periodic-flooding

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

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

Syntax Description

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

Command Default

180 seconds

Command Modes

Global configuration (config)

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.

Usage Guidelines

Use this command to set the interval for periodic flooding of traffic engineering (TE) topology information.

Changes in the Multiprotocol Label Switching (MPLS) TE topology database are flooded by the link state Interior Gateway Protocol (IGP). Some changes, such as those to link status (up/down) or configured parameters, trigger immediate flooding. Other changes are considered less urgent and are flooded periodically. For example, changes to the amount of link bandwidth allocated to TE tunnels are flooded periodically unless the change causes the bandwidth to cross a configurable threshold.

Examples

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

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

Related Commands

Command	Description
mpls traffic-eng flooding thresholds	Sets the reserved bandwidth thresholds of a link.

mpls traffic-eng link-management timers bandwidth-hold

To set the length of time that bandwidth is held for an RSVP path (setup) message while you wait for the corresponding RSVP Resv message to come back, use the **mpls traffic-eng link-management timers bandwidth-hold** command in global configuration mode. To disable this function, use the **no** form of this command.

mpls traffic-eng link-management timers bandwidth-hold *hold-time*
no mpls traffic-eng link-management timers bandwidth-hold

Syntax Description

hold-time	Length of time that bandwidth can be held. The range is 1 to 300 seconds.

Command Default

15 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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

In the following example, bandwidth is set to be held for 10 seconds:

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

Related Commands

Command	Description
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information.

mpls traffic-eng link-management timers periodic-flooding

To set the length of the interval for periodic flooding, use the **mpls traffic-eng link-management timers periodic-flooding** command in global configuration mode. To disable the specified interval length for periodic flooding, use the **no** form of this command.

mpls traffic-eng link-management timers periodic-flooding *interval*
no mpls traffic-eng link-management timers periodic-flooding

Syntax Description

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

Command Default

180 seconds (3 minutes)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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

Use this command to advertise link state information changes that do not trigger immediate action. For example, a change to the amount of allocated bandwidth that does not cross a threshold.

Examples

The following example shows how to set the interval length for periodic flooding to 120 seconds:

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

Related Commands

Command	Description
mpls traffic-eng flooding thresholds	Sets a link's reserved bandwidth thresholds.

mpls traffic-eng logging lsp

To log traffic engineering label switched path (LSP) events, use the **mpls traffic-eng logging lsp** command in global configuration mode. To disable logging of LSP events, use the **no** form of this command.

mpls traffic-eng logging lsp {**path-errors** | **reservation-errors** | **preemption** | **setups** | **teardowns**} [*acl-number*]
no mpls traffic-eng logging lsp {**path-errors** | **reservation-errors** | **preemption** | **setups** | **teardowns**} [*acl-number*]

Syntax Description

path-errors	Logs Resource Reservation Protocol (RSVP) path errors or headend path calculation failures for traffic engineering LSPs
reservation-errors	Logs RSVP reservation errors for traffic engineering LSPs.
preemption	Logs events related to the preemption of traffic engineering LSPs.
setups	Logs events related to the establishment of traffic engineering LSPs.
teardowns	Logs events related to the removal of traffic engineering LSPs.
acl-number	(Optional) The specified access list to filter the events that are logged. Events are only for LSPs that match the access list.

Command Default

Logging of LSP events is disabled.

Command Modes

Global configuration (config)

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.
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.
15.2(2)S	This command was modified to generate traffic engineering log messages when a traffic engineering headend path calculation fails. For details, see the “Usage Guidelines” section.
Cisco IOS XE Release 3.6S	This command was modified to generate traffic engineering log messages when a traffic engineering headend path calculation fails. For details, see the “Usage Guidelines” section.

Usage Guidelines

When a traffic engineering headend path calculation fails and the **mpls traffic-eng logging lsp path-errors** command is configured, the following traffic engineering log messages are generated and sent to the console, log file, or syslog depending on the logging configuration. Duplicate successive log entries of the same message for the same tunnel are suppressed.

Point-to-point (P2P) tunnels:

- When a destination is not present in the traffic engineering topology database:

  00:00:08: %MPLS_TE-5-LSP: LSP 10.30.30.3 1_1: Destination IP address, 10.30.30.2, not found

- When a link that was previously used as part of an LSP path is no longer usable (for example, insufficient bandwidth):

  00:16:09: %MPLS_TE-5-LSP: LSP 10.30.30.3 1_31: Can't use link 10.0.1.2 on node 10.30.30.3

- When an explicit path has an unknown address:

  00:25:54: %MPLS_TE-5-LSP: LSP 10.30.30.3 1_76: Explicit path has unknown address, 10.0.1.3

- When an Interior Gateway Protocol (IGP) neighbor adjacency goes down:

  00:04:28: %MPLS_TE-5-LSP: LSP 10.30.30.3 1_30: No addresses to connect 10.30.30.3 to 10.0.1.3

- When a dynamic path is present with no valid path to the destination:

  01:18:19: %MPLS_TE-5-LSP: LSP 10.30.30.3 3_36: No path to destination, 10.30.30.2

Point-to-multipoint (P2MP) tunnels:

- When there is no valid path that meets constraints to a destination in the destination list:

  00:00:12: %MPLS_TE-5-LSP: Sub-LSP 10.30.30.3[1:1]->10.30.30.2_4: pcalc failed to find a path for 10.30.30.2

Note For a short period after a reboot or network reconvergence, you may see some spurious log entries (due to temporary path calculation failures) until the topology converges.

Examples

The following example shows how to log path errors for LSPs that match access list 3:

```
Device(config)# mpls traffic-eng logging lsp path-errors 3
```

Related Commands

Command	Description
access-list (extended)	Defines an extended IP access list.
logging console	Limits the number of messages logged to the console.
mpls traffic-eng logging tunnel	Logs certain traffic engineering tunnel events.
show logging	Displays the messages that are logged in the buffer.

mpls traffic-eng logging tunnel

To log certain traffic engineering tunnel events, use the **mpls traffic-eng logging tunnel** command in global configuration mode. To disable logging of traffic engineering tunnel events, use the **no** form of this command.

mpls traffic-eng logging tunnel lsp-selection [*acl-number*]
no mpls traffic-eng logging tunnel lsp-selection [*acl-number*]

Syntax Description

lsp-selection	Logs events related to the selection of a label switched path (LSP) for a traffic engineering tunnel.
acl-number	(Optional) Uses the specified access list to filter the events that are logged. Logs events only for tunnels that match the access list.

Command Default

Logging of tunnel events is disabled.

Command Modes

Global configuration (config)

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.
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 example shows how to log traffic engineering tunnel events associated with access list 3:

```
Router(config)# mpls traffic-eng logging tunnel lsp-selection 3
```

Related Commands

Command	Description
access-list (extended)	Creates an extended access list.
logging console	Limits the number of messages logged to the console.
mpls traffic-eng logging lsp	Logs certain traffic engineering LSP events.
show logging	Displays the messages that are logged in the buffer.

mpls traffic-eng lsp attributes through route-target

mpls traffic-eng lsp attributes

To create or modify a label switched path (LSP) attribute list, use the**mpls traffic-eng lsp attributes** command in global configuration mode. To remove a specified LSP attribute list from the device configuration, use the **no** form of this command.

mpls traffic-eng lsp attributes *string*
no mpls traffic-eng lsp attributes *string*

Syntax Description

string	LSP attributes list identifier.

Command Default

An LSP attribute list is not created unless you create one.

Command Modes

Global configuration (config)

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.

Usage Guidelines

This command sets up an LSP attribute list and enters LSP Attributes configuration mode, in which you can enter LSP attributes.

To associate the LSP attributes and LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option attributes** *string* command, where *string* is the identifier for the specific LSP attribute list.

An LSP attribute referenced by the path option takes precedence over the values configured on the tunnel interface. If an attribute is not specified in the LSP attribute list, the devices takes the attribute from the tunnel configuration. LSP attribute lists do not have default values. If the attribute is not configured on the tunnel, then the device uses tunnel default values.

Once you type the **mpls traffic-eng lsp attributes** command, you enter the LSP Attributes configuration mode where you define the attributes for the LSP attribute list that you are creating.

The mode commands are as follows:

- **affinity**—Specifies attribute flags for links that make up an LSP.
- **auto-bw**—Specifies automatic bandwidth configuration.
- **bandwidth**—Specifies LSP bandwidth.
- **lockdown**—Disables reoptimization for the LSP.
- **priority**—Specifies LSP priority.

- **protection**—Enables failure protection.
- **record-route**—Records the route used by the LSP.

The following monitoring and management commands are also available in the LSP Attributes configuration mode:

- **exit**—Exits from LSP Attributes configuration mode.
- **list**—Relists all the entries in the LSP attribute list.
- **no**—Removes a specific attribute from the LSP attribute list.

Examples

The following example shows how to set up an LSP attribute list identified with the numeral 6 with the **bandwidth** and **priority** mode commands. The example also shows how to use the **list** mode command:

```
Device(config)# mpls traffic-eng lsp attributes 6
Device(config-lsp-attr)# bandwidth 500
Device(config-lsp-attr)# list
LIST 6
 bandwidth 500

Device(config-lsp-attr)# priority 1 1
Device(config-lsp-attr)# list
LIST 6
 bandwidth 500
 priority 1 1
Device(config-lsp-attr)# exit
```

Related Commands

Command	Description
show mpls traffic-eng lsp attributes	Displays global LSP attributes lists.

mpls traffic-eng mesh-group

To configure a mesh group in an Interior Gateway Protocol (IGP) to allow Multiprotocol Label Switching (MPLS) traffic engineering (TE) label switch routers (LSRs) that belong to the same mesh group to signal tunnels to the local router, use the **mpls traffic-eng mesh-group** command in router configuration mode. To disable signaling of tunnels from LSRs in the same mesh group to the local router, use the **no** form of this command.

mpls traffic-eng mesh-group *mesh-group-id type number* **area** *area-id*
no mpls traffic-eng mesh-group *mesh-group-id type number* **area** *area-id*

Syntax Description

mesh-group-id	Number that identifies a specific mesh group.
type	Type of interface.
number	Interface number.
area *area-id*	Specifies an IGP area.

Command Default

No tunnels are signaled for routers in the same mesh group.

Command Modes

Router configuration (config-router)#

Command History

Release	Modification
12.0(29)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.

Usage Guidelines

Use this command to configure a mesh group in an IGP. This allows the MPLS TE LSRs that belong to the specified mesh group to signal tunnels to the local router. The IGP floods mesh group configuration to all routers belonging to the same mesh group. An autotemplate determines how a router participates in an autotunnel. A router can participate in a mesh group through two-way tunnels or one-way tunnels.

Open Shortest Path First (OSPF) is the only IGP supported for the MPLS Traffic Engineering--AutoTunnel Mesh Groups feature.

Examples

The following example shows how to configure OSPF to allow LSRs that belong to the same mesh group (mesh group 10) to signal tunnels to the local router:

```
Router(config)# router ospf 100
Router(config-router)# mpls traffic-eng mesh-group 10 loopback 0 area 100
```

Related Commands

Command	Description
tunnel destination mesh-group	Configures an autotemplate to signal tunnels to all other members of a specified mesh group.

mpls traffic-eng multicast-intact

To configure a router running Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF) so that Protocol-Independent Multicast (PIM) and Multiprotocol Label Switching (MPLS) traffic engineering (TE) can work together, use the **mpls traffic-eng multicast-intact** command in router configuration mode. To disable interoperability between PIM and MPLS TE, use the **no** form of this command.

mpls traffic-eng multicast-intact
no mpls traffic-eng multicast-intact

Syntax Description

This command has no arguments or keywords.

Command Default

PIM and MPLS TE do not work together.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(12)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
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 **mpls traffic-eng multicast-intact** command allows PIM to use the native hop-by-hop neighbors while unicast routing is using MPLS TE tunnels.

This command works only for OSPF and IS-IS protocols.

Examples

The following example shows how to enable PIM and MPLS TE to interoperate:

```
Router(config)# router ospf 1
Router(config-router)# mpls traffic-eng multicast-intact
```

Related Commands

Command	Description
mpls traffic-eng interface	Configures a router running OSPF or IS-IS so that it floods MPLS TE link information in the indicated OSPF area or IS-IS level.
show ospf routes multicast intact	Displays multicast-intact paths of OSPF routes.

mpls traffic-eng nsr

To enable Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Nonstop Routing (NSR) support on a device, use the **mpls traffic-eng nsr** command in global configuration mode. To disable MPLS TE NSR support, use the **no** form of this command.

mpls traffic-eng nsr

no mpls traffic-eng nsr

This command has no arguments or keywords.

Command Default

MPLS TE NSR support is not enabled.

Command Modes

Global configuration (config)

Command History

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

The following example shows how to enable MPLS TE NSR support using the use the **mpls traffic-eng nsr** command.

```
enable
 configure terminal
  ip cef
  mpls traffic-eng nsr
  end
```

Related Commands

Command	Description
show mpls traffic-eng nsr	Displays information about MPLS TE NSR.

mpls traffic-eng passive-interface

To configure a link as a passive interface between two Autonomous System Boundary Routers (ASBRs), use the **mpls traffic-eng passive-interface** command in interface configuration mode. To disable the passive link, use the **no** form of this command.

mpls traffic-eng passive-interface nbr-te-id *te-router-id* [**nbr-if-addr** *if-addr*] [**nbr-igp-id** {**isis** *sysid* | **ospf** *sysid*}]
no mpls traffic-eng passive-interface nbr-te-id *te-router-id* [**nbr-if-addr** *if-addr*] [**nbr-igp-id** {**isis** *sysid* | **ospf** *sysid*}]

Syntax Description

nbr-te-id *te-router-id*	Traffic engineering router ID of the neighbor router on the remote side of the link where this command is configured.
nbr-if-addr *if-addr*	(Optional) Interface address of the remote ASBR.
nbr-igp-id	(Optional) Specifies a unique *sysid* for neighboring Interior Gateway Protocols (IGPs) when two or more autonomous systems use different IGPs and have more than one neighbor on the link. Enter the **nbr-igp-id** keyword (followed by the **isis** or **ospf** keyword) and the *sysid* for each IGP. The *sysid* must be unique for each neighbor.
isis *sysid*	System identification of Intermediate System-to-Intermediate System (IS-IS).
ospf *sysid*	System identification of Open Shortest Path First (OSPF).

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	The **nbr-if-addr** keyword was added.
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 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

The **mpls traffic-eng passive-interface** command sets the next-hop address for a passive interface. The command is required only for a broadcast link.

Enter the **mpls traffic-eng passive-interface** command only on the outgoing interface on which the label-switched path (LSP) will exit; you do not have to enter this command on both ends of the interautonomous system (Inter-AS) link.

On a point-to-point link or on a multiaccess link where there is only one neighbor, you do not have to enter the **isis** or **ospf** keyword (or the *sysid* argument).

If two autonomous systems use different IGPs and have more than one neighbor on the link, you must enter the **nbr-igp-id** keyword followed by **isis** or **ospf** and the *sysid*. The *sysid* must be unique for each neighbor.

For a broadcast link (that is, other Resource Reservation Protocol (RSVP)) features are using the passive link), you must enter the **nbr-if-addr** keyword.

For an RSVP Hello configuration on an Inter-AS link, all keywords are required.

Examples

In the following example there is only one neighbor:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.10.10
```

In the following example, two autonomous systems use different IGPs and have more than one neighbor on the link:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.11.12 nbr-igp-id ospf
 10.10.15.18
```

If autonomous system 1 (AS1) is running IS-IS and AS2 is running OSPF, the unique ID on A1 must be in the system ID format. To form the system ID, we recommend that you append zeros to the router ID of the neighbor. For example, if the AS2 router is 10.20.20.20, then you could enter a system ID of 10.0020.0020.0020.00 for IS-IS on the AS1 router.

In the following example there is a remote ASBR and an IS-IS:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.20.20.20 nbr-igp-id isis
 10.0020.0020.0020.00
```

In the following example, there is a broadcast link and the interface address of the remote ASBR is 10.0.0.2:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.10.10 nbr-if-addr
10.0.0.2
```

mpls traffic-eng path-option list

To configure a path option list, use the **mpls traffic-eng path-option list** command in global configuration mode. To disable this function, use the **no** form of this command.

mpls traffic-eng path-option list [{**name** *pathlist-name* | **identifier** *pathlist-number*}]
no mpls traffic-eng path-option list [{**name** *pathlist-name* | **identifier** *pathlist-number*}]

Syntax Description

name *pathlist-name*	Specifies the name of the path option list.
identifier *pathlist-number*	Specifies the identification number of the path option list. The range is 1 through 65535.

Command Default

There are no path option lists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

A path option list contains a list of backup paths for a primary path option. You can specify a path option list by entering its name or identifier.

After you enter the **mpls traffic-eng path-option list** command, the router enters path option list configuration mode and you can enter the following commands:

- **path-option** --Specifies the name or identification number of the next path option to add, edit, or delete.
- **list** --Lists all path options.
- **no** --Deletes a specified path option.
- **exit** --Exits from path option list configuration mode.

Then you can specify explicit backup paths by entering their name or identifier.

Examples

The following example configures the path option list named pathlist-01, adds path option 10, lists the backup path that is in the path option list, and exits from path option list configuration mode:

```
Router(config)# mpls traffic-eng path-option list name pathlist-01
Router(cfg-pathoption-list)# path-option 10 explicit name bk-path-01
Router(cfg-pathoption-list)# list
 path-option 10 explicit name bk-path-01
Router(cfg-pathoption-list)# exit
```

Related Commands

Command	Description
tunnel mpls traffic-eng path option	Configures a path option for an MPLS TE tunnel.
tunnel mpls traffic-eng path-option protect	Configures a secondary path option or a path option list for an MPLS TE tunnel.

mpls traffic-eng path-selection metric

To specify the metric type to use for path selection for tunnels for which the metric type has not been explicitly configured, use the **mpls traffic-eng path-selection metric** command in global configuration mode. To remove the specified metric type, use the **no** form of this command.

mpls traffic-eng path-selection metric {**igp** | **te**}
no mpls traffic-eng path-selection metric

Syntax Description

igp	Use the Interior Gateway Protocol (IGP) metric.
te	Use the traffic engineering metric.

Command Default

The default is the **te** metric.

Command Modes

Global configuration

Command History

Release	Modification
12.0(18)ST	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4	This command was integrated into Cisco IOS Release 12.4.
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.

Usage Guidelines

Use this command to specify the metric type to be used for traffic engineering (TE) tunnels for which the **tunnel mpls traffic-eng path-selection metric** command has not been specified.

The metric type to be used for path calculation for a given tunnel is determined as follows:

- If the **tunnel mpls traffic-eng path-selection metric** command was entered to specify a metric type for the tunnel, use that metric type.
- Otherwise, if the **mpls traffic-eng path-selection metric** was entered to specify a metric type, use that metric type.
- Otherwise, use the default (**te**) metric.

Examples

The following command specifies that if a metric type was not specified for a given TE tunnel, the igp metric should be used for tunnel path calculation:

```
Router(config)# mpls traffic-eng path-selection metric igp
```

Related Commands

Command	Description
tunnel mpls traffic-eng path-selection metric	Specifies the metric type to use when calculating a tunnel's path.

mpls traffic-eng reoptimize

To force immediate reoptimization of all traffic engineering tunnels, use the **mpls traffic-eng reoptimize** command in privileged EXEC mode.

mpls traffic-eng reoptimize

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)ST	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
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.

Examples

The following example shows how to reoptimize all traffic engineering tunnels immediately:

```
Router# mpls traffic-eng reoptimize
```

Related Commands

Command	Description
mpls traffic-eng reoptimize timers delay	Delays removal of old LSPs or installation of new LSPs after tunnel reoptimization.

mpls traffic-eng reoptimize events

To turn on automatic reoptimization of Multiprotocol Label Switching (MPLS) traffic engineering when certain events occur, such as when an interface becomes operational, use the **mpls traffic-eng reoptimize events** command in global configuration mode. To disable automatic reoptimization, use the **no** form of this command.

mpls traffic-eng reoptimize events link-up
no mpls traffic-eng reoptimize events link-up

Syntax Description

link-up	Triggers automatic reoptimization whenever an interface becomes operational.

Command Default

Event-based reoptimization is disabled.

Command Modes

Global configuration (config)

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.
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 example shows how to turn on automatic reoptimization whenever an interface becomes operational:

```
Router(config)# mpls traffic-eng reoptimize events link-up
```

Related Commands

Command	Description
mpls traffic-eng logging lsp	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.
mpls traffic-eng reoptimize	Reoptimizes all traffic engineering tunnels immediately.
mpls traffic-eng reoptimize timers delay	Delays removal of old LSPs or installation of new LSPs after tunnel reoptimization.

mpls traffic-eng reoptimize timers delay

To delay the removal of old label switched paths (LSPs) or installation of new LSPs after tunnel reoptimization, use the **mpls traffic-eng reoptimize timers delay** command in global configuration mode. To restore the default value, use the **no** form of this command.

mpls traffic-eng reoptimize timers delay {**cleanup** *delay-time* | **installation** *delay-time*}
no mpls traffic-eng reoptimize timers delay {**cleanup** *delay-time* | **installation** *delay-time*}

Syntax Description

cleanup *delay-time*	Delays the removal of old LSPs after tunnel reoptimization for the specified number of seconds. The range is from 0 to 300. A value of 0 disables the delay. The default is 10.
installation *delay-time*	Delays the installation of new LSPs with new labels, for the specified number of seconds, after tunnel reoptimization. The range is from 0 to 3600. A value of 0 disables the delay. The default is 3.

Command Default

Removal of old LSPs and installation of new LSPs is not delayed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(32)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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.
12.2(33)SRE7	This command was integrated into Cisco IOS Release 12.2(33)SRE7. The maximum value for the **cleanup** *delay-time* argument was changed from 60 to 300 seconds.
15.0(1)S6	This command was modified. The maximum value for the **cleanup** *delay-time* argument was changed from 60 to 300 seconds.

Usage Guidelines

A device with Multiprotocol Label Switching traffic engineering (MPLS-TE) tunnels periodically examines tunnels with established LSPs to discover if more efficient LSPs (paths) are available. If a better LSP is available, the device signals the more efficient LSP. If the signaling is successful, the device replaces the older LSP with the new, more efficient LSP.

Sometimes, the slower router-point nodes may not utilize the new label's forwarding plane. In this case, if the headend node replaces the labels quickly, packet loss can occur. The packet loss is avoided by delaying the cleanup of the old LSP by using the **mpls traffic-eng reoptimize timers delay cleanup** command. Until the cleanup of the old LSP is performed, subsequent reoptimizations for the tunnel are prevented.

Examples

The following example shows how to set the reoptimization cleanup delay time to one minute:

```
Device# configure terminal
Device(config)# mpls traffic-eng reoptimize timers delay cleanup 60
```

The following example shows how to set the reoptimization installation delay time to one hour:

```
Device# configure terminal
Device(config)# mpls traffic-eng reoptimize timers delay installation 3600
```

Related Commands

Command	Description
mpls traffic-eng reoptimize	Forces immediate reoptimization of all traffic engineering tunnels.
mpls traffic-eng reoptimize events	Turns on automatic reoptimization of MPLS traffic engineering when certain events occur, such as when an interface becomes operational.
mpls traffic-eng reoptimize timers frequency	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.

mpls traffic-eng reoptimize timers frequency

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

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

Syntax Description

seconds	Sets the frequency of reoptimization (in seconds). A value of 0 disables reoptimization. The range is 0 to 604800 seconds (1 week).

Command Default

3600 seconds (1 hour)

Command Modes

Global configuration (config)

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.

Usage Guidelines

A device with traffic engineering tunnels periodically examines tunnels with established LSPs to learn if better LSPs are available. If a better LSP seems to be available, the device attempts to signal the better LSP; if the signaling is successful, the device replaces the old, inferior LSP with the new, better LSP.

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

If you configure a traffic engineering tunnel with an explicit path that is not fully specified (a series of router IDs or a combination of router IDs and interface addresses), then reoptimization may not occur.

Note If you specify a low reoptimization frequency (for example, less than 30 seconds), there may be an increase in CPU utilization for configurations with a large number of traffic engineering tunnels.

Examples

The following example shows how to set the reoptimization frequency to 1 day:

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

Related Commands

Command	Description
mpls traffic-eng reoptimize	Reoptimizes all traffic engineering tunnels immediately.
mpls traffic-eng reoptimize timers delay	Delays removal of old LSPs or installation of new LSPs after tunnel reoptimization.
tunnel mpls traffic-eng path-option	Configures a path option for an MPLS traffic engineering tunnel.

mpls traffic-eng router-id

To specify that the traffic engineering router identifier for the node is the IP address associated with a given interface, use the **mpls traffic-eng router-id** command in router configuration mode. To remove the traffic engineering router identifier, use the **no** form of this command.

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

Syntax Description

interface-name	Interface whose primary IP address is the router's identifier.

Command Default

No traffic engineering router identifier is specified.

Command Modes

Router configuration (config-router)

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 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This router identifier acts as a stable IP address for the traffic engineering configuration. This IP address is flooded to all nodes. For all traffic engineering tunnels originating at other nodes and ending at this node, you must set the tunnel destination to the traffic engineering router identifier of the destination node, because that is the address that the traffic engineering topology database at the tunnel head uses for its path calculation.

You should configure the same traffic engineering router id for all Interior Gateway Protocol (IGP) routing processes.

Examples

The following example shows how to specify the traffic engineering router identifier as the IP address associated with interface Loopback0:

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

Related Commands

Command	Description
mpls atm control-vc	Turns on flooding of MPLS traffic engineering link information in the indicated IGP level/area.

mpls traffic-eng scanner

To specify how often Intermediate System-to-Intermediate System (IS-IS) extracts traffic engineering type, length, values (TLVs) objects from flagged label switched paths (LSPs) and passes them to the traffic engineering topology database, and the maximum number of LSPs that the router can process immediately, use the **mpls traffic-eng scanner** command in router configuration mode. To disable the frequency that IS-IS extracts traffic engineering TLVs and the maximum number of LSPs IS-IS passes to the traffic engineering topology database, use the **no** form of this command.

mpls traffic-eng scanner [**interval seconds**] [**max-flash LSPs**]
no mpls traffic-eng scanner

Syntax Description

interval *seconds*	(Optional) Frequency, in seconds, at which IS-IS sends traffic engineering TLVs into the traffic engineering database. The range is 1 to 60. The default value is 5.
max-flash *LSPs*	(Optional) Maximum number of LSPs that the router can process immediately without incurring a delay. The range is 0 to 200. The default value is 15.

Command Default

IS-IS sends traffic engineering TLVs into the traffic engineering topology database every 5 seconds after the first 15 LSPs are processed.

Command Modes

Router configuration (config-router)

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.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
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.

Usage Guidelines

When IS-IS receives a new LSP, it inserts it into the IS-IS database. If the LSP contains traffic engineering TLVs, IS-IS flags the LSPs for transmission to the traffic engineering database. Depending on the default or user-specified interval, traffic engineering TLVs are extracted and sent to the traffic engineering database. Users can also specify the maximum number of LSPs that the router can process immediately. Processing

entails checking for traffic engineering TLVs, extracting them, and passing them to the traffic engineering database. If more than 50 LSPs need to be processed, there is a delay of 5 seconds for subsequent LSPs.

The first 15 LSPs are sent without a delay into the traffic engineering database. If more LSPs are received, the default delay of 5 seconds applies.

If you specify the **no** form of this command, there is a delay of 5 seconds before IS-IS scans its database and passes traffic engineering TLVs associated with flagged LSPs to the traffic engineering database

Examples

In the following example, the router is allowed to process up to 50 IS-IS LSPs without any delay.

```
Router(config)# router isis
Router(config-router)# mpls traffic-eng scanner interval 5 max-flash 50
```

Related Commands

Command	Description
mpls traffic-eng	Configures a router running IS-IS so that it floods MPLS traffic engineering link information into the indicated IS-IS level.
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

mpls traffic-eng signalling advertise explicit-null

Note Effective with Cisco IOS Release 15.2(2)S, the **mpls traffic-eng signalling advertise implicit-null** command is deprecated by the **mpls traffic-eng signalling advertise explicit-null** command because the IOS MPLS-TE tail router now advertises the implicit-null label in signaling messages sent to neighbors by default. Prior to this release, the IOS MPLS-TE tail router advertised the explicit-null label by default.

To configure the MPLS-TE tail router to override the new default (implicit-null label) to use the MPLS encoding for the explicit-null label in signaling messages advertised to neighbors, use the **mpls traffic-eng signalling advertise explicit-null** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng signalling advertise explicit-null [{*acl-number*}]
no mpls traffic-eng signalling advertise explicit-null

Syntax Description

acl-number	(Optional) Matches the number of the IP access list to determine applicable signalling peers.

Command Default

The IOS MPLS-TE tail router now advertises the implicit-null label in signaling messages sent to neighbors.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.2(2)S	This command was introduced. This command replaces the **mpls traffic-eng signalling advertise implicit-null** command.
Cisco IOS-XE Release 3.6	This command was introduced.

Usage Guidelines

If the **mpls traffic-eng signalling advertise implicit-null** command exists your configuration we recommend that you remove it from your configuration.

The **mpls traffic-eng signalling advertise explicit-null** command is used on an IOS or IOS-XE MPLS-TE tail router to advertise explicit-null label in signaling messages. If the **mpls traffic-eng signalling advertise explicit-null** command is not configured, an implicit-null label (IETF label 3) is advertised in signaling messages.

Examples

The following example shows how to configure the router to use MPLS encoding for the explicit-null label when it sends signaling messages to all peers:

```
Router(config)# mpls traffic-eng signalling advertise explicit-null
```

mpls traffic-eng signalling advertise implicit-null

Note Effective with Cisco IOS Release 15.2(2)S, the **mpls traffic-eng signalling advertise implicit-null** command is deprecated by the **mpls traffic-eng signalling advertise explicit-null** command because the IOS MPLS-TE tail router now advertises the implicit-null label in signaling messages sent to neighbors by default. Prior to this release, the IOS MPLS-TE tail router advertised the explicit-null label by default. See the **mpls traffic-eng signalling advertise explicit-null** command if you want to configure the IOS MPLS-TE tail router to override the new default (implicit-null label) and advertise the explicit-null label to neighbors instead.

To use MPLS encoding for the implicit-null label in signaling messages sent to neighbors, use the **mpls traffic-eng signalling advertise implicit-null** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng signalling advertise implicit-null [{*acl-number*}]
no mpls traffic-eng signalling advertise implicit-null

Syntax Description

acl-number	(Optional) Matches the number of the IP access list to determine applicable signalling peers.

Command Default

None

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.0(5)ST	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
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.
15.2(2)S	This command was replaced by the **mpls traffic-eng signalling advertise explicit-null** command.

Usage Guidelines

The **mpls traffic-eng signalling advertise implicit-null** command is typically used on an IOS MPLS-TE tail router to advertise the IETF implicit-null label "3" signalling message to an non-IOS router.

Examples

The following example shows how to configure the router to use MPLS encoding for the implicit-null label when it sends signaling messages to certain peers:

```
Router(config)# mpls traffic-eng signalling advertise implicit-null
```

mpls traffic-eng srlg

To configure the Shared Risk Link Group (SRLG) membership of a link (interface), use the **mpls traffic-eng srlg** command in interface configuration mode. To remove a link from membership of one or more SRLGs, use the **no** form of this command.

mpls traffic-eng srlg [*num*]
no mpls traffic-eng srlg [*num*]

Syntax Description

num	(Optional) SRLG identifier. The range is 0 to 4294967295.

Command Default

A link does not have membership in any SRLG.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(28)S	This command was introduced.
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

You can enter the **mpls traffic-eng srlg** command multiple times to make a link a member of multiple SRLGs.

Examples

The following example makes the interface a member of SRLG 5:

```
Router(config-if)# mpls traffic-eng srlg 5
```

If you enter the following commands, the interface is a member of both SRLG 5 and SRLG 6:

```
Router(config-if)# mpls traffic-eng srlg 5
Router(config-if)# mpls traffic-eng srlg 6
```

To remove a link from membership of SRLG 5, enter the following command:

```
Router(config-if)# no mpls traffic-eng srlg 5
```

To remove a link from membership of all SRLGs, enter the following command:

```
Router(config-if)# no mpls traffic-eng srlg
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup srlg exclude	Specifies that autocreated backup tunnels should avoid SRLGs of the protected interface.

mpls traffic-eng topology holddown sigerr

To specify the amount of time that a router ignores a link in its traffic engineering topology database in tunnel path Constrained Shortest Path First (CSPF) computations following a traffic engineering tunnel error on the link, use the **mpls traffic-eng topology holddown sigerr** command in global configuration mode. To disable the time set to ignore a ink following a traffic engineering tunnel error on the link, use the **no** form of this command.

mpls traffic-eng topology holddown sigerr *seconds*
no mpls traffic-eng topology holddown sigerr

Syntax Description

seconds	Length of time (in seconds) a router should ignore a link during tunnel path calculations following a traffic engineering tunnel error on the link. The range is 0 to 300.

Command Default

If you do not specify this command, tunnel path calculations ignore a link on which there is a traffic engineering error until either 10 seconds have elapsed or a topology update is received from the Interior Gateway Protocol (IGP).

Command Modes

Global configuration (config)

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.

Usage Guidelines

A router that is at the headend for traffic engineering tunnels might receive a Resource Reservation Protocol (RSVP) No Route error message for an existing tunnel or for one being signaled due to the failure of a link the tunnel traffic traverses before the router receives a topology update from the IGP routing protocol announcing that the link is down. In such a case, the headend router ignores the link in subsequent tunnel path calculations to avoid generating paths that include the link and are likely to fail when signaled. The link is ignored until the router receives a topology update from its IGP or a link hold-down timeout occurs. You can use the **mpls traffic-eng topology holddown sigerr** command to change the link hold-down time from its 10-second default value.

Examples

In the following example, the link hold-down time for signaling errors is set at 15 seconds:

```
Router(config)# mpls traffic-eng topology holddown sigerr 15
```

Related Commands

Command	Description
show mpls traffic-eng topology	Displays the MPLS traffic engineering global topology as currently known at the node.

mpls traffic-eng tunnels (global configuration)

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

mpls traffic-eng tunnels
no mpls traffic-eng tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled.

Command Modes

Global configuration (config)

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 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

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

Examples

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

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

Related Commands

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

mpls traffic-eng tunnels (interface configuration)

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

mpls traffic-eng tunnels

no mpls traffic-eng tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

The MPLS TE is disabled on all interfaces.

Command Modes

Interface configuration (config-if)

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 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Before you enable MPLS TE on the interface, you must enable MPLS TE on the device. An enabled interface has its resource information flooded into the appropriate Interior Gateway Protocol (IGP) link-state database and accepts traffic engineering tunnel signaling requests.

You can use this command to enable MPLS traffic engineering on an interface, thereby eliminating the need to use the **ip rsvp bandwidth** command. However, if your configuration includes Call Admission Control (CAC) for IPv4 Resource Reservation Protocol (RSVP) flows, you must use the **ip rsvp bandwidth rsvp bandwidth** command.

Examples

The following example shows how to enable MPLS traffic engineering on Ethernet interface 0/0:

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

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
mpls traffic-eng tunnels (global configuration)	Enables MPLS traffic engineering tunnel signaling on a device.

mpls ttl-dec

To specify standard Multiprotocol Label Switching (MPLS) tagging, use the **mpls ttl-dec** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mpls ttl-dec
no mpls ttl-dec

Syntax Description

This command has no arguments or keywords.

Command Default

Optimized MPLS tagging (**no mpls ttl-dec**).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	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.

Usage Guidelines

In Cisco IOS Release 12.2(18)SXE and later releases, MPLS tagging has been optimized to allow the rewriting of the original packet's IP type of service (ToS) and Time to Live (TTL) values before the MPLS label is pushed onto the packet header. This change can result in a slightly lower performance for certain types of traffic. If the packet's original ToS/TTL values are not significant, you enter the **mpls ttl-dec** command for standard MPLS tagging.

Examples

This example shows how to configure the Cisco 7600 series router to use standard MPLS tagging behavior:

```
Router(config)# mpls ttl-dec
Router(config)#
```

This example shows how to configure the Cisco 7600 series router to use optimized MPLS tagging behavior:

```
Router(config)# no mpls ttl-dec
Router(config)#
```

Related Commands

Command	Description
mpls l2transport route	Enables routing of Layer 2 packets over MPLS.

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode, connect configuration mode, or xconnect subinterface configuration mode. To restore the MTU value to its original default value, use the **no** form of this command.

mtu *bytes*
no mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

The table below lists default MTU values according to media type.

Table 6: Default Media MTU Values

Media Type	Default MTU (Bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

Command Modes

Interface configuration (config-if)
Connect configuration (xconnect-conn-config)
xconnect subinterface configuration (config-if-xconn)

Command History

Release	Modification
10.0	This command was introduced.
12.0(26)S	This command was modified. This command was updated to support the connect configuration mode for Frame Relay Layer 2 interworking.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command was introduced on the Supervisor Engine 2.
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.

Release	Modification
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4. This command supports xconnect subinterface configuration mode.
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 template configuration mode.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type. On serial interfaces, the MTU size varies but cannot be set to a value less than 64 bytes.

Note The connect configuration mode is used only for Frame Relay Layer 2 interworking.

Changing the MTU Size

Changing the MTU size is not supported on a loopback interface.

Changing the MTU size on a Cisco 7500 series router results in the recarving of buffers and resetting of all interfaces. The following message is displayed: RSP-3-Restart:cbus complex .

You can configure native Gigabit Ethernet ports on the Cisco 7200 series router to a maximum MTU size of 9216 bytes. The MTU values range from 1500 to 9216 bytes. The MTU values can be configured to any range that is supported by the corresponding main interface.

MTU Size for an IPSec Configuration

In an IPSec configuration, such as in a crypto environment, an MTU value that is less than 256 bytes is not accepted. If you configure an MTU value less than 256 bytes, then the MTU value is automatically overwritten and given a value of 256 bytes.

Protocol-Specific Versions of the mtu Command

Changing the MTU value with the **mtu** interface configuration command can affect values for the protocol-specific versions of the command (the **ip mtu** command, for example). If the value specified with the **ip mtu** interface configuration command is the same as the value specified with the **mtu** interface configuration command, and you change the value for the **mtu** interface configuration command, the **ip mtu** value automatically matches the new **mtu** interface configuration command value. However, changing the values for the **ip mtu** configuration commands has no effect on the value for the **mtu** interface configuration command.

ATM and LANE Interfaces

ATM interfaces are not bound by what is configured on the major interface. By default, the MTU on a subinterface is equal to the default MTU (4490 bytes). A client is configured with the range supported by the corresponding main interface. The MTU can be changed on subinterfaces, but it may result in recarving of buffers to accommodate the new maximum MTU on the interface.

VRF-Aware Service Infrastructure Interfaces

The mtu command does not support the VRF-Aware Service Infrastructure (VASI) type interface.

Cisco 7600 Valid MTU Values

On the Cisco 7600 platform, the following valid values are applicable:

- For the SVI ports: from 64 to 9216 bytes
- For the GE-WAN+ ports: from 1500 to 9170 bytes
- For all other ports: from 1500 to 9216 bytes

You can receive jumbo frames on access subinterfaces also. The MTU values can be configured to any range that is supported by the corresponding main interface. If you enable the jumbo frames, the default is 64 bytes for the SVI ports and 9216 bytes for all other ports. The jumbo frames are disabled by default.

Cisco uBR10012 Universal Broadband Router

While configuring the interface MTU size on a Gigabit Ethernet SPA on a Cisco uBR10012 router, consider the following guidelines:

- The default interface MTU size accommodates a 1500-byte packet, plus 22 additional bytes to cover the following overhead:
  - Layer 2 header--14 bytes
  - Dot1Q header--4 bytes
  - CRC--4 bytes
- If you are using MPLS, be sure that the **mpls mtu** command is configured with a value less than or equal to the interface MTU.
- If you are using MPLS labels, you should increase the default interface MTU size to accommodate the number of MPLS labels. Each MPLS label adds 4 bytes of overhead to a packet.

Note For the Gigabit Ethernet SPAs on the Cisco uBR10012 router, the default MTU size is 1500 bytes. When the interface is being used as a Layer 2 port, the maximum configurable MTU is 9000 bytes.

Examples

The following example shows how to specify an MTU of 1000 bytes:

```
Device(config)# interface serial 1
Device(config-if)# mtu 1000
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to specify an MTU size on a Gigabit Ethernet SPA on the Cisco uBR10012 router:

```
Device(config)# interface GigabitEthernet3/0/0
Device(config-if)# mtu 1800
```

The following example shows how to specify an MTU size on a pseudowire interface:

```
Device(config)#  interface pseudowire 100
```

```
Device(config-if)# encapsulation mpls
Device(config-if)# mtu 1800
```

The following example shows how to configure a template and specify an MTU size in template configuration mode: :

```
Device(config)#  template type pseudowire template1
Device(config-if)# encapsulation mpls
Device(config-if)# mtu 1800
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
encapsulation smds	Enables SMDS service on the desired interface.
ip mtu	Sets the MTU size of IP packets sent on an interface.

name (MST)

To set the name of a Multiple Spanning Tree (MST) region, use the **name** command in MST configuration submode. To return to the default name, use the **no** form of this command.

name *name*
no name *name*

Syntax Description

name	Name to give the MST region. It can be any string with a maximum length of 32 characters.

Command Default

Empty string

Command Modes

MST configuration (config-mst)

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

Two or more Cisco 7600 series routers with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.

Caution Be careful when using the **name** command to set the name of an MST region. If you make a mistake, you can put the Cisco 7600 series router in a different region. The configuration name is a case-sensitive parameter.

Examples

This example shows how to name a region:

```
Device(config-mst)# name Cisco
Device(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
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.
spanning-tree mst configuration	Enters MST configuration submode.

neighbor (MPLS)

To specify the peer IP address and virtual circuit (VC) ID value of a Layer 2 VPN (L2VPN) pseudowire, use the **neighbor** command in interface configuration mode. To remove the peer IP address and VC ID value of an L2VPN pseudowire, use the **no** form of this command.

neighbor *peer-address vcid-value*
no neighbor

Syntax Description

peer-address	IP address of the provider edge (PE) peer.
vcid-value	VC ID value. The range is from 1 to 4294967295.

Command Default

Peer address and VC ID value of a pseudowire are not specified.

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 L2VPN command modifications for cross-OS support. This command will replace the *peer-ip-address* `and` *vc-id* arguments 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

You must configure the **neighbor** command for the pseudowire to be functional.

Examples

The following example shows how to specify a peer IP address of 10.1.2.3 and VC ID value of 100.

```
Device(config)# interface pseudowire 100
Device(config-if)# neighbor 10.1.2.3 100
```

Related Commands

Command	Description
label (interface pseudowire)	Configures an AToM static pseudowire connection by defining local and remote circuit labels.
neighbor (L2VPN Pseudowire Switching)	Specifies the routers that should form a point-to-point L2 VFI connection.

neighbor activate

To enable the exchange of information with a Border Gateway Protocol (BGP) neighbor, use the **neighbor activate** command in address family configuration mode or router configuration mode. To disable the exchange of an address with a BGP neighbor, use the **no** form of this command.

neighbor {*ip-addresspeer-group-name* | *ipv6-address***%**} **activate**
no neighbor {*ip-addresspeer-group-name* | *ipv6-address***%**} **activate**

Syntax Description

ip-address	IP address of the neighboring router.
peer-group-name	Name of the BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.

Command Default

The exchange of addresses with BGP neighbors is enabled for the IPv4 address family. Enabling address exchange for all other address families is disabled.

Note Address exchange for address family IPv4 is enabled by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-activate** command before configuring the **neighbor remote-as** command, or you disable address exchange for address family IPv4 with a specific neighbor by using the **no neighbor activate** command.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	Support for address family configuration mode and the IPv4 address family was added.
12.2(2)T	The *ipv6-address* argument and support for the IPv6 address family were added.
12.0(21)ST	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(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added
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.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to advertise address information in the form of an IP or IPv6 prefix. The address prefix information is known as Network Layer Reachability Information (NLRI) in BGP.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

Note The use of the **no** form of the **neighbor activate** command will remove all configurations associated with the neighbor both inside and outside address family configuration mode. This command is not the same as the **neighbor shutdown** command, and you should not use this command to disconnect a BGP adjacency.

Address Exchange Example for Address Family vpn4

The following example shows how to enable address exchange for address family vpnv4 for all neighbors in the BGP peer group named PEPEER and for the neighbor 10.0.0.44:

```
Router(config)# address-family vpnv4
Router(config-router-af)# neighbor PEPEER activate
Router(config-router-af)# neighbor 10.0.0.44 activate
Router(config-router-af)# exit-address-family
```

Address Exchange Example for Address Family IPv4 Unicast

The following example shows how to enable address exchange for address family IPv4 unicast for all neighbors in the BGP peer group named group1 and for the BGP neighbor 172.16.1.1:

```
Device(config)# address-family ipv4 unicast
Device(config-router-af)# neighbor group1 activate
Device(config-router-af)# neighbor 172.16.1.1 activate
```

The following example shows how to enable address exchange for address family IPv6 for all neighbors in the BGP peer group named group2 and for the BGP neighbor 7000::2:

```
Device(config)# address-family ipv6
Device(config-router-af)# neighbor group2 activate
Device(config-router-af)# neighbor 7000::2 activate
```

The following example shows that the **no** command will remove all configurations associated with a neighbor both inside and outside the address family configuration mode. The first set of commands shows the configuration for a specific neighbor.

```
Device(config)# router bgp 64496
Device(config-router)# bgp log neighbor changes
Device(config-router)# neighbor 10.0.0.1 remote-as 64497
Device(config-router)# neighbor 10.0.0.1 update-source Loopback0
Device(config-router)# address-family ipv4
Device(config-router-af)# no synchronization
Device(config-router-af)# no neighbor 10.0.0.1 activate
Device(config-router-af)# no auto-summary
Device(config-router-af)# exit-address-family
Device(config-router)address-family vpnv4
Device(config-router-af)# neighbor 10.0.0.1 activate
Device(config-router-af)# neighbor 10.0.0.1 send-community extended
Device(config-router-af)# exit-address-family
Device(config-router)# address-family ipv4 vrf vrf1
Device(config-router-af)# no synchronization
Device(config-router-af)# redistribute connected
Device(config-router-af)# neighbor 192.168.1.4 remote-as 100
Device(config-router-af)# neighbor 192.168.1.4 version 4
Device(config-router-af)# neighbor 192.168.1.4 activate
Device(config-router-af)# neighbor 192.168.1.4 weight 200
Device(config-router-af)# neighbor 192.168.1.4 prefix-list test out
Device(config-router-af)# exit-address-family
```

The following example shows the router configuration after the use of the **no** command.

```
Device(config)# router bgp 64496
Device(config-router)# address-family ipv4 vrf vrf1
Device(config-router-af)# no neighbor 192.168.1.4 activate
01:01:19: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.1.4 IPv4 Unicast vpn vrf vrf1 topology
 base removed from session  Neighbor deleted
01:01:19: %BGP-5-ADJCHANGE: neighbor 192.168.1.4 vpn vrf vrf1 Down Neighbor deleted
Device(config-router-af)# do show running-config | begin router bgp

router bgp 64496
bgp log-neighbor-changes
neighbor 10.0.0.1 remote-as 64496
neighbor 10.0.0.1 update-source Loopback0
!
address-family ipv4
  no synchronization
  no neighbor 10.0.0.1 activate
  no auto-summary
exit-address-family
!
address-family vpnv4
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 send-community extended
exit-address-family
!
address-family ipv4 vrf vrf1
  no synchronization
  redistribute connected
exit-address-family
```

This example shows the router configuration when the neighbor is reactivated.

```
Device(config)# router bgp 64496
```

```
Device(config-router)# address-family ipv4 vrf vrf1
Device(config-router-af)# neighbor 192.168.1.4 activate
01:02:26: %BGP-5-ADJCHANGE: neighbor 192.168.1.4 vpn vrf vrf1 Up
Device(config-router-af)# do show running-config | begin router bgp

router bgp 64496
bgp log-neighbor-changes
neighbor 10.0.0.1 remote-as 64496
neighbor 10.0.0.1 update-source Loopback0
!
address-family ipv4
  no synchronization
  no neighbor 10.0.0.1 activate
  no auto-summary
exit-address-family
!
address-family vpnv4
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 send-community extended
exit-address-family
!
address-family ipv4 vrf vrf1
  no synchronization
  redistribute connected
  neighbor 192.168.1.4 remote-as 100
  neighbor 192.168.1.4 version 4
  neighbor 192.168.1.4 activate
exit-address-family
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
exit-address-family	Exits from the address family submode.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

neighbor allowas-in

To configure provider edge (PE) routers to allow readvertisement of all prefixes containing duplicate autonomous system numbers (ASNs), use the **neighbor allowas-in** command in router configuration mode. To disable the readvertisement of the ASN of the PE router, use the **no** form of this command.

neighbor *ip-address* **allowas-in** [*number*]
no neighbor allowas-in [*number*]

Syntax Description

ip-address	IP address of the neighboring router.
number	(Optional) Specifies the number of times to allow the advertisement of a PE router's ASN. The range is 1 to 10. If no number is supplied, the default value of 3 times is used.

Command Default

Readvertisement of all prefixes containing duplicate ASNs is disabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.3	This command was integrated into Cisco IOS Release 12.3.
12.3T	This command was integrated into Cisco IOS Release 12.3T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.4T	This command was integrated into Cisco IOS Release 12.4T.
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

In a hub and spoke configuration, a PE router readvertises all prefixes containing duplicate autonomous system numbers. Use the **neighbor allowas-in** command to configure two VRFs on each PE router to receive and readvertise prefixes are as follows:

- One Virtual Private Network routing and forwarding (VRF) instance receives prefixes with ASNs from all PE routers and then advertises them to neighboring PE routers.
- The other VRF receives prefixes with ASNs from the customer edge (CE) router and readvertises them to all PE routers in the hub and spoke configuration.

You control the number of times an ASN is advertised by specifying a number from 1 to 10.

Examples

The following example shows how to configure the PE router with ASN 100 to allow prefixes from the VRF address family Virtual Private Network (VPN) IPv4 vrf1. The neighboring PE router with the IP address 192.168.255.255 is set to be readvertised to other PE routers with the same ASN six times.

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf vrf1
Router(config-router)# neighbor 192.168.255.255 allowas-in 6
```

Related Commands

Command	Description
address-family	Enters the address family configuration submode used to configure routing protocols such as BGP, OSPF, RIP, and static routing.

neighbor as-override

To configure a provider edge (PE) router to override the autonomous system number (ASN) of a site with the ASN of a provider, use the **neighbor as-override** command in router configuration mode. To remove Virtual Private Network (VPN) IPv4 prefixes from a specified router, use the **no** form of this command.

neighbor *ip-address* **as-override**
no neighbor *ip-address* **as-override**

Syntax Description

ip-address	Specifies the IP address of the router that is to be overridden with the ASN provided.

Command Default

Automatic override of the ASN is disabled.

Command Modes

Router configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
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

This command is used in conjunction with the site-of-origin feature, identifying the site where a route originated, and preventing routing loops between routers within a VPN.

Examples

The following example shows how to configure a router to override the ASN of a site with the ASN of a provider:

```
Router(config)# router bgp 100
Router(config-router)# neighbor 192.168.255.255 remote-as 109
Router(config-router)# neighbor 192.168.255.255 update-source loopback0
Router(config-router)# address-family ipv4 vrf vpn1
Router(config-router)# neighbor 192.168.255.255 activate
Router(config-router)# neighbor 192.168.255.255 as-override
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
neighbor remote-as	Allows a neighboring router's IP address to be included in the BGP routing table.
neighbor update-source	Allows internal BGP sessions to use any operational interface for TCP/IP connections.
route-map	Redistributes routes from one routing protocol to another.

neighbor inter-as-hybrid

To configure the Exterior Border Gateway Protocol (eBGP) peer router, which is the neighboring Autonomous System Boundary Router (ASBR), as an Inter-AS Option AB peer, use the **neighbor inter-as-hybrid** command in address family configuration mode. The Inter-AS Option AB feature is a hybrid of Inter-AS Option (10)A and Inter-AS Option (10)B network configurations, enabling the interconnection of different autonomous systems to provide Virtual Private Network (VPN) services. To remove the peer router configuration, use the **no** form of this command.

neighbor {*ip-addresspeer-group-name*} **inter-as-hybrid**
no neighbor {*ip-addresspeer-group-name*} **inter-as-hybrid**

Syntax Description

ip-address	The IP address of the Inter-AS AB neighbor.
peer-group-name	The name of a Border Gateway Protocol (BGP) peer group.

Command Default

No Inter-AS AB neighbor eBGP (ASBR) router is specified.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

Advertised routes have the route targets (RTs) that are configured on the virtual private network (VPN) routing and forwarding (VRF) instance. Advertised routes do not have their original RTs.

If any prefixes are imported into Option AB VRFs, then the imported paths are advertised to this peer.

Examples

The following example shows how to configure an Inter-AS AB neighbor eBGP (ASBR) router:

```
Router(config)# router bgp 100
Router(config-router)# neighbor 192.168.0.1 remote-as 200
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 192.168.0.1 activate
Router(config-router-af)# neighbor 192.168.0.1 inter-as-hybrid
```

Related Commands

Command	Description
address-family vpnv4	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.

Command	Description
inter-as-hybrid	Specifies a VRF as an Option AB VRF.
neighbor	Adds an entry to the BGP or multiprotocol BGP neighbor table.
neighbor activate	Enables the exchange of information with a neighboring router.

neighbor override-capability-neg

To enable the IPv6 address family for a Border Gateway Protocol (BGP) neighbor that does not support capability negotiation, use the **neighbor override-capability-neg**command in address family configuration mode. To disable the IPv6 address family for a BGP neighbor that does not support capability negotiation, use the **no** form of this command.

neighbor {*peer-group-nameipv6-address*} **override-capability-neg**
no neighbor {*peer-group-nameipv6-address*} **override-capability-neg**

Syntax Description

peer-group-name	Name of a BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

Capability negotiation is enabled.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	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(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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

Capability negotiation is used to establish a connection between BGP-speaking peers. If one of the BGP peers does not support capability negotiation, the connection is automatically terminated. The **neighbor override-capability-neg**command overrides the capability negotiation process and enables BGP-speaking peers to establish a connection.

The **neighbor override-capability-neg**command is supported only in address family configuration mode for the IPv6 address family.

Examples

The following example enables the IPv6 address family for BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor 7000::2 override-capability-neg
```

The following example enables the IPv6 address family for all neighbors in the BGP peer group named group1:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group1 override-capability-neg
```

Related Commands

Command	Description
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.

neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the **neighbor remote-as** command in router configuration mode. To remove an entry from the table, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address***%***peer-group-name*} **remote-as** *autonomous-system-number* [{**alternate-as** *autonomous-system-number ...*}]
no neighbor {*ip-address* | *ipv6-address***%***peer-group-name*} **remote-as** *autonomous-system-number* [{**alternate-as** *autonomous-system-number ...*}]

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
peer-group-name	Name of a BGP peer group.
autonomous-system-number	Number of an autonomous system to which the neighbor belongs in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command. When used with the **alternate-as** keyword, up to five autonomous system numbers may be entered.
alternate-as	(Optional) Specifies an alternate autonomous system in which a potential dynamic neighbor can be identified. Up to five autonomous system numbers may be entered when this keyword is specified.

Command Default

There are no BGP or multiprotocol BGP neighbor peers.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
11.0	The *peer-group-name* argument was added.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed.
12.2(4)T	Support for the IPv6 address family was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The **%** keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The **alternate-as** keyword was added to support BGP dynamic neighbors.
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 introduced on Cisco ASR 1000 Series Routers.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Release	Modification
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. To exchange other address prefix types, such as multicast and Virtual Private Network (VPN) Version 4, neighbors must also be activated in the appropriate address family configuration mode.

Use the **alternate-as** keyword introduced in Cisco IOS Release 12.2(33)SXH to specify up to five alternate autonomous systems in which a dynamic BGP neighbor may be identified. BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. After a subnet range is configured and associated with a BGP peer group using the **bgp listen** command and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. The new BGP neighbor will inherit any configuration or templates for the group.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

To ensure a smooth transition, we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, be upgraded to support 4-byte autonomous system numbers.

Examples

The following example specifies that a router at the address 10.108.1.2 is an internal BGP (iBGP) neighbor in autonomous system number 65200:

```
router bgp 65200
 network 10.108.0.0
 neighbor 10.108.1.2 remote-as 65200
```

The following example specifies that a router at the IPv6 address 2001:0DB8:1:1000::72a is an external BGP (eBGP) neighbor in autonomous system number 65001:

```
router bgp 65300
 address-family ipv6 vrf site1
 neighbor 2001:0DB8:1:1000::72a remote-as 65001
```

The following example assigns a BGP router to autonomous system 65400, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 10.108.0.0 and 192.168.7.0 with the neighbor routers. The first router is a remote router in a different autonomous system from the router on which this configuration is entered (an eBGP neighbor); the second **neighbor remote-as** command shows an internal BGP neighbor (with the same autonomous system number) at address 10.108.234.2; and the last **neighbor remote-as** command specifies a neighbor on a different network from the router on which this configuration is entered (also an eBGP neighbor).

```
router bgp 65400
 network 10.108.0.0
 network 192.168.7.0
 neighbor 10.108.200.1 remote-as 65200
 neighbor 10.108.234.2 remote-as 65400
 neighbor 172.29.64.19 remote-as 65300
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only multicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
 address-family ipv4 multicast
  neighbor 10.108.1.1 activate
  neighbor 172.31 1.2 activate
  neighbor 172.16.2.2 activate
  exit-address-family
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only unicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
```

The following example, configurable only in Cisco IOS Release 12.2(33)SXH and later releases, configures a subnet range of 192.168.0.0/16 and associates this listen range with a BGP peer group. Note that the listen range peer group that is configured for the BGP dynamic neighbor feature can be activated in the IPv4 address family using the **neighbor activate** command. After the initial configuration on Router 1, when Router 2 starts a BGP router session and adds Router 1 to its BGP neighbor table, a TCP session is initiated, and Router 1 creates a new BGP neighbor dynamically because the IP address of the new neighbor is within the listen range subnet.

Router 1

```
enable
configure terminal
router bgp 45000
 bgp log-neighbor-changes
 neighbor group192 peer-group
 bgp listen range 192.168.0.0/16 peer-group group192
 neighbor group192 remote-as 40000 alternate-as 50000
 address-family ipv4 unicast
 neighbor group192 activate
 end
```

Router 2

```
enable
configure terminal
router bgp 50000
 neighbor 192.168.3.1 remote-as 45000
 exit
```

If the **show ip bgp summary** command is now entered on Router 1, the output shows the dynamically created BGP neighbor, 192.168.3.2.

```
Router1# show ip bgp summary
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1
BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain format. This example is supported only on Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
```

```
 no auto-summary
 no synchronization
 network 172.17.1.0 mask 255.255.255.0
 exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, or a later release.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp listen	Associates a subnet range with a BGP peer group and activates the BGP dynamic neighbors feature.
neighbor peer-group	Creates a BGP peer group.
router bgp	Configures the BGP routing process.

neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the **neighbor send-community** command in address family or router configuration mode. To remove the entry, use the **no** form of this command.

neighbor {*ip-addressipv6-addresspeer-group-name*} **send-community** [{**both** | **standard** | **extended**}]
no neighbor {*ip-addressipv6-addresspeer-group-name*} **send-community**

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
peer-group-name	Name of a BGP peer group.
both	(Optional) Specifies that both standard and extended communities will be sent.
standard	(Optional) Specifies that only standard communities will be sent.
extended	(Optional) Specifies that only extended communities will be sent.

Command Default

No communities attribute is sent to any neighbor.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.3	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The *ipv6-address* argument was added.
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.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

In the following router configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
 neighbor 172.16.70.23 send-community
```

In the following address family configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
address-family ipv4 multicast
 neighbor 172.16.70.23 send-community
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
match community	Matches a BGP community.
neighbor remote-as	Creates a BGP peer group.
set community	Sets the BGP communities attribute.

neighbor send-label

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with BGP routes to a neighboring BGP router, use the **neighbor send-label** command in address family configuration mode or router configuration mode. To disable this feature, use the **no** form of this command.

neighbor {*ip-addressipv6-addresspeer-group-name*} **send-label** [**explicit-null**]
no neighbor {*ip-addressipv6-addresspeer-group-name*} **send-label** [**explicit-null**]

Syntax Description

ip-address	IP address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
peer-group-name	Name of a BGP peer group.
send-label	Sends Network Layer Reachability Information (NLRI) and MPLS labels to this peer.
explicit-null	(Optional) Advertises the Explicit Null label.

Command Default

BGP routers distribute only BGP routes.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was modified. The *ipv6-address* argument was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **neighbor send-label** command enables a router to use BGP to distribute MPLS labels along with IPv4 routes to a peer router. You must issue this command on both the local and the neighboring router.

This command has the following restrictions:

- If a BGP session is running when you issue the **neighbor send-label** command, the BGP session flaps immediately after the command is issued.
- In router configuration mode, only IPv4 addresses are distributed.

Use the **neighbor send-label** command in address family configuration mode, to bind and advertise IPv6 prefix MPLS labels. Using this command in conjunction with the **mpls ipv6 source-interface** global configuration command allows IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers configured to run both IPv4 and IPv6 traffic forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).

Cisco IOS software installs /32 routes for directly connected external BGP (eBGP) peers when the BGP session for such a peer comes up. The /32 routes are installed only when MPLS labels are exchanged between such peers. Directly connected eBGP peers exchange MPLS labels for:

- IP address families (IPv4 and IPv6) with the **neighbor send-label** command enabled for the peers
- VPN address families (VPNv4 and VPNv6)

A single BGP session can include multiple address families. If one of the families exchanges MPLS labels, the /32 neighbor route is installed for the connected peer.

Examples

The following example shows how to enable a router in autonomous system 65000 to send MPLS labels with BGP routes to the neighboring BGP router at 192.168.0.1:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.0.1 remote-as 65001
Router(config-router)# neighbor 192.168.0.1 send-label
```

The following example shows how to enable a router in the autonomous system 65000 to bind and advertise IPv6 prefix MPLS labels and send the labels with BGP routes to the neighboring BGP router at 192.168.99.70:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.99.70 remote-as 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# neighbor 192.168.99.70 activate
Router(config-router-af)# neighbor 192.168.99.70 send-label
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
neighbor activate	Enables the exchange of information with a neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
mpls ipv6 source-interface	Specifies an IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over an MPLS network.

neighbor send-label explicit-null

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router, use the **neighbor send-label explicit-null** command in address family configuration mode or router configuration mode. To disable a BGP router from sending MPLS labels with explicit-null information, use the **no** form of this command.

neighbor *ip-address* **send-label explicit-null**
no neighbor *ip-address* **send-label explicit-null**

Syntax Description

ip-address	IP address of the neighboring router.

Command Default

None

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4
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.

Usage Guidelines

This command enables a CSC-CE router to use BGP to distribute MPLS labels with a value of zero for explicit-null instead of implicit-null along with IPv4 routes to a CSC-PE peer router.

You must issue this command only on the local CSC-CE router.

You can use this command only with IPv4 addresses.

Examples

In the following CSC-CE example, CSC is configured with BGP to distribute labels and to advertise explicit null for all its connected routes:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# router bgp 100
Router(config-router)# neighbor 10.0.0.2 remote-as 300
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.0.0.2 send-label explicit-null
```

In the following CSC-PE example, CSC is configured with BGP to distribute labels:

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# router bgp 300
Router(config-router)# neighbor 10.0.0.1 remote-as 100
Router(config-router)# address-family ipv4 vrf v1
Router(config-router-af)# neighbor 10.0.0.1 send-label
```

Note Explicit null is not applicable on a CSC-PE router.

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a neighboring router.
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.

neighbor suppress-signaling-protocol

To suppress a Virtual Private LAN Service (VPLS) signaling protocol use the **neighbor suppress-signaling-protocol** command in address family configuration or router configuration mode. To remove the entry, use the **no** form of this command.

neighbor {*ipv4-addressipv6-addresspeer-group-name*} **suppress-signaling-protocol ldp**
no neighbor {*ipv4-addressipv6-addresspeer-group-name*} **suppress-signaling-protocol ldp**

Syntax Description

ipv4-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
peer-group-name	Name of a BGP peer group.
ldp	Specifies that Label Distribution Protocol (LDP) signaling will be suppressed.

Command Default

LDP signaling is not suppressed.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

If you specify that LDP signaling is suppressed by using the **ldp** keyword, BGP signaling will be enabled.

Examples

```
Device(config-router-af)# neighbor 10.10.10.1 suppress-signaling-protocol ldp
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
neighbor remote-as	Creates a BGP peer group.

neighbor update-source

To have the Cisco software allow Border Gateway Protocol (BGP) sessions to use any operational interface for TCP connections, use the **neighbor update-source** command in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*[{**%**}]*peer-group-name*} **update-source** *interface-type interface-number*
neighbor {*ip-address* | *ipv6-address*[{**%**}]*peer-group-name*} **update-source** *interface-type interface-number*

Syntax Description

ip-address	IPv4 address of the BGP-speaking neighbor.
ipv6-address	IPv6 address of the BGP-speaking neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
peer-group-name	Name of a BGP peer group.
interface-type	Interface type.
interface-number	Interface number.

Command Default

Best local address

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)T	The *ipv6-address* argument was added.
12.0(21)ST	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(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added.
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.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command can work in conjunction with the loopback interface feature described in the "Interface Configuration Overview" chapter of the Cisco IOS Interface and Hardware Component Configuration Guide.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

The **neighbor update-source** command must be used to enable IPv6 link-local peering for internal or external BGP sessions.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces and for these link-local IPv6 addresses you must specify the interface they are on. The syntax becomes <IPv6 local-link address>%<interface name>, for example, FE80::1%Ethernet1/0. Note that the interface type and number must not contain any spaces, and be used in full-length form because name shortening is not supported in this situation. The % keyword and subsequent interface syntax is not used for non-link-local IPv6 addresses.

Examples

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:

```
router bgp 65000
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 110
 neighbor 172.16.2.3 update-source Loopback0
```

The following example sources IPv6 BGP TCP connections for the specified neighbor in autonomous system 65000 with the global IPv6 address of loopback interface 0 and the specified neighbor in autonomous system 65400 with the link-local IPv6 address of Fast Ethernet interface 0/0. Note that the link-local IPv6 address of FE80::2 is on Ethernet interface 1/0.

```
router bgp 65000
 neighbor 3ffe::3 remote-as 65000
 neighbor 3ffe::3 update-source Loopback0
 neighbor fe80::2%Ethernet1/0 remote-as 65400
 neighbor fe80::2%Ethernet1/0 update-source FastEthernet 0/0
 address-family ipv6
  neighbor 3ffe::3 activate
  neighbor fe80::2%Ethernet1/0 activate
  exit-address-family
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

neighbor (VPLS transport mode)

To create pseudowires with specific provider edge (PE) routers in an L2VPN Advanced VPLS configuration, use the **neighbor** command in VPLS transport configuration mode. To remove the pseudowires, use the **no** form of this command.

neighbor *remote-router-id* [**pw-class** *pw-class-name*]
no neighbor *remote-router-id*

Syntax Description

remote-router-id	Remote peer router identifier. The remote router ID can be any IP address, as long as it is reachable.
pw-class	(Optional) Specifies the pseudowire class configuration from which the data encapsulation type is taken.
pw-name-name	Name of the pseudowire class.

Command Default

Pseudowires are not created.

Command Modes

VPLS transport configuration (config-if-transport)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **neighbor** command uses default values for the VFI name, VPN ID, and encapsulation type.

Examples

The following example shows how two pseudowires are created with PE routers 10.2.2.2 and 10.3.3.3:

```
Router(config)# interface virtual-ethernet 1
Router(config-if)# transport vpls mesh
Router(config-if-transport)# neighbor 10.2.2.2 pw-class 1
Router(config-if-transport)# neighbor 10.3.3.3 pw-class 1
```

Related Commands

Command	Description
transport vpls mesh	Creates a full mesh of pseudowires under a virtual private LAN switching (VPLS) domain.

neighbor (VPLS)

To specify the type of tunnel signaling and encapsulation mechanism for each Virtual Private LAN Service (VPLS) peer, use the **neighbor** command in L2 VFI manual configuration mode. To disable a split horizon, use the **no** form of this command.

neighbor *remote-router-id vc-id* {**encapsulation** *encapsulation-type* | **pw-class** *pw-name*} [**no-split-horizon**]
no neighbor *remote-router-id* [*vc-id*]

Syntax Description

remote-router-id	Remote peer router identifier. The remote router ID can be any IP address, as long as it is reachable.
vc-id	32-bit identifier of the virtual circuit between the routers.
encapsulation	Specifies tunnel encapsulation.
encapsulation-type	Specifies the tunnel encapsulation type; valid values are **l2tpv3** and **mpls**.
pw-class	Specifies the pseudowire class configuration from which the data encapsulation type is taken.
pw-name	Name of the pseudowire class.
no-split-horizon	(Optional) Disables the Layer 2 split horizon forwarding in the data path.

Command Default

Split horizon is enabled.

Command Modes

L2 VFI manual configuration (config-vfi)

Command History

Release	Modification
12.2(18)SXF	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(33)SRB	This command was modified. This command was updated so that the remote router ID need not be the LDP router ID of the peer.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

In a full-mesh VPLS network, keep split horizon enabled to avoid looping.

With the introduction of VPLS Autodiscovery, the remote router ID no longer needs to be the LDP router ID. The address that you specify can be any IP address on the peer, as long as it is reachable. When VPLS Autodiscovery discovers peer routers for the VPLS, the peer router addresses might be any routable address.

Examples

This example shows how to specify the tunnel encapsulation type:

```
Device(config-vfi)# l2 vfi vfi-1 manual
Device(config-vfi)# vpn 1
Device(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls
```

This example shows how to disable the Layer 2 split horizon in the data path:

```
Device(config-vfi)# l2 vfi vfi-1 manual
Device(config-vfi)# vpn 1
Device(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls no-split-horizon
```

Related Commands

Command	Description
l2 vfi manual	Creates a Layer 2 VFI.

network (IPv6)

To configure the network source of the next hop to be used by the PE VPN, use the network command in router configuration mode. To disable the source, use the **no** form of this command.

network *ipv6-address/prefix-length*
no network *ipv6-address/prefix-length*

Syntax Description

ipv6-address	The IPv6 address to be used.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

Next-hop network sources are not configured.

Command Modes

Address family configuration
Router configuration

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.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The *ipv6-address* argument in this command configures the IPv6 network number.

Examples

The following example places the router in address family configuration mode and configures the network source to be used as the next hop:

```
Router(config)# router bgp 100
Router(config-router)# network 2001:DB8:100::1/128
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.

next-address

To specify the next IP address in the explicit path, use the **next-address** command in IP explicit path configuration mode.

next-address [{**loose** | **strict**}] *ip-address*

Syntax Description

loose	(Optional) Specifies that the previous address (if any) in the explicit path need not be directly connected to the next IP address, and that the router is free to determine the path from the previous address (if any) to the next IP address.
strict	(Optional) Specifies that the previous address (if any) in the explicit path must be directly connected to the next IP address.
ip-address	Next IP address in the explicit path.

Command Default

The next IP address in the explicit path is not specified.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(19)ST1	The **loose**and **strict** keywords were added.
12.0(21)ST	Support for the Cisco 12000 series router was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)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.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

To specify an explicit path that includes only the addresses specified, specify each address in sequence by using the **next-address** command without the **loose** keyword.

To configure an interarea traffic engineering (TE) tunnel, configure the tunnel path options as loose explicit paths. Specify that each Autonomous System Boundary Router (ASBR) traversed by the tunnel label switched path (LSP) is a loose hop by entering the **next-address loose** command.

To use explicit paths for TE tunnels within an Interior Gateway Protocol (IGP) area, you can specify a combination of both loose and strict hops.

When specifying an explicit path for an MPLS TE tunnel, you can specify link or node addresses of the next-hop routers in an explicit path. You can also specify a mixture of link and node addresses. However, there are some restrictions:

- In Cisco IOS Releases 12.2(33)SRD and 12.4(24)T, and Cisco XE Release 2.4 and earlier releases, you cannot specify an explicit path that uses a link address as the first hop and then node addresses as the subsequent hops. However, you can use a node address as the first hop andlink addresses as the subsequent hops.
- In Cisco IOS Releases after 12.2(33)SRD, 12.4(24)T , and Cisco XE Release 2.4, you can use a link address as the first hop and then node addresses as the subsequent hops. There are no restrictions when specifying a mixture of link and node addresses.

When specifying an explicit path, if you specify the "forward" address (the address of the interface that forwards the traffic to the next router) as the next-hop address, the explicit path might not be used. Using the forward address allows that entry to be treated as a loose hop for path calculation. Cisco recommends that you use the "receive"address (the address of the interface that receives traffic from the sending router) as the next-hop address.

In the following example, router R3 sends traffic to router R1. The paths marked a,b and x,y between routers R1 and R2 are parallel paths.

```
R1(a)----(b)R2(c)--(d)R3
  (x)----(y)
```

If you configure an explicit path from R3 to R1 using the "forward" addresses (addresses d and b), the tunnel might reroute traffic over the parallel path (x,y) instead of the explicit path. To ensure that the tunnel uses the explicit path, specify the "receive" addresses as part of the **next-address** command, as shown in the following example:

```
ip explicit-path name path1
  next-address ©)
  next-address (a)
```

Examples

The following example shows how to assign the number 60 to the IP explicit path, enable the path, and specify 10.3.27.3 as the next IP address in the list of IP addresses:

```
Router(config)# ip explicit-path identifier 60 enable
Router(cfg-ip-expl-path)# next-address 10.3.27.3
Explicit Path identifier 60:
    1: next-address 10.3.27.3
```

The following example shows a loose IP explicit path with ID 60. An interarea TE tunnel has a destination of 10.3.29.3 and traverses ASBRs 10.3.27.3 and 10.3.28.3.

```
Router(config)# ip explicit-path identifier 60
Router(cfg-ip-expl-path)# next-address loose 10.3.27.3
Router(cfg-ip-expl-path)# next-address loose 10.3.28.3
Router(cfg-ip-expl-path)# next-address loose 10.3.29.3
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number.

Command	Description
index	Inserts or modifies a path entry at a specified index.
ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.
list	Displays all or part of the explicit paths.
show ip explicit-paths	Displays configured IP explicit paths.

passive-interface (IPv6)

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

passive-interface [{**default** | *interface-type interface-number*}]
no passive-interface [{**default** | *interface-type interface-number*}]

Syntax Description

default	(Optional) All interfaces become passive.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Default

No interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
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.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

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

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

OSPF for IPv6 routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF for IPv6 domain.

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

Examples

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

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

oam retry

To configure parameters related to Operation, Administration, and Maintenance (OAM) management for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), VC class, or VC bundle, or label-controlled ATM (LC-ATM) VC, use the **oam retry** command in the appropriate command mode. To remove OAM management parameters, use the **no** form of this command.

oam retry *up-count down-count retry-frequency*
no oam retry

Syntax Description

up-count	Number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a connection state to up. This argument does not apply to SVCs.
down-count	Number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to change the state to down or tear down an SVC connection.
retry-frequency	The frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up/down state is being verified. For example, if a PVC is up and a loopback cell response is not received after the *retry-frequency* (in seconds) argument is specified using the **oam-pvc** command, loopback cells are sent at the *retry-frequency* to verify whether the PVC is down.

Command Default

ATM PVCs and SVCs

up-count : 3*down-count*: 5*retry-frequency*: 1 second

LC-ATM VCs

up-count : 2*down-count*: 2*retry-frequency*: 2 seconds

Command Modes

Bundle configuration mode (for a VC bundle)
Control-VC configuration (for an LC-ATM VC)
Interface-ATM-VC configuration (for an ATM PVC or SVC)
PVC range configuration (for an ATM PVC range)
PVC-in-range configuration (for an individual PVC within a PVC range)
VC-class configuration (for a VC class)

Command History

Release	Modification
11.3T	This command was introduced.
12.0(3)T	This command was modified to allow configuration parameters related to OAM management for ATM VC bundles.
12.1(5)T	This command was implemented in PVC range and PVC-in-range configuration modes.
12.3(2)T	This command was implemented in control-VC configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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 following guidelines apply to PVCs, SVCs, and VC classes. They do not apply to LC-ATM VCs.

- For ATM PVCs, SVCs, or VC bundles, if the **oam retry** command is not explicitly configured, the VC inherits the following default configuration (listed in order of precedence):
  - Configuration of the **oam retry** command in a VC class assigned to the PVC or SVC itself.
  - Configuration of the **oam retry** command in a VC class assigned to the PVC's or SVC's ATM subinterface.
  - Configuration of the **oam retry** command in a VC class assigned to the PVC's or SVC's ATM main interface.
  - Global default: *up-count* = 3, *down-count* = 5, *retry-frequency* = 1 second. This set of defaults assumes that OAM management is enabled using the **oam-pvc** or **oam-svc** command. The *up-count* and *retry-frequency* arguments do not apply to SVCs.
- To use this command in bundle configuration mode, enter the bundle command to create the bundle or to specify an existing bundle before you enter this command.
- If you use the **oam retry** command to configure a VC bundle, you configure all VC members of that bundle. VCs in a VC bundle are further subject to the following inheritance rules (listed in order of precedence):
  - VC configuration in bundle-vc mode
  - Bundle configuration in bundle mode (with the effect of assigned VC-class configuration)
  - Subinterface configuration in subinterface mode

Examples

The following example shows how to configure the OAM management parameters with an up count of 3, a down-count of 3, and the retry frequency set at 10 seconds:

```
Router(cfg-mpls-atm-cvc)# oam retry 3 3 10
```

Related Commands

Command	Description
broadcast	Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle.
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
encapsulation	Sets the encapsulation method used by the interface.
inarp	Configures the Inverse ARP time period for an ATM PVC, VC class, or VC bundle.
oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for a virtual circuit class that can be applied to a virtual circuit bundle.

Command	Description
oam-pvc	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM PVC or virtual circuit class.
oam-svc	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM SVC or virtual circuit class.
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.

oam-ac emulation-enable

To enable Operation, Administration, and Maintenance (OAM) cell emulation on ATM adaptation layer 5 (AAL5) over Multiprotocol Label Switching (MPLS) or Layer 2 Tunnel Protocol Version 3 (L2TPv3), use the **oam-ac emulation-enable** command in the appropriate configuration mode on both provider edge (PE) routers. To disable OAM cell emulation, use the **no** form of this command on both routers.

oam-ac emulation-enable [*seconds*]
no oam-ac emulation-enable

Syntax Description

seconds	(Optional) The rate (in seconds) at which the alarm indication signal (AIS) cells should be sent. The range is 0 to 60 seconds. If you specify 0, no AIS cells are sent. The default is 1 second, which means that one AIS cell is sent every second.

Command Default

OAM cell emulation is disabled.

Command Modes

L2transport PVC configuration--for an ATM PVC
VC class configuration mode--for a VC class

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(30)S	This command was updated to enable OAM cell emulation as part of a virtual circuit (VC) class.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
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(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

This command is used with AAL5 over MPLS or L2TPv3 and is not supported with ATM cell relay over MPLS or L2TPv3.

Examples

The following example shows how to enable OAM cell emulation on an ATM permanent virtual circuit (PVC):

```
Router# interface ATM 1/0/0
Router(config-if)# pvc ½00 l2transport
Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable
```

The following example shows how to set the rate at which an AIS cell is sent every 30 seconds:

```
Router# interface ATM 1/0/0
Router(config-if)# pvc ½00 l2transport
Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable 30
```

The following example configures OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to an interface.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm oamclass
Router(config-vc-class)# encapsulation aal5
Router(config-vc-class)# oam-ac emulation-enable 30
Router(config-vc-class)# oam-pvc manage
Router(config)# interface atm1/0
Router(config-if)# class-int oamclass
Router(config-if)# pvc ½00 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.

oam-pvc

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM permanent virtual circuit (PVC), virtual circuit (VC) class, or label-controlled ATM (LC-ATM) VC, use the **oam-pvc** command in the appropriate command mode. To disable generation of OAM loopback cells and OAM management, use the **no** form of this command.

ATM VC
oam-pvc [{*frequency* | **manage** [*frequency*] [{**auto-detect** [**optimum**] | **keep-vc-up** [**seg aisrdi failure**] | **loop-detection**}]}]
no oam-pvc [{*frequency* | **manage** [*frequency*] [{**auto-detect** [**optimum**] | **keep-vc-up** [**seg aisrdi failure**] | **loop-detection**}]}]

VC Class
oam-pvc [{*frequency* | **manage** [*frequency* [{**auto-detect** [**optimum**] | **loop-detection**}]]}]
no oam-pvc [{*frequency* | **manage** [*frequency* [{**auto-detect** [**optimum**] | **loop-detection**}]]}]

Loopback Mode Detection
oam-pvc manage [*frequency*] **loop-detection**
no oam-pvc manage loop-detection

Cisco 10000 Series Router
oam-pvc [{*frequency* | **manage** [*frequency* [{**auto-detect** [**optimum**] | **keep-vc-up** [**seg aisrdi failure**]}]]}]
no oam-pvc [{*frequency* | **manage** [*frequency* [{**auto-detect** [**optimum**] | **keep-vc-up** [**seg aisrdi failure**]}]]}]

Syntax Description

frequency	(Optional) Specifies the time delay between transmittals of OAM loopback cells, in seconds. For ATM VCs or VC classes and loopback mode detection, the range is 0 to 600, and the default is 10. For LC-ATM VCs, the range is 0 to 255, and the default is 5.
manage	(Optional) for ATM VCs or VC classes; required for LC-ATM VCs) Enables OAM management. The default is disabled.
auto-detect	(Optional) Enables automatic detection of peer OAM command cells.
optimum	(Optional) Configures an optimum mode so that when the traffic-monitoring timer expires, the PVC sends an OAM command cell at the locally configured frequency instead of going into retry mode immediately. If there is no response, the PVC goes into retry mode.
keep-vc-up	(Optional) Specifies that the VC will be kept in the UP state when continuity check (CC) cells detect connectivity failure.
seg aisrdi failure	(Optional) Specifies that if segment alarm indication signal/remote defect indication (AIS/RDI) cells are received, the VC will not be brought down because of end CC failure or loopback failure.

loop-detection	(Optional) Enables automatic detection of whether the physically connected ATM switch is in loopback mode. The default is disabled.

Command Default

OAM management and loop detection are disabled.

Command Modes

ATM VC class configuration (config-vc-class)
ATM VC configuration (config-if-atm-vc)
Control-VC configuration (cfg-mpls-atm-cvc)
PVC-in-range configuration (cfg-if-atm-range-pvc)

Command History

Release	Modification
11.3	This command was introduced.
12.1(5)T	This command was implemented in PVC-in-range configuration mode.
12.3(2)T	This command was implemented for LC-ATM VCs.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S, and the **loop-detection** 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.
12.2SX	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(31)SB10	The **loop-detection** keyword was added.
Cisco IOS XE Release 2.3	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

If OAM management is enabled, further control of OAM management is configured by using the **oam retry** command.

ATM VC or VC Classes

If the **oam-pvc** command is not explicitly configured on an ATM PVC, the PVC inherits the following default configuration (in order of precedence):

- Configuration from the **oam-pvc** command in a VC class assigned to the PVC itself.
- Configuration from the **oam-pvc** command in a VC class assigned to the ATM subinterface of the PVC.
- Configuration from the **oam-pvc**command in a VC class assigned to the ATM main interface of the PVC.
- Global default: End-to-end F5 OAM loopback cell generation and OAM management are disabled, but if OAM cells are received, they are looped back. The default value for the *frequency* argument is 10 seconds.

Specifying the ATM VC or VC Classes

You can select the VCs or VC classes to which to apply OAM management and loop detection by using the **oam-pvc** command in any of the following command modes:

- ATM VC class configuration--for a VC class
- ATM VC configuration mode--for an ATM PVC or loopback mode detection
- Control-VC configuration mode--for enabling OAM management on an LC-ATM VC
- PVC-in-range configuration--for an individual PVC within a PVC range

Loopback Mode Detection

When a PVC traverses an ATM cloud and OAM is enabled, the router sends a loopback cell to the other end and waits for a response to determine whether the circuit is up. However, if an intervening router within the ATM cloud is in loopback mode, the router considers the circuit to be up, when in fact the other end is not reachable.

When enabled, the Loopback Mode Detection Through OAM feature detects when an intervening router is in loopback mode, in which case it sets the OAM state to NOT_VERIFIED. This prevents traffic from being routed on the PVC for as long as any intervening router is detected as being in loopback mode.

Examples

The following example shows how to enable end-to-end F5 OAM loopback cell transmission and OAM management on an ATM PVC with a transmission frequency of 3 seconds:

```
Router(cfg-mpls-atm-cvc)# oam-pvc manage 3
```

The following example shows how to enable end-to-end F5 OAM loopback cell transmission and OAM management on an LC-ATM interface with a transmission frequency of 2 seconds:

```
Router(config)# interface Switch1.10 mpls
Router(config-subif)# ip unnumbered Loopback0
Router(config-subif)# mpls atm control-vc 0 32
Router(cfg-mpls-atm-cvc)# oam-pvc manage 2
```

The following example shows how to create a PVC and enable loopback detection:

```
Router(config)# interface ATM1/0
Router(config-if)# pvc 4/100
Router(config-if-atm-vc)# oam-pvc manage loop-detection
```

Related Commands

Command	Description
ilmi manage	Enables ILMI management on an ATM PVC.
oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or LC-ATM VC.
show atm pvc	Displays all ATM PVCs and traffic information.

psc refresh interval

To configure the refresh interval for Protection State Coordination (PSC) Protocol messages, use the **psc refresh interval** command in MPLS TP global configuration mode. To remove the configuration, use the **no** form of this command.

psc {**fast** | **slow** | **remote**} **refresh interval** {*time-in-msectime-in-sec*} [**message-count** *num*]
no psc {**fast** | **slow** | **remote**} **refresh interval** {*time-in-msectime-in-sec*} [**message-count** *num*]

Syntax Description

fast	Specifies the fast refresh interval for PSC messages. The default is 1000 ms with a jitter of 50 percent. The range is from 1000 ms to 5000 sec.
slow	Specifies the slow refresh interval for PSC messages. The default is 5 sec. The range is from 5 secs to 86400 secs (24 hours).
remote	Specifies the remote-event expiration timer. By default, this timer is disabled. The remote refresh interval range is from 5 to 86400 sec (24 hours). The message count is from 5 to 1000. If you do not specify the message count value, it is set to 5, which is the default.
message-count *num*	(Optional) Indicates the number of messages.

Command Default

No intervals are specified.

Command Modes

MPLS TP global configuration mode (config-mpls-tp)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

The following example configures a fast refresh interval of 1000 ms.

```
Device(config-mpls-tp)# psc fast refresh interval 1000
```

The following example configures a slow refresh interval of 60 sec.

```
Device(config-mpls-tp)# psc slow refresh interval 60
```

The following example configures a remote refresh interval of 2400 sec and a message count of 10.

```
Device(config-mpls-tp)# psc remote refresh interval 2400 message-count 10
```

Related Commands

Command	Description
emulated-lockout	Enables the sending of emulated lockout commands on working/protection transport entities.

Command	Description
manual-switch	Issues a local manual switch condition on a working LSP.
show mpls tp	Displays a summary of MPLS-TP settings or a detailed list of MPLS-TP tunnels.
debug mpls tp	Enables debugging for MPLS-TP.
clear mpls tp	Clears the counters or a remote event for PSC signaling messages based on a tunnel number or name.

ping mpls

To check Multiprotocol Label Switching (MPLS) label switched path (LSP) connectivity, use the **ping mpls** command in privileged EXEC mode.

ping mpls {**ipv4** *destination-address/destination-mask-length* [{**destination** *address-start address-end increment*}] {**ttl** *time-to-live*} | **pseudowire** *ipv4-address vc-id* [{**segment** [{*segment-number*}]}] [{**destination** *address-start address-end increment*}] | **traffic-eng** *tunnel-interface tunnel-number* [{**ttl** *time-to-live*}]}[{**revision** {**1** | **2** | **3** | **4**}}][{**source** *source-address*}][{**repeat** *count*}][{**timeout** *seconds*}][{**size** *packet-size* | *minimum maximum size-increment*}][{**pad** *pattern*}][{**reply dscp** *dscp-value*}][{**reply pad-tlv**}][{**reply mode** {**ipv4** | **router-alert**}}][{**interval** *ms*}][{**exp** *exp-bits*}][{**verbose**}][{**revision** *tlv-revision-number*}][{**force-explicit-null** }][{**output interface** *tx-interface* [{**nexthop** *ip-address*}]}][{**dsmap** [{**hashkey** {**none** | **ipv4 bitmap** *bitmap-size*}}]}][{**flags fec**}]

Syntax Description

ipv4	Specifies the destination type as a Label Distribution Protocol (LDP) IPv4 address.
destination-address	Address prefix of the target to be tested.
/ *destination-mask-length*	Number of bits in the network mask of the target address. The slash is required.
destination	(Optional) Specifies a network 127 address.
address-start	(Optional) Beginning network 127 address.
address-end	(Optional) Ending network 127 address.
increment	(Optional) Number by which to increment the network 127 address.
ttl *time-to-live*	(Optional) Specifies a time-to-live (TTL) value. The default is 225 seconds.
pseudowire	Specifies the destination type as an Any Transport over MPLS (AToM) virtual circuit (VC).
ipv4-address	IPv4 address of the AToM VC to be tested.
vc-id	Specifies the VC identifier of the AToM VC to be tested.
segment *segment-number*	(Optional) Specifies a segment of a multisegment pseudowire.
traffic-eng	Specifies the destination type as an MPLS traffic engineering (TE) tunnel.
tunnel-interface	Tunnel interface to be tested.
tunnel-number	Tunnel interface number.

revision {**1** | **2** | **3** | **4**}	(Optional) Selects the type, length, values (TLVs) version of the implementation. Use the **revision 4** as the default unless attempting to interoperate with devices running Cisco IOS Release 12.0(27)S1 or 12.0(27)S2. If you do not select a **revision** keyword, the software uses the latest version. See the table in the "Revision Keyword Usage" section of the "Usage Guidelines" section for information on when to select the **1**, **2**, **3**, and **4** keywords.
source *source-address*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
repeat *count*	(Optional) Specifies the number of times to resend the same packet. The range is 1 to 2147483647. The default is 1. If you do not enter the **repeat** keyword, the software resends the same packet five times.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds for an MPLS request packet. The range is 0 to 3600. The default is 2 seconds.
size *packet-size*	(Optional) Specifies the size of the packet with the label stack imposed. Packet size is the number of bytes in each ping. The range is 40 to 18024. The default is 100.
sweep	(Optional) Enables you to send a number of packets of different sizes, ranging from a start size to an end size. This parameter is similar to the Internet Control Message Protocol (ICMP) **ping sweep** parameter.
minimum	(Optional) Minimum or start size for an MPLS echo packet. The lower boundary of the **sweep** range varies depending on the LSP type. The default is 100 bytes.
maximum	(Optional) Maximum or end size for an echo packet. The default is 17,986 bytes.
size-increment	(Optional) Number by which to increment the echo packet size. The default is 100 bytes.
pad *pattern*	(Optional) The pad TLV is used to fill the datagram so that the MPLS echo request (User Datagram Protocol [UDP] packet with a label stack) is the specified size. The default is 0xABCD.
reply dscp *dscp-value*	(Optional) Provides the capability to request a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value. The echo reply is returned with the IP header type of service (ToS) byte set to the value specified in the **reply dscp** command.
reply pad-tlv	(Optional) Tests the ability of the sender of an echo reply to support the copy pad TLV to echo reply.

reply mode {**ipv4** | **router-alert**}	(Optional) Specifies the reply mode for the echo request packet. **ipv4** --Reply with an IPv4 UDP packet (default). **router-alert** --Reply with an IPv4 UDP packet with router alert.
interval *ms*	(Optional) Specifies the time, in milliseconds (ms), between successive MPLS echo requests. This parameter allows you to pace the transmission of packets so that the receiving router does not drop packets. Default is 0.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. The range is 0 to 7. Default is 0.
verbose	(Optional) Displays the MPLS echo reply sender address of the packet and displays return codes.
revision *tlv-revision-number*	(Optional) Cisco TLV revision number.
force-explicit-null	(Optional) Forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.
output interface *tx-interface*	(Optional) Specifies the output interface for echo requests.
nexthop *ip-address*	(Optional) Causes packets to go through the specified next-hop address.
dsmap	(Optional) Interrogates a transit router for downstream mapping (DSMAP) information.
hashkey {**none** | **ipv4 bitmap** *bitmap-size*}	(Optional) Allows you to control the hash key and multipath settings. Valid values are: **none** --There is no multipath (type 0). **ipv4bitmap** *bitmap-size*--Size of the IPv4 addresses (type 8) bitmap. If you enter the **none** keyword, multipath LSP traceroute acts like enhanced LSP traceroute; that is, it uses multipath LSP traceroute retry logic and consistency checking.
flags fec	(Optional) Allows Forward Equivalence Class (FEC) checking on the transit router. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Target FEC stack validation is always done at the egress router. Be sure to use this keyword with the **ttl** keyword.

Command Default

You cannot check MPLS LSP connectivity.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(18)SXE	The **reply dscp** and **reply pad-tlv** keywords were added.

Release	Modification
12.4(6)T	The following keywords were added: **revision**, **force-explicit-null**, **output interface**, **dsmap**, **hashkey**, **none**, **ipv4 bitmap**, and **flags fec**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.0(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. The **nexthop** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.3	This command was updated with the **segment** keyword.
12.2(33)SRE	This command was modified. Restrictions were added to the **pseudowire**keyword.
Cisco IOS XE Release 3.6	The **interval** keyword value range changed. The new values are either 0 (default) or from 100 to 3,600,000 ms between successive MPLS echo requests.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Note It is recommended that you use the **mpls oam** global configuration command instead of this command.

Use the **ping mpls** command to validate, test, or troubleshoot IPv4 LDP LSPs, IPv4 Resource Reservation Protocol (RSVP) TE tunnels, and AToM VCs.

With the introduction of Cisco IOS-XE Release 3.6, the **interval** keyword value range changed from 0 to 3,600,000 ms to 0 or 100 to 3,600,000 ms between successive MPLS echo requests.

UDP Destination Address Usage

The destination address is a valid 127/8 address. You have the option to specify a single *x.y.z-address* or a range of numbers from 0.0.0 to *x.y.z* , where *x* , *y* , and *z* are numbers from 0 to 255 and correspond to the 127.*x.y.z* destination address.

The MPLS echo request destination address in the UDP packet is not used to forward the MPLS packet to the destination router. The label stack that is used to forward the echo request routes the MPLS packet to the destination router. The 127/8 address guarantees that the packets are routed to the local host (the default loopback address of the router processing the address) if the UDP packet destination address is used for forwarding.

In addition, the destination address is used to adjust load balancing when the destination address of the IP payload is used for load balancing.

Time-to-Live Usage

The time-to-live value indicates the maximum number of hops a packet should take to reach its destination. The value in the TTL field in a packet is decremented by 1 each time the packet travels through a router.

For MPLS LSP ping, the TTL is a value after which the packet is discarded and an MPLS echo reply is sent back to the originating router.

For MPLS multipath LSP traceroute, the TTL is a maximum time-to-live value and is used to discover the number of downstream hops to the destination router. MPLS LSP traceroute incrementally increases the TTL value in its MPLS echo requests (TTL = 1, 2, 3, 4, ...) to accomplish this.

Downstream Map TLVs

The presence of a downstream map in an echo request is interpreted by the responding transit (not egress) router to include downstream map information in the echo reply. Specify the **ttl** and **dsmap** keywords to cause TTL expiry during LSP ping to interrogate a transit router for downstream information.

Pseudowire Usage

The following keywords are not available with the **ping mpls pseudowire** command:

- **dsmap**
- **flags**
- **force-explicit-null**
- **output**
- **revision**
- **ttl**

The **ping mpls pseudowire** command is not supported when flow label (FAT) is enabled. If you enter the **ping mpls pseudowire** command when FAT is enabled the following message is displayed:

```
% Pseudowire Target Not Supported
```

Revision Keyword Usage

The **revision** keyword allows you to issue a **ping mpls ipv4**, **ping mpls pseudowire**, or **trace mpls traffic-eng** command based on the format of the TLV. The table below lists the revision option and usage guidelines for each option.

Table 7: Revision Options and Option Usage Guidelines

Revision Option	Option Usage Guidelines
1[1]	Not supported in Cisco IOS Release 12.4(11)T or later releases. Version 1 (draft-ietf-mpls-ping-03). For a device running Cisco IOS Release 12.0(27)S3 or a later release, you must use the **revision 1** keyword when you send LSP ping or LSP traceroute commands to devices running Cisco IOS Release 12.0(27)S1 or 12.0(27)S2.
2	Version 2 functionality was replaced by Version 3 functionality before an image was released.

Revision Option	Option Usage Guidelines
3	Version 3 (draft-ietf-mpls-ping-03). • For a device implementing Version 3 (Cisco IOS Release 12.0(27)S3 or a later release), you must use the **revision 1** keyword when you send the LSP **ping** or LSP **traceroute** command to a device implementing Version 1 (that is, either Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2). • A **ping mpls mpls pseudowire** command does not work with devices running Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2.
4	• Version 8 (draft-ietf-mpls-ping-08)--Applicable before Cisco IOS Release 12.4(11)T. All echo packet's TLVs are formatted as specified in Version 8. • RFC 4379 compliant--Applicable after Cisco IOS Release 12.4(11)T. All echo packet's TLVs are formatted as specified in RFC 4379.

[1] If you do not specify a revision keyword, the software uses the latest version.

With the introduction of Cisco IOS

Examples

The following example shows how to use the **ping mpls** command to test connectivity of an IPv4 LDP LSP:

```
Router# ping mpls ipv4 10.131.191.252/32 repeat 5 exp 5 verbose
Sending 5, 100-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/102/112 ms
```

The following example shows how to invoke the **ping mpls** command in the interactive mode to check MPLS LSP connectivity:

```
Router# ping
Protocol [ip]: mpls
Target IPv4, pseudowire or traffic-eng [ipv4]: ipv4
Target IPv4 address: 10.131.159.252
Target mask: 255.255.255.255
Repeat count [5]: 1
Datagram size [100]:
Timeout in seconds [2]:
Send interval in msec [0]:
Extended commands? [no]: yes
Destination address or destination start address: 127.0.0.1
```

```
Destination end address: 127.0.0.1
Destination address increment: 0.0.0.1
Source address:
EXP bits in mpls header [0]:
Pad TLV pattern [ABCD]:
Time To Live [255]:
Reply mode ( 2-ipv4 via udp, 3-ipv4 via udp with router alert) [2]:
Reply ip header DSCP bits [0]:
Verbose mode? [no]: yes
Sweep range of sizes? [no]:
Sending 1, 100-byte MPLS Echos to 10.131.159.252/32,
      timeout is 2 seconds, send interval is 0 msec:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
Destination address 127.0.0.1
!   10.131.159.245, return code 3
Destination address 127.0.0.1
!   10.131.159.245, return code 3
Destination address 127.0.0.1
!   10.131.159.245, return code 3
Success rate is 100 percent (3/3), round-trip min/avg/max = 40/48/52 ms
```

Note The “Destination end address” and “Destination address increment” prompts display only if you enter an address at the “Destination address or destination start address” prompt. Also, the “Sweep min size,” “Sweep max size,” and “Sweep interval” prompts display only if you enter “yes”at the “Sweep range of sizes? [no]” prompt.

The following example shows how to determine the destination address of an AToM VC:

```
Router# show mpls l2transport vc
Local intf     Local circuit           Dest address    VC ID      Status
-------------  ----------------------- --------------- ---------- ----------
Et2/0          Ethernet                10.131.191.252
 333        UP
Router# show mpls l2transport vc detail
Local interface: Et2/0 up, line protocol up, Ethernet up
  Destination address: 10.131.191.252, VC ID: 333, VC status: up
    Preferred path: not configured
    Default path: active
    Tunnel label: imp-null, next hop 10.131.159.246
    Output interface: Et1/0, imposed label stack {16}
  Create time: 06:46:08, last status change time: 06:45:51
  Signaling protocol: LDP, peer 10.131.191.252:0 up
    MPLS VC labels: local 16, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

This **ping mpls pseudowire** command can be used to test the connectivity of the AToM VC 333 discovered in the preceding **show** command:

```
Router# ping mpls pseudowire 10.131.191.252 333 repeat 200 size 1400
Sending 1, 100-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 92/92/92 ms
```

This ping is particularly useful because the VC might be up and the LDP session between the PE and its downstream neighbor might also be up, but LDP might be configured somewhere in between. In such cases, you can use an LSP ping to verify that the LSP is actually up.

A related point concerns the situation when a pseudowire has been configured to use a specific TE tunnel. For example:

```
Router# show running-config interface ethernet 2/0
Building configuration...
Current configuration : 129 bytes
!
interface Ethernet2/0
 no ip address
 no ip directed-broadcast
 no cdp enable
xconnect 10.131.191.252 333 pw-class test1
end
Router# show running-config
| begin pseudowire
pseudowire-class test1
 encapsulation mpls
 preferred-path interface Tunnel0
```

In such cases, you can use an LSP ping to verify the connectivity of the LSP that a certain pseudowire is taking, be it LDP based or a TE tunnel:

```
Router#

ping mpls pseudowire 10.131.191.252 333 repeat 200 size 1400
Sending 200, 1400-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (200/200), round-trip min/avg/max = 72/85/112 ms
```

You can also use the **ping mpls** command to verify the maximum packet size that can be successfully sent. The following command uses a packet size of 1500 bytes:

```
Router# ping mpls pseudowire 10.131.191.252 333 repeat 5 size 1500
Sending 5, 1500-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
QQQQQ
Success rate is 0 percent (0/5)
```

The Qs indicate that the packets are not sent.

The following command uses a packet size of 1476 bytes:

```
Router# ping mpls pseudowire 10.131.191.252 333 repeat 5 size 1476
Sending 5, 1476-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/83/92 ms
```

The following example shows how to test the connectivity of an MPLS TE tunnel:

```
Router# ping mpls traffic-eng tunnel tun3 repeat 5 verbose
Sending 5, 100-byte MPLS Echos to Tunnel3,
     timeout is 2 seconds, send interval is 0 msec:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/37/40 ms
```

The MPLS LSP ping feature is useful if you want to verify TE tunnels before actually mapping traffic onto them.

The following example shows a **ping mpls** command that specifies segment 2 of a multisegment pseudowire:

```
Router# ping mpls pseudowire 10.131.191.252 333 segment 2
```

Related Commands

Command	Description
mpls oam	Customizes the default behavior of echo packets.
trace mpls	Discovers MPLS LSP routes that packets will actually take when traveling to their destinations.

ping mpls mldp

To check connectivity, isolate failure point, thus providing the Multiprotocol Label Switching (MPLS) Operation, Administration, and Maintenance (OAM) solution, use the **ping mpls mldp** command in privileged EXEC mode.

ping mpls mldp {**mp2mp** | **p2mp**} *root-address* {**ipv4** *source-address group-address* | **ipv6** *source-address group-address* | **mdt** *vpn-id mdt-number* | **vpnv4** *vpn-distinguisher source-address group-address* | **vpnv6** *vpn-distinguisher source-address group-address* | **hex** *opaque-type hex-string*} [{**ddmap** [{**hashkey** {**none** | **ipv4 bitmap** *bitmap-size*}}]}] [{**destination** *address-start address-end* [{*increment increment-mask*}]}] [{**exp** *exp-bits*}] **flags** {**fec** | [{**flags ttl**}] | **ttl** | [{**flags fec**}]} [{**force-explicit-null** }] [{**interval** *delay*}] [{**jitter** *jitter-value*}] [{**output interface** *tx-interface* [{**nexthop** *ip-address*}]}] [{**pad** *pattern*}] [{**repeat** *count*}] [{**reply** {**dscp** *dscp-value* | **mode** | {**ipv4** | **router-alert**}}}] [{**responder-id** *id-address*}] [{**revision** *tlv-revision-number*}] [{**size** *packet-size*}] [{**source** *source-address*}] [{**sweep** *sweep-min-value sweep-max-value sweep-interval*}] [{**timeout** *seconds*}] [{**ttl** *time-to-live*}] [{**verbose**}]

Syntax Description

mp2mp	Checks the connectivity of a multipoint-to-multipoint Multicast Label Distribution Protocol (MLDP) tree from any LSR to egress LSRs (leaves).
p2mp	Checks the connectivity of a point-to-multipoint MLDP tree from ingress LSR (root) to egress LSRs (leaves).
root-address	Specifies MLDP tree root address.
ipv4	Defines IPv4 opaque encoding.
source-address	Specifies the IPv4 source address.
group-address	Specifies the IPv4 group address.
ipv6	Defines IPv6 opaque encoding.
source-address	Specifies the IPv6 source address.
group-address	Specifies the IPv6 group address.
mdt	Defines VPN ID opaque encoding
vpn-id	Specifies the VPN-id. The range of 3-byte OUI is from 0 to 16777215.
mdt-number	Specifies the MDT number. The range is from 0 to 4294967295.
vpnv4	Defines the VPNv4 opaque encoding.
vpn-distinguisher	Specifies the autonomous system number or IP address of VPNv4 route distinguisher.

source-address	Specifies the IPv4 source address.
group-address	Specifies the IPv4 group address.
vpnv6	Defines VPNv6 opaque encoding.
vpn-distinguisher	Specifies the autonomous system number or IP address of VPNv6 route distinguisher.
source-address	Specifies the IPv6 source address.
group-address	Specifies the IPv6 group address.
hex	Allows MLDP forwarding equivalence class (FEC) to be constructed using the type value and the hexadecimal string.
opaque-type	Specifies the type value in the opaque value element of MLDP FEC.
hex-string	Specifies the value in the opaque value element of MLDP FEC.
ddmap	(Optional) Indicates that a downstream detailed mapping TLV (ddmap) must be included in the LSP echo request.
hashkey {**none** | **ipv4 bitmap** *bitmap-size*}	(Optional) Allows you to control the hash key and multipath settings. Valid values are: **none** --There is no multipath (type 0). **ipv4 bitmap** *bitmap-size*--Size of the IPv4 addresses (type 8) bitmap.
destination	(Optional) Specifies a network 127 address.
address-start	(Optional) Specifies the beginning network 127 address.
address-end	(Optional) Specifies an ending network 127 address.
increment	(Optional) Specifies the number by which to increment the destination local host address.
increment-mask	(Optional) Specifies the mask by which to increment the destination local host address.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. The range is 0 to 7. Default is 0.

flags	(Optional) Allows FEC checking on the transit device. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Target FEC stack validation is always done at the egress device. Be sure to use this keyword with the **ttl** keyword.
fec	(Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit devices.
ttl	(Optional) Sets TTL expired flag in the echo request to indicate responder node to respond if echo request was received through TTL expiry.
force-explicit-null	(Optional) Forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.
interval *delay*	(Optional) Specifies the time, in milliseconds (ms), between successive MPLS echo requests. This parameter allows you to pace the transmission of packets so that the receiving device does not drop packets. Default is 0.
jitter *jitter-value*	(Optional) Configures the jitter value, in milliseconds, that is used in the jitter type, length, values (TLVs) and sent as part of the echo request packets. The range is from 1 to 2147483647. The default is 200.
output interface *tx-interface*	(Optional) Specifies the output interface for echo requests.
nexthop *ip-address*	(Optional) Causes packets to go through the specified next-hop address.
pad *pattern*	(Optional) The pad TLV is used to fill the datagram so that the MPLS echo request (User Datagram Protocol [UDP] packet with a label stack) is the specified size. The default is 0xABCD.
repeat *count*	(Optional) Specifies the number of times to resend the same packet. The range is 1 to 2147483647. The default is 1. If you do not enter the **repeat** keyword, the software resends the same packet five times.

reply dscp *dscp-value*	(Optional) Provides the capability to request a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value. The echo reply is returned with the IP header type of service (ToS) byte set to the value specified in the **reply dscp** command.
reply mode {**ipv4** | **router-alert**}	(Optional) Specifies the reply mode for the echo request packet. **ipv4** --Reply with an IPv4 UDP packet (default). **router-alert** --Reply with an IPv4 UDP packet with router alert.
responder-id *ip-address*	(Optional) Adds responder identifier into corresponding echo request
revision *tlv-revision-number*	(Optional) Cisco TLV revision number.
size *packet-size*	(Optional) Specifies the size of the packet with the label stack imposed. Packet size is the number of bytes in each ping. The range is 72 to 18024. The default is 100.
source *source-address*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
sweep	(Optional) Specifies sweep range of packet size.
sweep-min-val	(Optional) Specifies the minimum or start size for an MPLS echo packet. The range is from 72 to 18024. The default is 100.
sweep-max-val	(Optional) Specifies the maximum or end size for an MPLS echo packet. The range is from 100 to 18024.
sweep-interval	(Optional) Specifies the sweep interval. The range is from 1 to 8993.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds for an MPLS request packet. The range is 0 to 3600. The default is 2.
ttl *time-to-live*	(Optional) Specifies a time-to-live (TTL) value to be used in the MPLS labels. The default is 225 seconds.
verbose	(Optional) Displays the MPLS echo reply sender address of the packet and displays return codes.

Command Default

You cannot check MPLS LSP connectivity.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(3)S	This command was introduced.

Usage Guidelines

Note It is recommended that you use the **mpls oam** global configuration command instead of this command.

Use the **ping mpls mldp** command to check connectivity and isolate failure point, thus providing the Multiprotocol Label Switching (MPLS) Operation, Administration, and Maintenance (OAM) solution.

Destination IP Address Usage

The destination IP address is a localhost 127/8 address. You can specify a single 127/8 IP address or a range of IP addresses between 127.0.0.0 and 127.255.255.255.

Initiator LSR-imposed label stack is used to forward an echo request packet to target(s). Localhost destination IP address used in an MPLS echo request packet is to ensure the packet is never IP routed even if all labels are mistakenly popped along the LSP.

In addition, the destination IP address is used to adjust load balancing when the destination IP address of the IP payload is used for load balancing.

Time-to-Live Usage

The time-to-live value indicates the maximum number of hops a packet should take to reach its destination. The value in the TTL field in a packet is decremented by 1 each time the packet travels through a device.

For MPLS MLDP ping, the TTL is a value after which the packet is discarded and an MPLS echo reply is sent back to the originating device.

Examples

The following example shows how to check connectivity for point-to-multipoint by using the **ping mpls mldp p2mp** command:

```
Device# ping mpls mldp p2mp 10.0.0.5 vpnv4 100:100 38.0.0.8 232.1.1.2
verbose size 200 interval 100 exp 4 timeout 2 repeat 3 jitter 140 ddmap ttl 1

p2mp Root node addr 10.0.0.5
Opaque type VPNv4, source 38.0.0.8, group 232.1.1.2
Sending 3, 200-byte MPLS Echos to Target FEC Stack TLV descriptor,
    timeout is 2.1 seconds, send interval is 100 msec, jitter value is 140 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
```

```
Request #1
L    size 200, reply addr 30.0.0.2, return code 8
Echo Reply received from 30.0.0.2
  DDMAP 0, DS Router Addr 33.0.0.3, DS Intf Addr 33.0.0.3
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

  DDMAP 1, DS Router Addr 34.0.0.6, DS Intf Addr 34.0.0.6
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

 Received 0 replies

Request #2
L    size 200, reply addr 30.0.0.2, return code 8
Echo Reply received from 30.0.0.2
  DDMAP 0, DS Router Addr 33.0.0.3, DS Intf Addr 33.0.0.3
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

  DDMAP 1, DS Router Addr 34.0.0.6, DS Intf Addr 34.0.0.6
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

 Received 0 replies

Request #3
L    size 200, reply addr 30.0.0.2, return code 8
Echo Reply received from 30.0.0.2
  DDMAP 0, DS Router Addr 33.0.0.3, DS Intf Addr 33.0.0.3
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

  DDMAP 1, DS Router Addr 34.0.0.6, DS Intf Addr 34.0.0.6
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

 Received 0 replies

 Total Time Elapsed 6120 ms
```

The following example shows how to check connectivity for multipoint-to-multipoint by using the **ping mpls mldp mp2mp** command:

```
Device#  ping mpls mldp mp2mp 10.0.0.1 mdt 100:100 0
verbose size 200 interval 100 exp 4 timeout 2 repeat 3 jitter 230

mp2mp Root node addr 10.0.0.1
Opaque type MDT, oui:index 0x100:0100, mdtnum 0
Sending 3, 200-byte MPLS Echos to Target FEC Stack TLV descriptor,
    timeout is 2.2 seconds, send interval is 100 msec, jitter value is 230 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

Request #1
!    size 200, reply addr 35.0.0.4, return code 3
!    size 200, reply addr 34.0.0.6, return code 3
!    size 200, reply addr 36.0.0.7, return code 3

Round-trip min/avg/max = 52/92/118 ms
 Received 3 replies
```

```
Request #2
!    size 200, reply addr 34.0.0.6, return code 3
!    size 200, reply addr 36.0.0.7, return code 3
!    size 200, reply addr 35.0.0.4, return code 3

Round-trip min/avg/max = 118/158/196 ms
 Received 3 replies

Request #3
!    size 200, reply addr 36.0.0.7, return code 3
!    size 200, reply addr 34.0.0.6, return code 3
!    size 200, reply addr 35.0.0.4, return code 3

Round-trip min/avg/max = 80/116/155 ms
 Received 3 replies

 Total Time Elapsed 6409 ms
```

Related Commands

Command	Description
mpls oam	Customizes the default behavior of echo packets.
ping mpls	Checks Multiprotocol Label Switching (MPLS) label switched path (LSP) connectivity.

ping mpls tp

To check Multiprotocol Label Switching (MPLS) transport protocol (TP) label switched path (LSP) connectivity, use the **ping mpls tp** command in privileged EXEC mode.

ping mpls tp tunnel-tp *num* **lsp** {**working** | **protect** | **active**} [**ddmap**[{**hashkey ipv4 bitmap** *bitmap-size* | **none**}]] [**dsmap** [{**hashkey ipv4 bitmap** *bitmap-size* | **none**}]] [**destination** *ip-addr*] [**exp** *num*] [**flags fec**] [**interval** *num*] [**pad** *num*] [**repeat** *num*] {[**reply desc** *num*] | [**mode control channel**]} [**size** *num*] [**source** *ip-addr*] [**sweep** *num num num*] [**timeout** *num*] [**ttl** *num*] [**verbose**]

Syntax Description

tunnel-tp *num*	Sepcifies the MPLS-TP tunnel number.
lsp {**working** | **protect** | **active**}	Specifies the type of MPLS-TP label switched path (LSP) on which to send echo request packets.
ddmap [**hashkey ipv4 bitmap** *bitmap-size* | **none**	(Optional) Interrogates a transit router for downstream detailed mapping (DDMAP) information. Allows you to control the hash key and multipath settings.Valid values are: **none** —There is no multipath (type 0). **hashkey ipv4 bitmap** *bitmap-size* —Size of the IPv4 addresses (type 8) bitmap. If you enter the **none** keyword, multipath LSP traceroute acts like enhanced LSP traceroute; that is, it uses multipath LSP traceroute retry logic and consistency checking.
dsmap [**hashkey ipv4 bitmap** *bitmap-size* | **none**	(Optional) Interrogates a transit router for downstream mapping (DSMAP) information. Allows you to control the hash key and multipath settings. Valid values are: **none** —There is no multipath (type 0). **hashkey ipv4 bitmap** *bitmap-size* —Size of the IPv4 addresses (type 8) bitmap. If you enter the **none** keyword, multipath LSP traceroute acts like enhanced LSP traceroute; that is, it uses multipath LSP traceroute retry logic and consistency checking.
destination *ip-addr*	(Optional) Specifies a network 127 address.
exp *num*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. Valid values are from 0 to 7. Default is 0.
flags fec	(Optional) Allows Forward Equivalence Class (FEC) checking on the transit router. A downstream map type, length, variable (TLV) containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Target FEC stack validation is always done at the egress router. Be sure to use this keyword in conjunction with the **ttl**keyword.

interval *num*	(Optional) Specifies the time, in milliseconds (ms), between successive MPLS echo requests. This parameter allows you to pace the transmission of packets so that the receiving router does not drop packets. Default is 0.
pad *num*	(Optional) The pad TLV is used to fill the datagram so that the MPLS echo request (User Datagram Protocol [UDP] packet with a label stack) is the specified size. The default is 0xABCD.
repeat *num*	(Optional) Specifies the repeat count. Range: 1 to 2147483647.
reply dscp *num* | **mode control channel**	(Optional) Provides the capability to request a specific quality of service (QoS) in an echo reply by providing a differentiated services code point (DSCP) value. The echo reply is returned with the IP header type of service (ToS) byte set to the value specified in the **reply dscp** command.
size *num*	Specifies the packet size.
source *ip-addr*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
sweep *num num num*	(Optional) Enables you to send a number of packets of different sizes, ranging from a start size to an end size. This parameter is similar to the Internet Control Message Protocol (ICMP) ping sweep parameter.
timeout *num*	(Optional) Specifies the timeout interval in seconds for an MPLS request packet. The range is from 0 to 3600. The default is 2 seconds.
ttl *num*	(Optional) Specifies a time-to-live (TTL) value. The default is 225 seconds.
verbose	(Optional) Enables verbose output mode.

Command Default

Connectivity is not checked.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Usage Guidelines

Use the **ping mpls tp**command to validate, test, or troubleshoot MPLS TP LSPs.

Note The **ping mpls tp** command does not support interactive mode.

You can use ping and trace in an MPLS-TP network without IP addressing. However, no IP addresses are displayed in the output.

The following rules determine the source IP address:

1. Use the IP address of the TP interface.
2. Use the global router ID.
3. Use the router ID: A.B.C.D local node ID in IPv4 address format. This is not an IP address; however, it is better to use a value rather than leave it as 0.0.0.0 and risk the packet being deemed invalid and dropped.

Examples

The following example checks connectivity of an MPLS-TP LSP:

```
Router# ping mpls tp tunnel-tp 1 repeat 1 ttl 2
Sending 1, 100-byte MPLS Echos to Tunnel-tp1,
     timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 156/156/156 ms
```

Related Commands

Command	Description
trace mpls tp	Displays the MPLS LSP routes that packets take to their destinations.

ping vrf

To test a connection in the context of a specific VPN connection, use the **ping vrf** command in user EXEC or privileged EXEC mode.

ping vrf *vrf-name* [**tag**] [*connection*] *target-address* [*connection-options*]

Syntax Description

vrf-name	The name of the VPN (VRF context).
tag	(Optional) Specifies a tag encapsulated IP (tagIP) ping.
connection	(Optional) Connection options include **atm**, **clns**, **decnet**, **ip**, **ipv6**, **ipx**, **sna**, or **srb**. The default is **ip**.
target-address	The destination ID for the ping operation. Usually, this is the IPv4 address of the host. For example, the target for an IPv4 ping in a VRF context would be the IPv4 address or domain name of the target host. The target for an IPv6 ping in a VRF context would be the IPv6 prefix or domain name of the target host. • If the target address is not specified, the CLI will enter the interactive dialog for ping.
connection-options	(Optional) Each connection type may have its own set of connection options. For example, connection options for IPv4 are **source**, **df-bit**, and **timeout**. See the appropriate **ping** command documentation for details.

Command Default

The default connection type for ping is IPv4.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.1(12c)E, 12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.

Usage Guidelines

A VPN routing and forwarding (VRF) instance is used to identify a VPN. To check if a configured VRF is working, you can use the **ping vrf** command.

When attempting to ping from a provider edge (PE) router to a customer edge (CE) router, or from a PE router to PE router, the standard **ping** command will not usually work. The **ping vrf** command allows you to ping the IP addresses of LAN interfaces on CE routers.

If you are on a PE router, be sure to indicate the specific VRF (VPN) name, as shown in the "Examples" section.

If all required information is not provided at the command line, the system will enter the interactive dialog (extended mode) for ping.

Examples

In the following example, the target host in the domain 209.165.201.1 is pinged (using IP/ICMP) in the context of the "CustomerA" VPN connection.

```
Router# ping vrf CustomerA 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 176/264/576 ms
```

Pressing the Enter key before providing all of the required options will begin the interactive dialog for ping. In the following example, the interactive dialog is started after the "ip" protocol is specified, but no address is given:

```
Router# ping vrf CustomerB ip

Target IP address: 209.165.200.225
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record

Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
 .
 .
 .
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The following example shows the various options for IP in the **ping vrf** command:

```
Router# show parser dump exec | include ping vrf

1 ping vrf <string>
1 ping vrf <string> ip <string>
```

```
1 ping vrf <string> ip (interactive)
1 ping vrf <string> ip <string>
1 ping vrf <string> ip <string> source <address>
1 ping vrf <string> ip <string> source <interface>
1 ping vrf <string> ip <string> repeat <1-2147483647>
1 ping vrf <string> ip <string> size Number
1 ping vrf <string> ip <string> df-bit
1 ping vrf <string> ip <string> validate
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> ip <string> verbose
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> tag
1 ping vrf <string> atm
1 ping vrf <string> ipv6
1 ping vrf <string> appletalk
1 ping vrf <string> decnet
1 ping vrf <string> clns
1 ping vrf <string> ipx
1 ping vrf <string> sna
1 ping vrf <string> srb
```

Cisco CMTS Routers: Example

The following example shows how to verify the matching and marking configuration in an MPLS network:

```
Router# ping vrf vrfa 1.3.99.98

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.3.99.98, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/20 ms
```

Related Commands

Command	Description
ping	Diagnoses basic network connectivity to a specific host.
ping atm interface atm	Tests the connectivity of a specific PVC.
ping ip	Tests the connection to a remote host on the network using IPv4.
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping sna	Tests network integrity and timing characteristics over an SNA Switching network.

platform mpls load-balance ingress-port

To improve ingress port-based P router load balancing performance between two Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) line cards, use the **platform mpls load-balance ingress-port** command in global configuration mode. Entering this command will enable this feature. To disable this feature, use the **no** form of the command.

platform mpls load-balance ingress-port
no platform mpls load-balance ingress-port

Syntax Description

This command has no arguments or keywords.

Command Default

Load balancing performance improvements are not enabled .

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was introduced.
15.0M	This command was introduced.

Usage Guidelines

The H-VPLS with Port-Channel Core Interface feature provides support for VPLS to port-channels. You can use this feature to:

- Configure VPLS on the port channel interfaces of the ES+ line card using a load balancing mechanism.
- Match the capabilities and requirements of the VPLS in a single link. Due to multiple links in a link aggregation (LAG), the packets of a particular flow are always transmitted only to one link.
- Configure VPLS with port-channel interfaces as the core facing interface, where the member links of the port-channel are from a ES40 line card. The load-balancing is per-flow based, that is, traffic of a VPLS VC will be load-balanced across member links based on the flow.

Examples

This example shows how to enable improved load-balancing performance on a Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) line card:

```
Router(config)# platform mpls load-balance ingress-port
```

Related Commands

Command	Description
show mpls	Displays information for a line card.

platform mpls mtu-enable

To enable MPLS MTU on the router, use the **platform mpls mtu-enable** command in global configuration mode. To disable this feature, use the **no** form of the command.

platform mpls mtu-enable
no platform mplsmtu-enable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default .

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.10.2	This command was introduced on the Cisco ASR 900 Series Router.

Usage Guidelines

This command configures MPLS MTU on the router.

Note IP MTU does *not* affect MPLS MTU value.

Note It is *not* recommended to toggle the command as in-consistent MTU values may be displayed.

After configuring or un-configuring the command, it is recommended to re-configure all MTU values on all the interfaces.

Examples

This example shows how to enable MPLS MTU on the Cisco ASR 900 Series Router:

```
Router(config)# platform mpls mtu-enable
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# mpls mtu 700
```

Related Commands

Command	Description
show platform hardware pp active feature mpls mtu-table	Displays information MPLS MTU information configured on the router.

policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map**command in global configuration mode. To delete a policy map, use the **no** form of this command.

Supported Platforms Other Than Cisco 10000 and Cisco 7600 Series Routers
policy-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-policy*}] *policy-map-name*
no policy-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-policy*}] *policy-map-name*

Cisco 10000 Series Router
policy-map [**type** {**control** | **service**}] *policy-map-name*
no policy-map [**type** {**control** | **service**}] *policy-map-name*

Cisco CMTS and 7600 Series Router
policy-map [**type** {**class-routing ipv4 unicast** *unicast-name* | **control** *control-name* | **service** *service-name*}] *policy-map-name*
no policy-map [**type** {**class-routing ipv4 unicast** *unicast-name* | **control** *control-name* | **service** *service-name*}] *policy-map-name*

Syntax Description

type	(Optional) Specifies the policy-map type.
stack	(Optional) Determines the exact pattern to look for in the protocol stack of interest.
access-control	(Optional) Enables the policy map for the flexible packet matching feature.
port-filter	(Optional) Enables the policy map for the port-filter feature.
queue-threshold	(Optional) Enables the policy map for the queue-threshold feature.
logging	(Optional) Enables the policy map for the control-plane packet logging feature.
log-policy	(Optional) Type of log policy for control-plane logging.
policy-map-name	Name of the policy map.
control	(Optional) Creates a control policy map.
control-name	Name of the control policy map.
service	(Optional) Creates a service policy map.
service-name	Name of the policy-map service.
class-routing	Configures the class-routing policy map.
ipv4	Configures the class-routing IPv4 policy map.
unicast	Configures the class-routing IPv4 unicast policy map.

unicast-name	Unicast policy-map name.

Command Default

The policy map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(4)T	This command was modified. The **type** and**access-control**keywords were added to support flexible packet matching. The **port-filter** and **queue-threshold** keywords were added to support control-plane protection.
12.4(6)T	This command was modified. The **logging** keyword was added to support control-plane packet logging.
12.2(31)SB	This command was modified. The **control** and **service**keywords were added to support the Cisco 10000 series router.
12.2(18)ZY	This command was modified. • The **type** and**access-control**keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine. • The command was modified to enhance the Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/PISA engine.
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. Support for this command was implemented on Cisco 7600 series routers.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 series routers.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.

Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added, or modified before you configure policies for classes whose match criteria are defined in a class map. The **policy-map** command enters policy-map configuration mode, in which you can configure or modify the class policies for a policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. Use the **class-map** and **match** commands to configure match criteria for a class. Because you can configure a maximum of 64 class maps, a policy map cannot contain more than 64 class policies, except as noted for quality of service (QoS) class maps on Cisco 7600 systems.

Note For QoS class maps on Cisco 7600 series routers, the limits are 1024 class maps and 256 classes in a policy map.

A policy map containing ATM set cell loss priority (CLP) bit QoS cannot be attached to PPP over X (PPPoX) sessions. The policy map is accepted only if you do not specify the **set atm-clp** command.

A single policy map can be attached to more than one interface concurrently. Except as noted, when you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by class policies that make up the policy map. In such cases, if the policy map is already attached to other interfaces, the map is removed from those interfaces.

Note This limitation does not apply on Cisco 7600 series routers that have session initiation protocol (SIP)-400 access-facing line cards.

Whenever you modify a class policy in an attached policy map, class-based weighted fair queuing (CBWFQ) is notified and the new classes are installed as part of the policy map in the CBWFQ system.

Note Policy-map installation via subscriber-profile is not supported. If you configure an unsupported policy map and there are a large number of sessions, an equally large number of messages print on the console. For example, if there are 32,000 sessions, then 32,000 messages print on the console at 9,600 baud.

Class Queues (Cisco 10000 Series Routers Only)

The Performance Routing Engine (PRE)2 allows you to configure 31 class queues in a policy map.

In a policy map, the PRE3 allows you to configure one priority level 1 queue, one priority level 2 queue, 12 class queues, and one default queue.

Control Policies (Cisco 10000 Series Routers Only)

Control policies define the actions that your system will take in response to the specified events and conditions.

A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions are executed.

There are three steps involved in defining a control policy:

1. Using the **class-map type control** command, create one or more control class maps.
2. Using the **policy-map type control** command, create a control policy map.

A control policy map contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Actions are numbered and executed sequentially.

1. Using the **service-policy type control** command, apply the control policy map to a context.

Service Policies (Cisco 10000 Series Routers Only)

Service policy maps and service profiles contain a collection of traffic policies and other functions. Traffic policies determine which function is applied to which session traffic. A service policy map or service profile may also contain a network-forwarding policy, which is a specific type of traffic policy that determines how session data packets will be forwarded to the network.

Policy Map Restrictions (Catalyst 6500 Series Switches Only)

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. This release and platform has the following restrictions for using policy maps and **match** commands:

- You cannot modify an existing policy map if the policy map is attached to an interface. To modify the policy map, remove the policy map from the interface by using the **no** form of the **service-policy** command.
- Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed. However, the following restrictions apply:
  - A single traffic class can be configured to match a maximum of 8 protocols or applications.
  - Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

Examples

The following example shows how to create a policy map called “policy1” and configure two class policies included in that policy map. The class policy called “class1” specifies a policy for traffic that matches access control list (ACL) 136. The second class is the default class to which packets that do not satisfy the configured match criteria are directed.

```
! The following commands create class-map class1 and define its match criteria:
class-map class1
 match access-group 136
! The following commands create the policy map, which is defined to contain policy
! specification for class1 and the default class:
policy-map policy1
class class1
 bandwidth 2000
 queue-limit 40
class class-default
 fair-queue 16
 queue-limit 20
```

The following example shows how to create a policy map called “policy9” and configure three class policies to belong to that map. Of these classes, two specify the policy for classes with class maps that specify match criteria based on either a numbered ACL or an interface name, and one specifies a policy for the default class called “class-default” to which packets that do not satisfy the configured match criteria are directed.

```
policy-map policy9

class acl136
 bandwidth 2000
 queue-limit 40

class ethernet101
 bandwidth 3000
```

```
 random-detect exponential-weighting-constant 10
class class-default
 fair-queue 10
 queue-limit 20
```

The following is an example of a modular QoS command-line interface (MQC) policy map configured to initiate the QoS service at the start of a session.

```
Router> enable
Router# configure terminal
Router(config)# policy-map type control TEST
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1
 service-policy type service name QoS_Service
Router(config-control-policymap-class-control)# end
```

Examples for Cisco 10000 Series Routers Only

The following example shows the configuration of a control policy map named “rule4”. Control policy map rule4 contains one policy rule, which is the association of the control class named “class3” with the action to authorize subscribers using the network access server (NAS) port ID. The **service-policy type control** command is used to apply the control policy map globally.

```
class-map type control match-all class3
 match vlan 400
 match access-type pppoe
 match domain cisco.com
 available nas-port-id
!
policy-map type control rule4
 class type control class3
  authorize nas-port-id
!
service-policy type control rule4
```

The following example shows the configuration of a service policy map named “redirect-profile”:

```
policy-map type service redirect-profile
 class type traffic CLASS-ALL
  redirect to group redirect-sg
```

Examples for the Cisco CMTS Router

The following example shows how to define a policy map for the 802.1p domain:

```
enable
configure terminal
 policy-map cos7
  class cos7
  set cos 2
  end
```

The following example shows how to define a policy map for the MPLS domain:

```
enable
configure terminal
 policy-map exp7
  class exp7
```

```
set mpls experimental topmost 2
end
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and its default class before you configure its policy.
class class-default	Specifies the default class whose bandwidth is to be configured or modified.
class-map	Creates a class map to be used for matching packets to a specified class.
fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
queue-limit	Specifies or modifies the maximum number of packets that the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detectservice-policy precedence	Configures WRED and DWRED parameters for a particular IP precedence.
service-policy	Attaches a policy map to an input interface or VC or an output interface or VC to be used as the service policy for that interface or VC.
set atm-clp precedence	Sets the ATM CLP bit when a policy map is configured.

preferred-path

To specify the path (a Multiprotocol Label Switching [MPLS] Traffic engineering [TE] tunnel or destination IP address and Domain Name Server [DNS] name) that traffic uses, use the **preferred-path** command in the appropriate configuration mode. To remove path selection, use the **no** form of this command.

preferred-path {[{**interface**}] **tunnel** *tunnel-number* | **peer** *host-ip-address*} [**disable-fallback**]
no preferred-path {**interface tunnel** *tunnel-number* | **peer** *host-ip-address*} [**disable-fallback**]

Syntax Description

interface	Specifies the preferred path using an output interface.
tunnel	Specifies an MPLS TE tunnel interface that is the core-facing output interface.
tunnel-number	The tunnel interface number.
peer	Specifies a destination IP address or DNS name configured on the peer provider edge (PE) router, which is reachable through a label switched path (LSP).
host-ip-address	Peer host name or IP address.
disable-fallback	(Optional) Disables the router from using the default path when the preferred path is unreachable.

Command Default

Path selection is not specified.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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.
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.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

The following guidelines provide more information about using this command:

- The destination IP address can be different from the peer router ID used in MPLS Label Distribution Protocol (LDP). For example, a peer PE router can have multiple loopback IP addresses, which can be reached by different paths, such as a TE tunnel, static IP route, or Interior Gateway Protocol (IGP) route.
- This command is available only if the pseudowire encapsulation type is MPLS.
- Tunnel selection is enabled when you exit from pseudowire configuration mode.
- The selected path should be an LSP destined to the peer PE router.
- The selected tunnel must be an MPLS traffic engineering tunnel.
- If you select a tunnel, the tunnel tailend must be on the remote PE router.
- If you specify an IP address, that address must be the IP address of the loopback interface on the remote PE. The address must have a /32 mask.

Examples

The following example shows how to create a pseudowire class and specifies tunnel 1 as the preferred path:

```
Device(config)# pseudowire-class pw1
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# preferred-path interface tunnel 1 disable-fallback
```

The following example shows how to specify tunnel 1 as the preferred path from interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# preferred-path interface tunnel 1 disable-fallback
```

The following example shows how to specify tunnel 1 as the preferred path from tunnel configuration mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# preferred-path interface tunnel 1
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
show l2vpn atom vc	Displays information about AToM VCs that have been enabled to route Layer 2 VPN packets on a device.
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a device.

priority (LSP Attributes)

To specify the label switched path (LSP) priority in an LSP attribute list, use the **priority** command in LSP Attributes configuration mode. To remove the specified priority, use the **no** form of this command.

priority *setup-priority* [*hold-priority*]
no priority

Syntax Description

setup-priority	Priority used when signaling an LSP to determine which existing LSPs can be preempted. The range is 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.
hold-priority	(Optional) Priority associated with an LSP to determine if it should be preempted by other LSPs that are being signaled. The range is 0 to 7, where a lower number indicates a higher priority.

Command Default

No priority is set in the attribute list.

Command Modes

LSP Attributes configuration (config-lsp-attr)

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.

Usage Guidelines

Use this command to configure setup and hold priority for an LSP in an LSP attribute list. Setup priority and hold priority are typically configured to be equal, and setup priority cannot be better (numerically smaller) than the hold priority.

To associate the LSP priority attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to set the LSP hold and setup property to 0 in an LSP attribute list identified by the string hipriority:

```
configure terminal
!
mpls traffic-eng lsp attributes hipriority
 priority 0 0
 exit
end
```

Related Commands

Command	Description
mpls traffic-end lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

protection (LSP Attributes)

To configure failure protection on the label switched path (LSP) in an LSP attribute list, use the **protection** command in LSP Attributes configuration mode. To disable failure protection, use the **no** form of this command.

protection [**fast reroute** [**bw-protect**]]
no protection

Syntax Description

fast-reroute	Enables an LSP to use an established backup LSP in the event of a link failure.
bw-protect	Enables bandwidth protection.

Command Default

Failure protection is not enabled for the LSP in the LSP attribute list.

Command Modes

LSP Attributes configuration (config-lsp-attr)

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.

Usage Guidelines

Use this command to set up LSP failure protection in an LSP attribute list.

To associate the LSP failure protection attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to enable failure protection on an LSP in an LSP attribute list:

```
configure terminal
!
mpls traffic-eng lsp attributes protect
 protection fast-reroute
 exit
end
```

Related Commands

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

protection local-prefixes

To enable provider edge (PE)-to-customer edge (CE) link protection by preserving the local label (due to a link failure that caused Border Gateway Protocol (BGP) to begin reconverging), use the **protection local-prefixed** in VRF configuration or in VRF address family configuration mode. To disable this form of link protection, use the **no** form of this command.

protection local-prefixes
no protection local-prefixes

Syntax Description

This command has no arguments or keywords.

Command Default

This protection is disabled by default.

Command Modes

VRF configuration (config-vrf)
VRF address family configuration (config-vrf-af)

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.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS Release 15.0(1)S	This command was modified. Supported was added for PE-CE link protection for IPv6 and this command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

Each Virtual Routing and Forwarding (VRF) that provides protection or a backup path must have a unique route distinguisher (RD) to ensure route reflectors advertise all available paths. Use the **rd** command to specify a route distinguisher for the VRF if none has been created previously.

If your Cisco IOS version includes support for IPv6 and IPv4, use the global configuration **vrf definition** and **rd** commands followed by the **address-family ipv6** or **address-family ipv4** command before you use the **protection local-prefixes**command.

If your Cisco IOS version supports only IPv4, use the global configuration **ip vrf** command before you enter the **rd** and **protection local-prefixes** commands.

If VRF-lite has already been enabled, local protection will not take place. This is true even if entering the **protection local-prefixes** command does not trigger an error message.

Local link protection will only work properly if the failure is quickly detected and an alternate, backup route already exists. Therefore, in addition to the **protection local-prefixes** command, the use of Bidirectional Forwarding Detection (BFD) and topology-specific routing protocols are both required.

Examples

The following example enables local protection in an IPv6-supporting version of Cisco IOS software:

```
vrf definition vrf2
rd 100:3
address-family ipv6
protection local-prefixes
```

The following example enables local protection in an IPv4-only version of Cisco IOS software:

```
ip vrf vpn1
rd 100:3
protection local-prefixes
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enter address family or router scope address family configuration mode to configure a routing session using standard IPv4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bfd interval min_rx multiplier	Sets the BFD session parameters on an interface.
ip vrf	Defines a VPN VRF instance and enters VRF configuration mode.
neighbor fall-over	Enables BGP to monitor the peering session of a specified neighbor for adjacency changes and to deactivate the peering session.
rd	Specifies a RD for a VPN VRF instance.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

pseudowire

To bind a virtual circuit to a Layer 2 pseudowire for an xconnect service, use the **pseudowire** command in interface configuration mode. To remove the binding between a virtual circuit and a Layer 2 pseudowire, use the **no** form of this command.

pseudowire *peer-ip-address vcid* **pw-class** *pw-class-name* [**sequencing** {**transmit** | **receive** | **both**}]
no pseudowire

Syntax Description

peer-ip-address	IP address of the remote peer.
vcid	32-bit identifier of the virtual circuit between devices at each end of a Layer 2 control channel.
pw-class *pw-class-name*	Specifies the pseudowire class configuration from which the data encapsulation type is derived.
sequencing	(Optional) Configures sequencing options for xconnect.
transmit	(Optional) Transmits sequence numbers.
receive	(Optional) Receives sequence numbers.
both	(Optional) Transmits and receives sequence numbers.

Command Default

A virtual circuit is not bound to a Layer 2 pseudowire for an xconnect service.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.2(4)S	This command was modified. The behavior of the **no** form of this command was modified. A configured pseudowire must be disabled before disabling a virtual-ppp interface.

Usage Guidelines

The combination of the *peer-ip-address* and *vcid* arguments must be unique on a device.

The same *vcid* value that identifies a virtual circuit must be configured by using the **pseudowire** command on local and remote devices at each end of a Layer 2 session. The virtual circuit identifier creates a binding between a pseudowire and a virtual circuit.

The **pw-class** *pw-class-name* binds the pseudowire configuration of a virtual circuit to a specific pseudowire class. The pseudowire class configuration serves as a template that contains settings used by all virtual circuits bound to it by using the **pseudowire** command.

When removing a virtual-PPP interface that has a configured pseudowire, you must first remove the pseudowire by using the **no pseudowire** command.

Examples

The following example shows how to create a virtual-PPP interface, configure PPP on the virtual-PPP interface, and bind a virtual circuit to a Layer 2 pseudowire for an xconnect service for a pseudowire class named pwclass1:

```
interface virtual-ppp 1
 ppp authentication chap
 ppp chap hostname peer1
 pseudowire 172.24.13.196 10 pw-class pwclass1
```

The following example shows how to remove a virtual-PPP interface that has a configured pseudowire. You must first remove the configured pseudowire or an error is generated. Note that you can remove the virtual-PPP interface in interface configuration mode as shown below:

```
no interface virtual-ppp 1
% Interface Virtual-PPP1 not removed - Remove the Pseudowire
interface virtual-ppp 1
 no pseudowire
 no interface virtual-ppp 1
 end
```

Related Commands

Command	Description
interface virtual-ppp	Configures a virtual-PPP interface.
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which protocols are selected on the interface.
ppp chap hostname	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
pseudowire-class	Specifies the name of a Layer 2 pseudowire class and enters pseudowire class configuration mode.

pseudowire-class

To specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode, use the **pseudowire-class** command in global configuration mode. To remove a pseudowire class configuration, use the **no** form of this command.

pseudowire-class *pw-class-name*
no pseudowire-class *pw-class-name*

Syntax Description

pw-class-name	The name of a Layer 2 pseudowire class.

Command Default

No pseudowire classes are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

The **pseudowire-class** command allows you to configure a pseudowire class template that consists of configuration settings used by all attachment circuits bound to the class. A pseudowire class includes the following configuration settings:

- Data encapsulation type
- Control protocol
- Sequencing
- IP address of the local Layer 2 interface
- Type of service (ToS) value in IP headers

The local interface name for each pseudowire class configured between a pair of PE routers can be the same or different.

After you enter the **pseudowire-class** command, the router switches to pseudowire class configuration mode, where pseudowire settings may be configured.

Examples

The following example shows how to enter pseudowire class configuration mode to configure a pseudowire configuration template named “ether-pw”:

```
Router(config)
# pseudowire-class ether-pw
Router(config-pw)#
```

The following example shows how to enter pseudowire class configuration mode to configure a pseudowire configuration template named “mpls-ip”:

```
Router(config)
# pseudowire-class mpls-ip
```

Related Commands

Command	Description
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.
pseudowire	Binds an attachment circuit to a Layer 2 pseudowire for xconnect service.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

pseudowire-static-oam class

To create an Operations, Administration, and Maintenance (OAM) class and specify the timeout intervals, use the **pseudowire-static-oam class** command in global configuration mode. To remove the specified class, use the **no** form of this command.

pseudowire-static-oam class *class-name*
no pseudowire-static-oam class *class-name*

Syntax Description

class-name	Name of the class map.

Command Default

OAM classes are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Usage Guidelines

This command creates an OAM class and enters static pseudowire OAM configuration mode, from which you can enter timeout intervals.

Examples

The following example create the class oam-class3 and enters static pseudowire OAM configuration mode:

```
Router(config)# pseudowire-static-oam class oam-class3
Router(config-st-pw-oam-class)# timeout refresh send  ?
  <1-4095>  Seconds, default is 30
Router(config-st-pw-oam-class)# timeout refresh send  45
```

Related Commands

Command	Description
status protocol notification static	Invokes the specified class as part of the static pseudowire.

pseudowire-tlv template

To create a template of pseudowire type-length-value (TLV) parameters to use in an MPLS-TP configuration, use the **pseudowire-tlv template** command in privileged EXEC configuration mode. To remove the template, use the **no** form of this command.

pseudowire-tlv template *template-name*
no pseudowire-tlv template *template-name*

Syntax Description

template-name	Name for the TLV template.

Command Default

TLV values are not specified.

Command Modes

Privileged EXEC (config#)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Examples

The following example shows how to create a TLV template called tlv3:

```
Router(config)# pseudowire-tlv template tlv3
```

Related Commands

Command	Description
tlv template	Specifies a TLV template to use as part of local interface coniguration.

pseudowire routing

To configure Layer 2 VPN (L2VPN) pseudowire routing, use the **pseudowire routing** command in L2VPN configuration mode. To disable L2VPN pseudowire routing configuration, use the **no** form of this command.

pseudowire routing
no pseudowire routing

Syntax Description

This command has no arguments or keywords.

Command Default

L2VPN pseudowire routing is not configured.

Command Modes

L2VPN configuration (config-l2vpn)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **l2 pseudowire routing** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

The **pseudowire routing** command enters Layer 2 pseudowire routing configuration mode (config-l2_pw_rtg), in which you can use additional commands such as the **switching-point** command and the **terminating-pe tie-breaker** command. The **switching-point** command and the **terminating-pe tie-breaker** command are used to configure the L2VPN Virtual Private LAN Services (VPLS) interautonomous systems (Inter-AS) Option B feature. For more information about the L2VPN VPLS Inter-AS Option B feature, see the *Multiprotocol Label Switching Configuration Guide*.

Examples

The following example show how to enable Layer 2 pseudowire routing configuration mode:

```
Device(config)# l2vpn
Device(l2vpn-config)# pseudowire routing
Device(config-l2_pw_rtg)# terminating-pe tie-breaker
Device(config-l2_pw_rtg)# end
```

Related Commands

Command	Description
l2 pseudowire routing	Enter Layer 2 pseudowire routing configuration mode.
switching-point	Configures a switching point and specifies a VC ID range.
terminating-pe tie-breaker	Negotiates the behavior mode (either active or passive) for a TPE router.

pseudowire type

To specify the pseudowire type when configuring pseudowires in a Multiprotocol Label Switching Transport Protocol (MPLS-TP) network, use the **pseudowire type** command in interface configuration mode. To remove the pseudowire type, use the **no** form of this command.

pseudowire type *type-number*
no pseudowire type

Syntax Description

type-number	Type of pseudowire. The range is from 01 to 17 in hexadecimal format.

Command Default

The pseudowire type is not specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the MPLS-based Layer 2 VPN command modifications for cross-OS support. This command will replace the **local interface** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Pseudowires of type 01 to 17 in hexadecimal format are supported.

Note This command is only available for static pseudowires; that is, this command is only available when the signaling protocol is defined as none.

Examples

The following example shows how to specify a pseudowire of type 16:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# signaling protocol none
Device(config-if)# pseudowire type 16
```

Related Commands

Command	Description
local interface	Specifies the pseudowire type when configuring pseudowires in a MPLS-TP network.

redundancy delay (xconnect)

To specify how long a backup pseudowire should wait before resuming operation after the primary pseudowire goes down, use the **redundancy delay** command in xconnect configuration mode. To remove the specified delay time, use the **no** form of this command.

redundancy delay *enable-delay* {*disable-delay* | **never**}
no redundancy delay *enable-delay* {*disable-delay* | **never**}

Syntax Description

enable-delay	Number of seconds that elapse after the primary pseudowire VC goes down before the Cisco software activates the secondary pseudowire VC. The range is from 0 to 180. The default is 0.
disable-delay	Number of seconds that elapse after the primary pseudowire VC comes up before the Cisco software deactivates the secondary pseudowire VC. The range is from 0 to 180. The default is 0.
never	Specifies that the secondary pseudowire VC will not fall back to the primary pseudowire VC if the primary pseudowire VC becomes available again, unless the secondary pseudowire VC fails.

Command Default

If a failover occurs, the xconnect redundancy algorithm will immediately switch over or fall back to the backup or primary member in the redundancy group.

Command Modes

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. This command will replace the **backup delay** 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 an L2VPN xconnect with one redundant peer. Once a switchover to the secondary pseudowire occurs, there will be no fallback to the primary pseudowire unless the secondary pseudowire fails:

```
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# redundancy delay 0 never
```

Related Commands

Command	Description
backup delay (L2VPN local switching)	Configures a redundant peer for a pseudowire VC.

redundancy predictive

To enable predictive switchover to a backup pseudowire after the primary pseudowire goes down, use the **redundancy predictive** command in global configuration mode or xconnect configuration mode. To disable redundancy predictive mode, use the **no** form of this command.

redundancy predictive {**enabled** | **disabled**}
no redundancy predictive

Syntax Description

enabled	Enables redundancy predictive mode.
disabled	Disables redundancy predictive mode.

Command Default

Redundancy predictive mode is disabled.

Command Modes

Global configuration mode

Xconnect configuration (config-xconnect)

Command History

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

Examples

The following example shows how to enable redundancy predictive mode in global configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# l2vpn
Device(config-l2vpn)# redundancy predictive enabled
Device(config-l2vpn)# end
```

The following example shows how to enable redundancy predictive mode in xconnect configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# redundancy predictive enabled
Device(config-xconnect)# end
```

rd

To specify a route distinguisher (RD) for a VPN routing and forwarding (VRF) instance, use the **rd**command in VRF configuration mode. To remove a route distinguisher, use the **no** form of this command.

rd *route-distinguisher*
no rd *route-distinguisher*

Syntax Description

route-distinguisher	An 8-byte value to be added to an IPv4 prefix to create a VPN IPv4 prefix.

Command Default

No RD is specified.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)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.
12.2(33)SRB	Support for IPv6 was added.
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.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

An RD is either:

- ASN-related--Composed of an autonomous system number and an arbitrary number.

- IP-address-related--Composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

- *16-bit autonomous-system-number*:*your 32-bit number*. For example, 101:3.
- *32-bit IP address*:*your 16-bit-number*. For example, 192.168.122.15:1.

Examples

The following example shows how to configure a default RD for two VRFs. It illustrates the use of both autonomous-system-number-relative and IP-address-relative RDs:

```
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:3
Router(config-vrf)# exit
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 10.13.0.12:200
```

The following is an example of a VRF for IPv4 and IPv6 that has common policies defined in the global part of the VRF configuration:

```
vrf definition vrf2
 rd 200:1
 route-target both 200:2
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
 end
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.

rd (VPLS)

To specify a route distinguisher (RD) to distribute endpoint information in a Virtual Private LAN Service (VPLS) configuration, use the **rd** command in L2 VFI configuration or VFI autodiscovery configuration mode. To remove the manually configured RD and return to the automatically generated RD, use the **no** form of this command.

rd {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
no rd {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

Syntax Description

autonomous-system-number:*nn*	Specifies a 16-bit autonomous system number (ASN) and 32-bit arbitrary number. The ASN does not have to match the local autonomous system number.
ip-address:*nn*	Specifies a 32-bit IP address and a 16-bit arbitrary number. Only IPv4 addresses are supported.

Command Default

VPLS autodiscovery automatically generates a RD using the Border Gateway Protocol (BGP) autonomous system number and the configured virtual forwarding instance (VFI) VPN ID.

Command Modes

L2 VFI configuration (config-vfi)

VFI autodiscovery configuration (config-vfi-autodiscovery)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
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 VFI autodiscovery configuration mode.

Usage Guidelines

VPLS autodiscovery automatically generates an RD using the BGP autonomous system number and the configured VFI VPN ID. You can use this command to change the automatically generated RD.

The same RD value cannot be configured in multiple VFIs.

There are two formats for configuring the RD argument. It can be configured in the *autonomous-system-number*:*network-number* format, or it can be configured in the *ip-address*:*network-number* format.

An RD is either:

- Autonomous system-related—Composed of an autonomous system number and an arbitrary number.
- IP address-related—Composed of an IP address and an arbitrary number.

You can enter an RD in either of the following formats:

- *16-bit-autonomous-system-number*:*32-bit-number* —For example, 101:3.
- *32-bit-IP-address*:*16-bit-number* —For example, 192.168.122.15:1.

Examples

The following example shows a configuration using VPLS autodiscovery that sets the RD to an IP address of 10.4.4.4 and a network address of 70:

```
Device(config)# l2 vfi SP2 autodiscovery
Device(config-vfi)# vpn id 200
Device(config-vfi)# vpls-id 10.4.4.4:70
Device(config-vfi)# rd 10.4.5.5:7
```

The following example shows a configuration using VPLS Autodiscovery that sets the RD to an autonomous system number of 2 and a network address of 3:

```
Device(config)# l2 vfi SP2 autodiscovery
Device(config-vfi)# vpn id 200
Device(config-vfi)# vpls-id 10.4.4.4:70
Device(config-vfi)# rd 2:3
```

The following example shows a configuration using VPLS autodiscovery that sets the RD to an autonomous system number of 2 and a network address of 3 in VFI autodiscovery configuration mode:

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 200
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi-autodiscovery)# rd 2:3
```

Related Commands

Command	Description
autodiscovery (l2vpn vfi)	Designates VFI as having BGP autodiscovered pseudowire members.
l2 vfi autodiscovery	Enables a VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.

record-route (LSP Attributes)

To record the route used by the label switched path (LSP), use the **record-route**command in LSP Attributes configuration mode. To stop the recording the route used by the LSP, use the **no** form of this command.

record-route
no record-route

Syntax Description

This command has no arguments or keywords.

Command Default

The LSP route is not recorded.

Command Modes

LSP Attributes configuration (config-lsp-attr)

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.

Usage Guidelines

Use this command to set up in an LSP attribute list the recording of the route taken by the LSP.

To associate the LSP record-route attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to set up LSP route recording in an LSP attribute list:

```
configure terminal
!
mpls traffic-eng lsp attributes 9
 record-route
 exit
end
```

Related Commands

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

revision

To set the revision number for the Multiple Spanning Tree (802.1s) (MST) configuration, use the **revision** command in MST configuration submode. To return to the default settings, use the **no** form of this command.

revision *version*
no revision

Syntax Description

version	Revision number for the configuration; valid values are from 0 to 65535.

Command Default

version is **0**

Command Modes

MST configuration (config-mst)

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

Two Cisco 7600 series routers that have the same configuration but different revision numbers are considered to be part of two different regions.

Caution Be careful when using the **revision** command to set the revision number of the MST configuration because a mistake can put the switch in a different region.

Examples

This example shows how to set the revision number of the MST configuration:

```
Device(config-mst)# revision 5
Device(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST configuration submode)	Sets the name of an MST region.
show	Verifies the MST configuration.
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree mst configuration	Enters MST-configuration submode.

router-id

To specify a Layer 2 VPN (L2VPN) router ID for the provider edge (PE) router to use with Virtual Private LAN Services (VPLS) autodiscovery pseudowires, use the **router-id** command in L2VPN configuration mode. To reset the command to the default configuration, use the **no** form of this command.

router-id *ip-address*
no router-id *ip-address*

Syntax Description

ip-address	Router ID in IP address format.

Command Default

The L2VPN router ID is set to the Multiprotocol Label Switching (MPLS) global router ID.

Command Modes

L2VPN configuration (config-l2vpn)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **l2 router-id** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique.

The L2VPN router ID is used in the forward equivalence class (FEC) 129 encoding for pseudowire signaling. It is also used in the network layer reachability information (NLRI) for peer discovery.

Examples

The following example shows how to specify an L2VPN router ID:

```
Device(config)# l2vpn
Device(config-l2vpn)# router-id 10.1.1.1
```

Related Commands

Command	Description
l2 router-id	Specifies a router ID for the PE router to use with VPLS autodiscovery pseudowires.

route-target

To create a route-target extended community for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **route-target** command in VRF configuration or in VRF address family configuration mode. To disable the configuration of a route-target community option, use the **no** form of this command.

route-target [{**import** | **export** | **both**}] *route-target-ext-community*
no route-target [{**import** | **export** | **both**}] [*route-target-ext-community*]

Syntax Description

import	(Optional) Imports routing information from the target VPN extended community.
export	(Optional) Exports routing information to the target VPN extended community.
both	(Optional) Imports both import and export routing information to the target VPN extended community.
route-target-ext-community	The route-target extended community attributes to be added to the VRF's list of import, export, or both (import and export) route-target extended communities.

Command Default

A VRF has no route-target extended community attributes associated with it.

Command Modes

VRF address family configuration (config-vrf-af)
VRF configuration (config-vrf)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
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)SRB	This command was modified. Support for IPv6 was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers was changed to asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers was changed to asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 3.3SG	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **route-target** command creates lists of import and export route-target extended communities for the specified VRF. Enter the command one time for each target community. Learned routes that carry a specific route-target extended community are imported into all VRFs configured with that extended community as an import route target. Routes learned from a VRF site (for example, by Border Gateway Protocol (BGP), Routing Information Protocol (RIP), or static route configuration) contain export route targets for extended communities configured for the VRF added as route attributes to control the VRFs into which the route is imported.

The route target specifies a target VPN extended community. Like a route distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number. You can enter the numbers in either of these formats:

- 16-bit autonomous-system-number:your 32-bit number. For example, 101:3.
- 32-bit IP address:your 16-bit number. For example, 192.168.122.15:1.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538, for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2, for example--as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example shows how to configure route-target extended community attributes for a VRF in IPv4. The result of the command sequence is that VRF named vrf1 has two export extended communities (1000:1 and 1000:2) and two import extended communities (1000:1 and 10.27.0.130:200):

```
ip vrf vrf1
 route-target both 1000:1
 route-target export 1000:2
 route-target import 10.27.0.130:200
```

The following example shows how to configure route-target extended community attributes for a VRF that includes IPv4 and IPv6 address families:

```
vrf definition site1
rd 1000:1
address-family ipv4
 route-target export 100:1
 route-target import 100:1
address-family ipv6
 route-target export 200:1
 route-target import 200:1
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases shows how to create a VRF with a route target that uses a 4-byte autonomous system number in asplain format--65537--and how to set the route target to extended community value 65537:100 for routes that are permitted by the route map:

```
ip vrf vrf1
 rd 64500:100
 route-target both 65537:100
 exit
route-map vrf1 permit 10
 set extcommunity rt 65537:100
 end
```

After the configuration is completed, use the **show route-map** command to verify that the extended community is set to the route target containing the 4-byte autonomous system number of 65537:

```
Router# show route-map vrf1
route-map vrf1, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:65537:100
  Policy routing matches: 0 packets, 0 bytes
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, shows how to create a VRF with a route target that uses a 4-byte autonomous system number in asdot format--1.1--and how to set the route target to extended community value 1.1:100 for routes that are permitted by the route map:

```
ip vrf vrf1
 rd 64500:100
 route-target both 1.1:100
 exit
route-map vrf1 permit 10
 set extcommunity rt 1.1:100
 end
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
clear ip bgp	Resets Border Gateway Protocol (BGP) connections using hard or soft reconfiguration.
import map	Configures an import route map for a VRF.
ip vrf	Configures a VRF routing table.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.

route-target (VPLS)

To specify a route target for a Virtual Private LAN Services (VPLS) virtual forwarding instance (VFI), use the **route-target** command in L2 VFI configuration or VFI auto discovery configuration mode. To revert to the automatically generated route target, use the **no** form of this command.

route-target [{**import** | **export** | **both**}] {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
no route-target {**import** | **export** | **both**} {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

Syntax Description

import	(Optional) Imports routing information from the target VPN extended community.
export	(Optional) Exports routing information to the target VPN extended community.
both	(Optional) Imports and exports routing information to the target VPN extended community.
autonomous-system-number:*nn*	Specifies the autonomous system number (ASN) and a 32-bit number.
ip-address:*nn*	Specifies the IP address and a 16-bit number.

Command Default

VPLS Autodiscovery automatically generates a route target using the lower six bytes of the route distinguisher (RD) and VPLS ID.

Command Modes

L2 VFI configuration (config-vfi)

VFI autodiscovery configuration (config-vfi-autodiscovery)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
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 VFI autodiscovery configuration mode.

Usage Guidelines

The same route target cannot be configured in multiple VFIs.

The route target specifies a target VPN extended community. Like a route distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number. You can enter the numbers in either of the following formats:

- *16-bit-autonomous-system-number*:*32-bit-number*—For example, 101:3.
- *32-bit-IP-address*:*16-bit-number* —For example, 192.168.122.15:1.

Examples

The following example shows how to configure VPLS autodiscovery route-target extended community attributes for VFI SP1:

```
Device(config)# l2 vfi SP1 autodiscovery
Device(config-vfi)# vpn id 100
Device(config-vfi)# vpls-id 5:300
Device(config-vfi)# rd 4:4
Device(config-vfi)# route-target 10.1.1.1:29
```

The following example shows how to configure VPLS autodiscovery route-target extended community attributes for VFI vfi1:

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 100
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi-autodiscovery)# rd 4:4
Device(config-vfi-autodiscovery)# route-target 10.1.1.1:29
```

Related Commands

Command	Description
autodiscovery (l2vpn vfi)	Designates VFI as having BGP autodiscovered pseudowire members.
auto-route-target	Automatically generates the route target in a VFI.
l2 vfi autodiscovery	Enables a VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.

router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the **router bgp** command in global configuration mode. To remove a BGP routing process, use the **no** form of this command.

router bgp *autonomous-system-number*
no router bgp *autonomous-system-number*

Syntax Description

autonomous-system-number	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the "Usage Guidelines" section.

Command Default

No BGP routing process is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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)SRB	This command was modified. Support for IPv6 was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(33)SB	This command was modified. Support for IPv6 was added.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 3.3SG	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octet numbers in the range from 1 to 65535 as described in RFC 4271, *A Border Gateway Protocol 4 (BGP-4)* . Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) will start in January 2009 to allocate four-octet autonomous system numbers in the range from 65536 to 4294967295. RFC 5396, *Textual Representation of Autonomous System (AS) Numbers* , documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- Asplain—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- Asdot—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see RFC 5396.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

Asdot Only Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, the 4-octet (4-byte) autonomous system numbers are entered and displayed only in asdot notation, for example, 1.10 or 45000.64000. When using regular expressions to match 4-byte autonomous system numbers the asdot format includes a period which is a special character in regular expressions. A backslash must be entered before the period for example, 1\.14, to ensure the regular expression match does not fail. The table below shows the format in which 2-byte and 4-byte autonomous system numbers are configured, matched in regular expressions, and displayed in **show** command output in Cisco IOS images where only asdot formatting is available.

Table 8: Asdot Only 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Asplain as Default Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the default **show** command output to display 4-byte autonomous system numbers in the asdot format, use the **bgp asnotation dot** command under router configuration mode. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail. The tables below show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display **show** command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format. To display 4-byte autonomous system numbers in **show** command output and to control matching for regular expressions in the asdot format, you must configure the **bgp asnotation dot** command. After enabling the **bgp asnotation dot** command, a hard reset must be initiated for all BGP sessions by entering the **clear ip bgp *** command.

Note If you are upgrading to an image that supports 4-byte autonomous system numbers, you can still use 2-byte autonomous system numbers. The **show** command output and regular expression match are not changed and remain in asplain (decimal value) format for 2-byte autonomous system numbers regardless of the format configured for 4-byte autonomous system numbers.

Table 9: Default Asplain 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 65536 to 4294967295
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 65536 to 4294967295

Table 10: Asdot 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Reserved and Private Autonomous System Numbers

In Cisco IOS Release 12.0(32)S12, 12.0(32)SY8, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3 and later releases, the Cisco implementation of BGP supports RFC 4893. RFC 4893 was developed to allow BGP to support a gradual transition from 2-byte autonomous system numbers to 4-byte autonomous system numbers. A new reserved (private) autonomous system number, 23456, was created by RFC 4893 and this number cannot be configured as an autonomous system number in the Cisco IOS CLI.

RFC 5398, *Autonomous System (AS) Number Reservation for Documentation Use* , describes new reserved autonomous system numbers for documentation purposes. Use of the reserved numbers allow configuration examples to be accurately documented and avoids conflict with production networks if these configurations are literally copied. The reserved numbers are documented in the IANA autonomous system number registry. Reserved 2-byte autonomous system numbers are in the contiguous block, 64496 to 64511 and reserved 4-byte autonomous system numbers are from 65536 to 65551 inclusive.

Private 2-byte autonomous system numbers are still valid in the range from 64512 to 65534 with 65535 being reserved for special use. Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP should not be configured to advertise private autonomous system numbers to external networks. Cisco IOS software does not remove private autonomous system numbers from routing updates by default. We recommend that ISPs filter private autonomous system numbers.

Note Autonomous system number assignment for public and private networks is governed by the IANA. For information about autonomous-system numbers, including reserved number assignment, or to apply to register an autonomous system number, see the following URL: http://www.iana.org/.

Examples

The following example configures a BGP process for autonomous system 45000 and configures two external BGP neighbors in different autonomous systems using 2-byte autonomous system numbers:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain notation. This example is supported i n Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, and later releases.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

Command	Description
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

sdm prefer through show ip traffic-engineering configuration

sdm prefer

Use the **sdm prefer** global configuration command to configure the template used in Switch Database Management (SDM) resource allocation. A template allows you to allocate system memory to best support the features being used in your application. It allows you to approximate the maximum number of unicast MAC addresses, Internet Group Management Protocol (IGMP) groups, quality of service (QoS) access control entries (ACEs), security ACEs, unicast routes, multicast routes, subnet VLANs (routed interfaces), and Layer 2 VLANs that can be configured on the switch. Use the **no** form of the command to return to the default settings.

sdm prefer {**default** | **video** | **ip** | **mvpn_rsp1a** | **VPNv4/v6** | **netflow-video**}
no sdm prefer

Syntax Description

default	Balances all functions.
video	Increases multicast routes and access control lists (ACLs).
ip	Increases IPv4/VPNv4 routes. This option is available only on RSP1A.
mvpn_rsp1a	Supports MVPN. This option is available only on RSP1A.
VPNv4/v6	Increases VPNv4/VPNv6 routes. This option is available only on RSP1B.
netflow-video	Sets the template to video, and also allows configuration of netflow monitoring options by upgrading the router with the netflow supported FPGA. This keyword is introduced on the Cisco ASR 920 router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, and ASR-920-12SZ-IM) .

Command Default

The default template provides a balance to all features.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.10S	This command is supported on Cisco ASR 900 Series Aggregation Services Routers.
Cisxo IOS XE 3.18SP	This command is supported on Cisco ASR 920 Series Aggregation Services Routers. The **netflow-video** keyword is added. This keyword is introduced on the Cisco ASR 920 router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, and ASR-920-12SZ-IM) .

Usage Guidelines

The device must reload for the configuration to take effect.

When changing the SDM template, the router waits for two minutes before reloading. Do not perform any operation till the router reloads.

For the new SDM template to take effect, you must save and reload the new configuration, otherwise the current SDM template is retained.

The **sdm prefer netflow-video** command is used to enable Netflow monitoring through the FPGA image on the Cisco ASR 920 router (ASR-920-12CZ-A/ASR-920-12CZ-D/ASR-920-4SZ-A/ASR-920-4SZ-D and ASR-920-12SZ-IM).

The **sdm prefer video** command is used to enable Netflow monitoring on the ASR 900 RSP2 module and on the Cisco ASR 920 (ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M).

Examples

The following example shows how to configure the default template:

```
Router> enable
Device# configure terminal
Device(config)# sdm prefer default
```

The following example shows how to enable NetFlow on the router:

```
Router(config)# sdm prefer netflow-video
```

Related Commands

Command	Description
show sdm prefer current	Displays the current template configured on the device.

sdm prefer efp_feat_ext

Use the **sdm prefer efp_feat_ext** global configuration command to configure the split-horizon template. To disable the template use, **sdm prefer no efp_feat_ext** form of the command.

sdm prefer efp_feat_ext

Syntax Description

efp_feat_ext	Enables the template and allows for configuraion of 2 split-horizon groups on the EVc bridge domain.

Command Default

The command is not enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 16.6.1	This command was introduced on Cisco ASR 900 Series Aggregation Services Routers.

Usage Guidelines

Thie efp_feat_ext template when enabled allows configuation of two split-horizon groups on the EVC bridge domain.

Examples

The following example shows how to configure the template:

```
Device> enable
Device# configure terminal
Device(config)# sdm prefer efp_feat_ext
```

Related Commands

Command	Description
show sdm prefer current	Displays the current template configured on the device.

sequencing

To configure the direction in which sequencing is enabled for data packets in a Layer 2 pseudowire, use the **sequencing** command in the appropriate configuration mode. To remove the sequencing configuration from the pseudowire class, use the **no** form of this command.

sequencing {**transmit** | **receive** | **both** | **resync** *number*}
no sequencing {**transmit** | **receive** | **both** | **resync** *number*}

Syntax Description

transmit	Updates the Sequence Number field in the headers of data packets sent over the pseudowire according to the data encapsulation method that is used.
receive	Keeps the value in the Sequence Number field in the headers of data packets received over the pseudowire. Out-of-order packets are dropped.
both	Enables both the **transmit** and **receive** options.
resync	Enables packet sequencing reset after the disposition router receives a specified number of out-of-order packets.
number	The number of out-of-order packets that cause reset of packet sequencing. The range is from 5 to 65535.

Command Default

Sequencing is disabled.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
12.0(23)S	This command was introduced for Layer 2 Tunnel Protocol Version 3 (L2TPv3).
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.0(29)S	This command was updated to support Any Transport over MPLS (AToM).
12.0(30)S	This command was modified. The **resync** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was modified. L2TPv3 support for this command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was modified. AToM support for this command was integrated into Cisco IOS Release 12.2(28)SB.

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 MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support and 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.

Usage Guidelines

When you enable sequencing using any available options, the sequence numbers are automatically sent and a request is sent to the remote provider edge (PE) peer for sequence numbers. Out-of-order packets that are received on the pseudowire are dropped only if you use the **sequencing receive** or **sequencing both** command.

If you enable sequencing for Layer 2 pseudowires on the Cisco 7500 series routers and use the **ip cef distributed** command, all traffic on the pseudowires is switched through the line cards.

Use the **resync** keyword when the disposition router receives many out-of-order packets. It allows the router to recover when too many out-of-order packets are dropped.

Examples

The following example shows how to enable sequencing in data packets in Layer 2 pseudowires that were created from the pseudowire class named ether-pw. The Sequence Number field is updated in tunneled packet headers for data packets that are both sent and received over the pseudowire:

```
Device(config)# pseudowire-class ether-pw
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# sequencing both
```

The following example shows how to enable the disposition router to reset packet sequencing after it receives 1000 out-of-order packets:

```
Device(config)# pseudowire-class ether-pw
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# sequencing both
Device(config-pw-class)# sequencing resync 1000
```

The following example shows how to enable the disposition router to reset packet sequencing after it receives 1000 out-of-order packets in interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# sequencing both
Device(config-if)# sequencing resync 1000
```

The following example shows how to enable the disposition router to reset packet sequencing after it receives 1000 out-of-order packets in template configuration mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# sequencing both
Device(config-template)# sequencing resync 1000
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
ip cef	Enables Cisco Express Forwarding on the Route Processor card.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

set cos

To set the Layer 2 class of service (CoS) value of an outgoing packet, use the **setcos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

set cos {*cos-value* | *from-field* [**table** *table-map-name*]}
no set cos {*cos-value* | *from-field* [**table** *table-map-name*]}

Cisco CMTS and 10000 Series Router
set cos *cos-value*

Syntax Description

cos-value	Specific IEEE 802.1Q CoS value from 0 to 7.
from-field	Specific packet-marking category to be used to set the CoS value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows: • **precedence** • **dscp**
table	(Optional) Indicates that the values set in a specified table map will be used to set the CoS value.
table-map-name	(Optional) Name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

Command Default

No CoS value is set for the outgoing packet.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(13)T	This command was modified for Enhanced Packet Marking to allow a mapping table (table map)to be used to convert and propagate packet-marking values.
12.0(16)BX	This command was implemented on the Cisco 10000 series router for the ESR-PRE2.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.
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.

Release	Modification
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

CoS packet marking is supported only in the Cisco Express Forwarding switching path.

The **setcos** command should be used by a router if a user wants to mark a packet that is being sent to a switch. Switches can leverage Layer 2 header information, including a CoS value marking.

The **setcos** command can be used only in service policies that are attached in the output direction of an interface. Packets entering an interface cannot be set with a CoS value.

The **matchcos** and **setcos** commands can be used together to allow routers and switches to interoperate and provide quality of service (QoS) based on the CoS markings.

Layer 2 to Layer 3 mapping can be configured by matching on the CoS value because switches already can match and set CoS values. If a packet that needs to be marked to differentiate user-defined QoS services is leaving a router and entering a switch, the router should set the CoS value of the packet because the switch can process the Layer 2 header.

Using This Command with the Enhanced Packet Marking Feature

You can use this command as part of the Enhanced Packet Marking feature to specify the "from-field" packet-marking category to be used for mapping and setting the CoS value. The "from-field" packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-nam* e argument, the default action will be to copy the value associated with the "from-field" category as the CoS value. For instance, if you configure the **setcosprecedence** command, the precedence value will be copied and used as the CoS value.

You can do the same for the DSCP marking category. That is, you can configure the **setcosdscp** command, and the DSCP value will be copied and used as the CoS value.

Note If you configure the **setcosdscp**command, only the *first three bits* (the class selector bits) of the DSCP field are used.

Examples

In the following example, the policy map called "cos-set" is created to assign different CoS values for different types of traffic. This example assumes that the class maps called "voice" and "video-data" have already been created.

```
Router(config)#

policy-map cos-set

Router(config-pmap)#
```

```
class voice

Router(config-pmap-c)#

set cos 1

Router(config-pmap-c)#

exit

Router(config-pmap)#

class video-data

Router(config-pmap-c)#

set cos 2

Router(config-pmap-c)#

end
```

Enhanced Packet Marking Example

In the following example, the policy map called "policy-cos" is created to use the values defined in a table map called "table-map1". The table map called "table-map1" was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping)command, see the **table-map**(value mapping) command page.

In this example, the setting of the CoS value is based on the precedence value defined in "table-map1":

```
Router(config)#

policy-map policy-cos

Router(config-pmap)#

class class-default

Router(config-pmap-c)#

set cos precedence table table-map1
Router(config-pmap-c)#

end
```

Cisco CMTS Router: Example

The following example shows how to set the class of service for the 802.1p domain:

```
Router(config)# policy-map cos7
Router(config-pmap)# class cos7
Router(config-pmap-c)# set cos 2
Router(config-pmap-c)# end
```

Note The **setcos** command is applied when you create a service policy in QoS policy-map configuration mode and attach the service policy to an interface or ATM virtual circuit (VC). For information on attaching a service policy, refer to the "Modular Quality of Service Command-Line Interface Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide* .

Related Commands

Command	Description
match cos	Matches a packet on the basis of Layer 2 CoS marking.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
set precedence	Sets the precedence value in the packet header.
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 policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

set extcomm-list delete

To allow the deletion of extended community attributes based on an extended community list, use the **set extcomm-list delete** command in route-map configuration mode. To negate a previous **set extcomm-list detect** command, use the **no** form of this command.

set extcomm-list *extended-community-list-number* **delete**
no set extcomm-list *extended-community-list-number* **delete**

Syntax Description

extended-community-list-number	An extended community list number.

Command Default

Extended community attributes based on an extended community list cannot be deleted.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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

This command removes extended community attributes of an inbound or outbound Border Gateway Protocol (BGP) update using a route map to filter and determine the extended community attribute to be deleted and replaced. Depending upon whether the route map is applied to the inbound or outbound update for a neighbor, each extended community that passes the route map permit clause and matches the given extended community list will be removed and replaced from the extended community attribute being received from or sent to the BGP neighbor.

For information about how to use this command when translating a route target to a VPN distinguisher and vice versa, see the “BGP—VPN Distinguisher Attribute” module in the *IP Routing: BGP Configuration Guide*.

Examples

The following example shows how to replace a route target 100:3 on an incoming update with a route target of 100:4 using an inbound route map named extmap:

```
.
.
.
Device(config-af)# neighbor 10.10.10.10 route-map extmap in
.
.
.
Device(config)# ip extcommunity-list 1 permit rt 100:3
```

```
Device(config)# route-map extmap permit 10
Device(config-route-map)# match extcommunity 1
Device(config-route-map)# set extcomm-list 1 delete
Device(config-route-map)# set extcommunity rt 100:4 additive
```

The following example shows how to configure more than one replacement rule using the route-map configuration **continue** command. Prefixes with RT 100:2 are rewritten to RT 200:3 and prefixes with RT 100:4 are rewritten to RT 200:4. With the **continue** command, route-map evaluation proceeds even if a match is found in a previous sequence.

```
Device(config)# ip extcommunity-list 1 permit rt 100:3
Device(config)# ip extcommunity-list 2 permit rt 100:4
Device(config)# route-map extmap permit 10
Device(config-route-map)# match extcommunity 1
Device(config-route-map)# set extcomm-list 1 delete
Device(config-route-map)# set extcommunity rt 200:3 additive
Device(config-route-map)# continue 20
Device(config)# route-map extmap permit 20
Device(config-route-map)# match extcommunity 2
Device(config-route-map)# set extcomm-list 2 delete
Device(config-route-map)# set extcommunity rt 200:4 additive
Device(config-route-map)# exit
Device(config)# route-map extmap permit 30
```

Related Commands

Command	Description
ip community-list	Creates an extended community access list and controls access to it.
match extcommunity	Matches BGP extended community list attributes.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set extcommunity	Sets BGP extended community attributes.
set extcommunity vpn-distinguisher	Sets a VPN distinguisher attribute to routes.

set ipv6 default next-hop

To specify an IPv6 default next hop to which matching packets are forwarded, use the **set ipv6 default next-hop** command in route-map configuration mode. To delete the default next hop, use the **no** form of this command.

set ipv6 default [{**vrf** *vrf-name* | **global**}] **next-hop** *global-ipv6-address* [*global-ipv6-address...*]
no set ipv6 default [{**vrf** *vrf-name* | **global**}] **next-hop** *global-ipv6-address* [*global-ipv6-address...*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies explicitly that the default next-hops are under the specific Virtual Routing and Forwarding (VRF) instance.
global	(Optional) Specifies explicitly that the default next-hops are under the global routing table.
global-ipv6-address	IPv6 global address of the next hop to which packets are output. The next-hop router must be an adjacent router. This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

Packets are not forwarded to a default next hop.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *global-ipv6-address* argument.

Use the **set ipv6 default next-hop** command in policy-based routing PBR for IPv6 to specify an IPv6 next-hop address to which a packet is policy routed when the router has no route in the IPv6 routing table or the packets match the default route. The IPv6 next-hop address must be adjacent to the router; that is, reachable by using a directly connected IPv6 route in the IPv6 routing table. The IPv6 next-hop address also must be a global IPv6 address. An IPv6 link-local address cannot be used because the use of an IPv6 link-local address requires interface context.

If the software has no explicit route for the destination in the packet, then the software routes the packet to the next hop as specified by the **set ipv6 default next-hop** command. The optional specified IPv6 addresses are tried in turn.

Use the **ipv6 policy route-map** command, the **route-map** command, and the **match** and **set route-map** commands to define the conditions for PBR packets. The **ipv6 policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria, which are the conditions under which PBR occurs. The **set** commands specify the set actions, which are the particular routing actions to perform if the criteria enforced by the match commands are met.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**

Note The **set ipv6 next-hop** and **set ipv6 default next-hop** are similar commands. The **set ipv6 next-hop** command is used to policy route packets for which the router has a route in the IPv6 routing table. The **set ipv6 default next-hop** command is used to policy route packets for which the router does not have a route in the IPv6 routing table (or the packets match the default route).

Examples

The following example shows how to set the next hop to which the packet is routed:

```
ipv6 access-list match-dst-1
  permit ipv6 any 2001:DB8:4:1::1/64 any
route-map pbr-v6-default
  match ipv6 address match-dst-1
  set ipv6 default next-hop 2001:DB8:4:4::1/64
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 policy-based routing (PBR) on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.

Command	Description
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ipv6 next-hop (PBR)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy-based routing (PBR), use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 next-hop {*next-hop-ipv6-address* [{*next-hop-ipv6-address...*}] | **encapsulate l3vpn** *encapsulation-profile* | **peer-address** | **recursive** *next-hop-ipv6-address* | **verify-availability** *next-hop-ipv6-address sequence* **track** *object-number*}
no set ipv6 next-hop {*next-hop-ipv6-address* [{*next-hop-ipv6-address...*}] | **encapsulate l3vpn** *encapsulation-profile* | **peer-address** | **recursive** *next-hop-ipv6-address* | **verify-availability** *next-hop-ipv6-address sequence* **track** *object-number*}

Syntax Description

next-hop-ipv6-address [*next-hop-ipv6-address ...*]	IPv6 global address of the next hop to which packets are sent. The next-hop router must be an adjacent router. The IPv6 address must be specified in hexadecimal using 16-bit values between colons as specified in RFC 2373.
encapsulate	Specifies the encapsulation profile for the next-hop VPN.
l3vpn	Specifies Layer 3 VPN encapsulation.
encapsulation-profile	Encapsulation profile name.
peer-address	Specifies the peer address. This keyword is specific to Border Gateway Protocol (BGP).
recursive *next-hop-ipv6-address*	Specifies the IPv6 address of the recursive next-hop router. • The next-hop IPv6 address must be assigned separately from the recursive next-hop IPv6 address.
verify-availability	Verifies if the next-hop router is reachable.
sequence	Sequence number to insert into the next-hop list. Valid values for the *sequence* argument are from 1 to 65535.
track *object-number*	Sets the next-hop router depending on the state of a tracked object number. Valid values for the *object-number* argument are from 1 to 1000.

Command Default

Packets are not forwarded to a default next hop.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.

Release	Modification
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.4(2)S	This command was modified. The **recursive** keyword was added.

Usage Guidelines

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *next-hop-ipv6-address* argument. You must specify an IPv6 address; an IPv6 link-local address cannot be used because the use of an IPv6 link-local address requires interface context.

The *next-hop-ipv6-address* argument must specify an address that is configured in the IPv6 Routing Information Base (RIB) and is directly connected. A directly connected address is covered by an IPv6 prefix configured on an interface, or an address covered by an IPv6 prefix specified on a directly connected static route.

Examples

The following example shows how to set the next hop to which packets are routed:

```
ipv6 access-list match-dst-1
  permit ipv6 any 2001:DB8::1 any
!
route-map pbr-v6-default
  match ipv6 address match-dst-1
  set ipv6 next-hop 2001:DB8::F
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets are forwarded.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set mpls experimental

To set the Multiprotocol Label Switching (MPLS) experimental-bit value, use the **set mpls experimental** command in QoS policy-map configuration mode. To return to the default settings, use the **no** form of this command.

set mpls experimental {**imposition** | **topmost**} *experimental-value*
no set mpls experimental {**imposition** | **topmost**}

Syntax Description

imposition	Specifies the experimental-bit value on IP to Multiprotocol Label Switching (MPLS) or MPLS input in all newly imposed labels.
topmost	Specifies the experimental-bit value on the topmost label on the input or output flows.
experimental-value	Experimental-bit value; valid values are from 0 to 7.

Command Default

No experimental-bit value is set.

Command Modes

QoS policy-map configuration

Command History

Release	Modification
12.2(18)SXE	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.

Usage Guidelines

This command is not supported on systems that are configured with a Supervisor Engine 2.

Examples

This example shows how to set the experimental-bit value on the topmost label on input or output:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set mpls experimental topmost 5
```

set mpls experimental imposition

To set the value of the Multiprotocol Label Switching (MPLS) experimental (EXP) field on all imposed label entries, use the **set mpls experimental imposition** command in QoS policy-map class configuration mode. To disable the setting, use the **no** form of this command.

set mpls experimental imposition {*mpls-exp-value* | *from-field* [**table** *table-map-name*]}
no set mpls experimental imposition {*mpls-exp-value* | *from-field* [**table** *table-map-name*]}

Cisco 10000 Series Router
set mpls experimental imposition *mpls-exp-value*
no set mpls experimental imposition *mpls-exp-value*

Syntax Description

mpls-exp-value	Specifies the value used to set MPLS EXP bits defined by the policy map. Valid values are numbers from 0 to 7.
from-field	Specific packet-marking category to be used to set the MPLS EXP imposition value. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows: • **precedence** • **dscp**
table	(Optional) Used in conjunction with the *from-field*argument. Indicates that the values set in a specified table map will be used to set the MPLS EXP imposition value.
table-map-name	(Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the MPLS EXP imposition value. The name can be a maximum of 64 alphanumeric characters.

Command Default

No MPLS EXP value is set.

Command Modes

QoS policy-map class configuration

Command History

Release	Modification
12.2(13)T	This command was introduced; it replaces (renames) the **set mpls experimental** command, introduced in 12.1(5)T. The **set mpls experimental imposition** 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.
12.3(7)XII	This command was implemented on the ESR-PRE2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Release	Modification
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 **set mpls experimental imposition** command is supported only on input interfaces. Use this command during label imposition. This command sets the MPLS EXP field on all imposed label entries.

Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the class of service (CoS) value. The "from-field" packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the "from-field" category as the MPLS EXP imposition value. For instance, if you configure the **set mpls experimental imposition precedence** command, the precedence value will be copied and used as the MPLS EXP imposition value.

If you configure the **set mpls experimental imposition dscp** command, the DSCP value will be copied and used as the MPLS EXP imposition value.

Note If you configure the **set mpls experimental imposition dscp** command, only the *first three bits* (the class selector bits) of the DSCP field are used.

Cisco 10000 Series Router

Cisco IOS software replaced the **set mpls experimental** command with the **set mpls experimental imposition** command. However, the Cisco 10000 series router continues to use the **set mpls experimental** command for ESR-PRE1. For ESR-PRE2, the command is **set mpls experimental imposition** .

Examples

The following example shows how to set the MPLS EXP value to 3 on all imposed label entries:

```
Router(config-pmap-c)# set mpls experimental imposition 3
```

The following example shows how to create the policy map named policy1 to use the packet-marking values defined in a table map named table-map1. The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page. The MPLS EXP imposition value is set according to the DSCP value defined in table-map1.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set mpls experimental imposition dscp table table-map1
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
set dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
set mpls experimental topmost	Sets the MPLS EXP field value in the topmost label on either an input or an output interface.
set precedence	Sets the precedence value in the packet header.
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (value-mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set mpls experimental topmost

To set the Multiprotocol Label Switching (MPLS) experimental (EXP) field value in the topmost label on either an input or an output interface, use the **set mpls experimental topmost** command in QoS policy-map class configuration mode. To disable the setting, use the **no** form of this command.

set mpls experimental topmost {*mpls-exp-value* | **qos-group** [**table** *table-map-name*]}
no set mpls experimental topmost {*mpls-exp-value* | **qos-group** [**table** *table-map-name*]}

Syntax Description

mpls-exp-value	Specifies the value used to set MPLS experimental bits defined by the policy map. Valid values are numbers from 0 to 7.
qos-group	Specifies that the **qos-group** packet-marking category is used to set the MPLS EXP imposition value. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category.
table	(Optional) Used in conjunction with the **qos-group** keyword. Indicates that the values set in a specified table map will be used to set the MPLS EXP value.
table-map-name	(Optional) Used with the **table** keyword. Name of the table map used to specify the MPLS EXP value. The name can be a maximum of 64 alphanumeric characters.

Command Default

No MPLS EXP value is set.

Command Modes

QoS policy-map class configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
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)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

This command sets the MPLS EXP value only in the topmost label. This command does not affect an IP packet. The MPLS field in the topmost label header is not changed.

Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the qos-group packet-marking category to be used for mapping and setting the differentiated services code point (DSCP) value.

If you specify the qos-group category but do not specify the **table** *table-map-name* keyword and argument, the default action will be to copy the value associated with the qos-group category as the MPLS EXP topmost

value. For instance, if you configure the **set mpls experimental topmost qos-group** command, the QoS group value will be copied and used as the MPLS EXP topmost value.

The valid value range for the MPLS EXP topmost value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set mpls experimental topmost qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 6), the packet-marking value will be copied and the packets will be marked.
- If a QoS group value exceeds the MPLS EXP topmost range (for example, 10), the packet-marking value will not copied and the packet will not be marked. No action is taken.

Examples

The following example shows how to set the MPLS EXP value to 3 in the topmost label of an input or output interface:

```
Router(config-pmap)# set mpls experimental topmost 3
```

The following example shows how to create the policy map named policy1 to use the packet-marking values defined in a table map named table-map1. The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

The following example shows how to set the MPLS EXP value according to the QoS group value defined in table-map1.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set mpls experimental topmost qos-group table table-map1
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
match mpls experimental topmost	Matches the MPLS EXP field value in the topmost label.
set mpls experimental imposition	Sets the value of the MPLS EXP field on all imposed label entries.
set qos-group	Sets a group ID that can be used later to classify packets.
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set mpls-label

To enable a route to be distributed with a Multiprotocol Label Switching (MPLS) label if the route matches the conditions specified in the route map, use the **set mpls-label** command in route-map configuration mode. To disable this function, use the **no** form of this command.

set mpls-label
no set mpls-label

Syntax Description

This command has no arguments or keywords.

Command Default

No route with an MPLS label is distributed.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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)SRB	This command was modified. Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command can be used only with the **neighbor route-map out** command to manage outbound route maps for a Border Gateway Protocol (BGP) session.

Use the **route-map** global configuration command with **match** and **set route-map** commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Remember When you create a route-map, ensure that you configure the **set mpls-label** command for both locally originated and dynamically learnt prefixes. When you enable this command and apply the route-map in the outbound direction (using the command form **neighbor 2001:DB8:0::1 route-map outgoing out**), the MPLS label is retained.

Examples

The following example shows how to create a route map that enables the route to be distributed with a label if the IP address of the route matches an IP address in ACL1:

```
Device(config)# route-map outgoing permit 10
Device(config-route-map)# match ip address 1
Device(config-route-map)# set mpls-label
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list or specifies an IPv6 access list to use to match packets for PBR for IPv6.
match mpls-label	Redistributes routes that contain MPLS labels and match the conditions specified in the route map.
neighbor route-map out	Manage outbound route maps for a BGP session.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set ospf router-id

To set a separate Open Shortest Path First (OSPF) router ID for each interface or subinterface on a provider edge (PE) router for each directly attached customer edge (CE) router, use the **set ospf router-id** command in route map configuration mode.

set ospf router-id

Syntax Description

This command has no arguments or keywords.

Command Default

OSPF router ID is not set.

Command Modes

Route map configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
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

To use this command, you must enable OSPF and create a routing process.

Examples

The following example shows how to match the PE router IP address 192.168.0.0 against the interface in access list 1 and set to the OSPF router ID:

```
router ospf 2 vrfvpn1-site1
 redistribute bgp 100 metric-type 1 subnets
 network 202.0.0.0 0.0.0.255 area 1
router bgp 100
 neighbor 172.19.89. 62 remote-as 100
 access-list 1 permit 192.168.0.0
 route-map vpn1-site1-map permit 10
 match ip address 1
 set ospf router-id
```

Related Commands

Command	Description
router ospf	Enables OSPF routing, which places the router in router configuration mode.

set vrf

To enable VPN routing and forwarding (VRF) instance selection within a route map for policy-based routing (PBR) VRF selection, use the **set vrf** command in route-map configuration mode. To disable VRF selection within a route map, use the **no** form of this command.

set vrf *vrf-name*
no set vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to the VRF.

Command Default

VRF instance selection is not enabled within a route map for policy-based routing VRF selection.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SXI4	This command was modified. Support for IPv6 was added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **set vrf** route-map configuration command was introduced with the Multi-VRF Selection Using Policy-Based Routing feature to provide a PBR mechanism for VRF selection. This command enables VRF selection by policy routing packets through a route map. The route map is attached to the incoming interface. The match criteria are defined in an IP access list or in an IP prefix list. The match criteria can also be defined based on the packet length with the **match length** route map command. The VRF must be defined before you configure this command, and the **ip policy route-map** interface configuration command must be configured to enable policy routing under the interface or subinterface. If the VRF is not defined or if policy routing is not enabled, an error message will be displayed on the console when you attempt to configure the **set vrf** command.

Note The **set vrf** command is not supported in the hardware with the IP Services feature set. If this command is configured in IP Services, the packets are software switched. Hardware forwarding with this command in place requires packet circulation and is only supported in the Advanced IP Services feature set, which supports Multiprotocol Label Switching (MPLS).

In Cisco IOS Release 12.2(33)SXI4 on the Cisco Catalyst 6500, IPv6 PBR allows users to override normal destination IPv6 address-based routing and forwarding results. VRF allows multiple routing instances in Cisco software. The PBR feature is VRF-aware, meaning that it works under multiple routing instances, beyond the default or global routing table.

In PBR, the **set vrf** command decouples the VRF and interface association and allows the selection of a VRF based on the ACL-based classification using the existing PBR or route-map configurations. It provides a single router with multiple routing tables and the ability to select routes based on the ACL classification. The router classifies packets based on ACL, selects a routing table, looks up the destination address, and then routes the packet.

Note The functionality provided by the **set vrf** and **set ip global next-hop** commands can also be configured with the **set default interface**, **set interface**, **set ip default next-hop**, and **set ip next-hop** commands. However, the **set vrf** and **set ip global next-hop** commands take precedence over the **set default interface**, **set interface**,**set ip default next-hop**, and **set ip next-hop** commands. No error message is displayed indicating that VRF is already enabled if you attempt to configure the **set vrf** command with any of these four **set** commands.

Examples

The following example shows a route-map sequence that selects and sets a VRF based on the match criteria defined in three different access lists. (The access list configuration is not shown in this example.) If the route map falls through and a match does not occur, the packet will be dropped if the destination is local.

```
route-map PBR-VRF-Selection permit 10
match ip address 40
set vrf VRF1
!
route-map PBR-VRF-Selection permit 20
match ip address 50
set vrf VRF2
!
route-map PBR-VRF-Selection permit 30
match ip address 60
set vrf VRF3
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
debug ip policy	Displays the IP policy routing packet activity.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ip vrf	Configures a VRF routing table.
ip vrf receive	Inserts the IP address of an interface as a connected route entry in a VRF routing table.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or performs policy routing on packets.

Command	Description
match length	Bases policy routing on the Level 3 length of a packet.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and that have no explicit route to the destination.
set interface	Indicates where to forward packets that pass a match clause of a route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

show acircuit checkpoint

To display checkpointing information for each attachment circuit (AC), use the **show acircuit checkpoint** command in privileged EXEC mode.

show acircuit checkpoint

Syntax Description

This command has no arguments or keywords.

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.
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 integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

This command is used for interface-based attachment circuits. For Frame Relay and ATM circuits, use the following commands to show redundancy information:

- **debug atm ha-error**
- **debug atm ha-events**
- **debug atm ha-state**
- **debug atm l2transport**
- **debug frame-relay redundancy**

Examples

The following show acircuit checkpoint command displays information about the ACs that have been check-pointed. The output varies, depending on whether the command output is for the active or standby Route Processor (RP).

On the active RP, the command displays the following output:

```
Router# show acircuit checkpoint
AC HA Checkpoint info:
Last Bulk Sync: 1 ACs
 AC    IW    XC    Id  VCId   Switch    Segment  St  Chkpt
----  ----  ----  ---  ----  --------  --------  --  -----
HDLC  LIKE  ATOM    3   100      1000      1000   0    N
VLAN  LIKE  ATOM    2  1002      2001      2001   3    Y
```

On the standby RP, the command displays the following output::

```
Router# show acircuit checkpoint
```

```
AC HA Checkpoint info:
 AC    IW    XC    Id  VCId   Switch    Segment  St  F-SLP
----  ----  ----  ---  ----  --------  --------  --  -----
HDLC  LIKE  ATOM    3   100         0         0   0   001
VLAN  LIKE  ATOM    2  1002      2001      2001   2   000
```

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

Table 11: show acircuit checkpoint Field Descriptions

Field	Description
Last Bulk Sync	The number of ACs that were sent to the backup RP during the last bulk synchronization between the active and backup RPs.
AC	The type of attachment circuit.
IW	The type of interworking, either like-to-like (AToM) or any-to-any (Interworking).
XC	The type of cross-connect. Only AToM ACs are checkpointed.
ID	This field varies, depending on the type of attachment circuit. For Ethernet VLANs, the ID is the VLAN ID. For PPP and High-Level Data Link Control (HDLC), the ID is the AC circuit ID.
VCID	The configured virtual circuit ID.
Switch	An ID used to correlate the control plane and data plane contexts for this virtual circuit (VC). This is an internal value that is not for customer use.
Segment	An ID used to correlate the control plane and data plane contexts for this VC. This is an internal value that is not for customer use.
St	The state of the attachment circuit. This is an internal value that is not for customer use.
Chkpt	Whether the information about the AC was checkpointed.
F-SLP	Flags that provide more information about the state of the AC circuit. These values are not for customer use.

Related Commands

Command	Description
show mpls l2transport vc	Displays AToM status information.
show mpls l2transport vc checkpoint	Displays the status of the checkpointing process for both the active and standby RPs.

show atm cell-packing

To display the average number of cells in packets sent from an ATM permanent virtual circuit (PVC) to a single Multiprotocol Label Switching (MPLS) pseudowire and the average number of cells in packets that are received from an MPLS pseudowire and sent to the respective ATM virtual circuits (VCs), use the **show atm cell-packing** command in privileged EXEC mode.

show atm cell-packing

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

To map one or more ATM PVCs to a single pseudowire, an N:1 PVC must be created on an ATM interface. The output of the **show atm cell-packing** command can be used to gauge the amount of cell packing in packets that originate from a device and are received by the device, for a specific pseudowire. Cisco IOS software calculates the average number of cells per packet in each direction.

Examples

The following is sample output from the **show atm cell-packing** command. The fields in the output are self-explanatory.

```
Device# show atm cell-packing

                                 average                    average
circuit                 local    nbr of cells     peer      nbr of cells       MCPT
type                    MNCP     rcvd in one pkt  MNCP      sent in one pkt    us)

ATM4/0/0.1  vc   1/41    20            1     20         1                 100
ATM4/0/0.1  vc   1/42    20            1     20         1                 100
```

Related Commands

Command	Description
cell-packing	Enables multiple cell packing.

show atm vc

To display all ATM permanent virtual circuits (PVCs), switched virtual circuits (SVCs), and traffic information, use the **show atm vc** command in privileged EXEC mode.

show atm vc [{*vcd-number* | **range** *lower-limit-vcd upper-limit-vcd*}] [**interface atm** *interface-number*] [**detail** [**prefix** {**vpi/vci** | **vcd** | **interface** | **vc_name**}]] [*connection-name*] [**signalling** [{**freed-svcs** | [**cast-type** {**p2mp** | **p2p**}]}]] [**detail**] [{**interface atm** *interface-number* | **summary atm** *interface-number*}]

Syntax Description

vcd-number	(Optional) Specifies a unique virtual circuit descriptor (VCD) number that identifies PVCs within one ATM interface.
range *lower-limit-vcd upper-limit-vcd*	(Optional) Specifies the range of VCs. Displays all the VC information for the specified range of VCDs. The *lower-limit-vcd* argument specifies the lower limit of the VCD range. The *upper-limit-vcd* argument specifies the upper limit of the VCD range.
interface atm *interface-number*	(Optional) Interface number or subinterface number of the PVC or SVC. Displays all PVCs and SVCs on the specified interface or subinterface. The *interface-number* uses one of the following formats, depending on the router platform you use: • For the ATM Interface Processor (AIP) on Cisco 7500 series routers; for the ATM port adapter, ATM-CES port adapter, and enhanced ATM port adapter on Cisco 7200 series routers; for the 1-port ATM-25 network module on Cisco 2600 and 3600 series routers: *slot* **/ 0 .** *subinterface-number* **multipoint** • For the ATM port adapter and enhanced ATM port adapter on Cisco 7500 series routers : *slot* / *port-adapter* **/ 0 .** *subinterface-number* **multipoint** • For the network processing module (NPM) on Cisco 4500 and Cisco 4700 routers : *number* **.** *subinterface-number* **multipoint** • For a description of these arguments, refer to the **interface atm** command.
detail	(Optional) Displays the detailed information about the VCs.
prefix	(Optional) Displays detailed information about the selected VC category. You must specify one of the following VC categories: • **vpi/vci** --Virtual path identifier and virtual channel identifier. • **vcd** --Virtual circuit descriptor. • **interface** --Interface in which the VCD is configured. • **vc_name** --Name of the PVC or SVC.
connection-name	(Optional) Connection name of the PVC or SVC.

signalling	(Optional) Displays the ATM interface signaling information for all the interfaces.
freed-svcs	(Optional) Displays the details of the last few freed SVCs.
cast-type	(Optional) SVC cast type. You must specify one of the following connections: • **p2mp** --Point to multipoint connection. • **p2p** --Point to point connection.
summary atm *interface-number*	(Optional) Displays a summary of VCs.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
11.1CA	This command was modified. Information about VCs on an ATM-CES port adapter was added to the command output.
12.0(5)T	This command was modified. Information about VCs on an extended Multiprotocol Label Switching (MPLS) ATM interface was added to the command output.
12.2(25)S	This command was modified. Information about packet drops and errors was added to the command output.
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)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB and the **signalling** keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

If no value is specified for the *vcd* argument, the command displays information for all PVCs and SVCs. The output is in summary form (one line per virtual circuit).

VCs on the extended MPLS ATM interfaces do not appear in the **show atm vc** command output. Instead, the **show xtagatm vc** command provides a similar output that shows information only on extended MPLS ATM VCs.

Note The SVCs and the **signalling** keyword are not supported on the Cisco ASR 1000 series routers.

Examples

The following is sample output from the **show atm vc** command when no value for the *vcd* argument is specified. The status field is either ACTIVE or IN (inactive).

```
Router# show atm vc
Interface     VCD   VPI   VCI Type  AAL/Encaps     Peak   Avg.  Burst Status
ATM2/0          1     0     5  PVC  AAL5-SAAL     155000 155000    93 ACTIVE
ATM2/0.4        3     0    32  SVC  AAL5-SNAP     155000 155000    93 ACTIVE
ATM2/0.65432   10    10    10  PVC  AAL5-SNAP     100000  40000    10 ACTIVE
ATM2/0         99     0    16  PVC  AAL5-ILMI     155000 155000    93 ACTIVE
ATM2/0.105    250    33    44  PVC  AAL5-SNAP     155000 155000    93 ACTIVE
ATM2/0.100    300    22    33  PVC  AAL5-SNAP     155000 155000    93 ACTIVE
ATM2/0.12345 2047   255 65535  PVC  AAL5-SNAP         56     28  2047 ACTIVE
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified for a circuit emulation service (CES) circuit:

```
Router# show atm vc 2
ATM6/0: VCD: 2, VPI: 10, VCI: 10
PeakRate: 2310, Average Rate: 2310, Burst Cells: 94
CES-AAL1, etype:0x0, Flags: 0x20138, VCmode: 0x0
OAM DISABLED
InARP DISABLED
OAM cells received: 0
OAM cells sent: 334272
Status: ACTIVE
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified, displaying statistics for that virtual circuit only:

```
Router# show atm vc 8
ATM4/0: VCD: 8, VPI: 8, VCI: 8
PeakRate: 155000, Average Rate: 155000, Burst Cells: 0
AAL5-LLC/SNAP, etype:0x0, Flags: 0x30, VCmode: 0xE000
OAM frequency: 0 second(s)
InARP frequency: 1 minute(s)
InPkts: 181061, OutPkts: 570499, InBytes: 757314267, OutBytes: 2137187609
InPRoc: 181011, OutPRoc: 10, Broadcasts: 570459
InFast: 39, OutFast: 36, InAS: 11, OutAS: 6
OAM cells received: 0
OAM cells sent: 0
Status: UP
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified, AAL3/4 is enabled, an ATM Switched Multimegabit Data Service (SMDS) subinterface has been defined, and a range of message identifier numbers (MIDs) has been assigned to the PVC:

```
Router# show atm vc 1
ATM4/0.1: VCD: 1, VPI: 0, VCI: 1
PeakRate: 0, Average Rate: 0, Burst Cells: 0
AAL3/4-SMDS, etype:0x1, Flags: 0x35, VCmode: 0xE200
MID start: 1, MID end: 16
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified and generation of Operation, Administration, and Maintenance (OAM) F5 loopback cells has been enabled:

```
Router# show atm vc 7
ATM4/0: VCD: 7, VPI: 7, VCI: 7
PeakRate: 0, Average Rate: 0, Burst Cells: 0
AAL5-LLC/SNAP, etype:0x0, Flags: 0x30, VCmode: 0xE000
OAM frequency: 10 second(s)
InARP DISABLED
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast:0, OutFast:0, InAS:0, OutAS:0
OAM cells received: 0
OAM cells sent: 1
Status: UP
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified, and there is an incoming multipoint virtual circuit:

```
Router# show atm vc 3
ATM2/0: VCD: 3, VPI: 0, VCI: 33
PeakRate: 0, Average Rate: 0, Burst Cells: 0
AAL5-MUX, etype:0x809B, Flags: 0x53, VCmode: 0xE000
OAM DISABLED
InARP DISABLED
InPkts: 6646, OutPkts: 0, InBytes: 153078, OutBytes: 0
InPRoc: 6646, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
interface =  ATM2/0, call remotely initiated, call reference = 18082
vcnum = 3, vpi = 0, vci = 33, state = Active
 aal5mux vc, multipoint call
Retry count: Current = 0, Max = 10
timer currently inactive, timer value = never
Root Atm Nsap address: DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified, and there is an outgoing multipoint virtual circuit:

```
Router# show atm vc 6
ATM2/0: VCD: 6, VPI: 0, VCI: 35
PeakRate: 0, Average Rate: 0, Burst Cells: 0
AAL5-MUX, etype:0x800, Flags: 0x53, VCmode: 0xE000
OAM DISABLED
InARP DISABLED
InPkts: 0, OutPkts: 818, InBytes: 0, OutBytes: 37628
InPRoc: 0, OutPRoc: 0, Broadcasts: 818
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
interface =  ATM2/0, call locally initiated, call reference = 3
vcnum = 6, vpi = 0, vci = 35, state = Active
 aal5mux vc, multipoint call
Retry count: Current = 0, Max = 10
timer currently inactive, timer value = never
Leaf Atm Nsap address: DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12
Leaf Atm Nsap address: CD.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified and there is a PPP-over-ATM connection:

```
Router# show atm vc 1
ATM8/0.1: VCD: 1, VPI: 41, VCI: 41
PeakRate: 155000, Average Rate: 155000, Burst Cells: 96
AAL5-CISCOPPP, etype:0x9, Flags: 0xC38, VCmode: 0xE000
virtual-access: 1, virtual-template: 1
OAM DISABLED
```

```
InARP DISABLED
InPkts: 13, OutPkts: 10, InBytes: 198, OutBytes: 156
InPRoc: 13, OutPRoc: 10, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
OAM cells received: 0
OAM cells sent: 0
```

The following is sample output from the **show atm vc** command for IP multicast virtual circuits. The display shows the leaf count for multipoint VCs opened by the root. VCD 3 is a root of a multipoint VC with three leaf routers. VCD 4 is a leaf of some other router's multipoint VC. VCD 12 is a root of a multipoint VC with only one leaf router.

```
Router# show atm vc
            VCD/                                        Peak     Avg/Min     Burst
Interface   Name  VPI   VCI   Type     Encaps      Kbps    Kbps       Cells         Sts
0/0         1       0     5    PVC      SAAL     155000  155000       96           UP
0/0         2       0    16    PVC      ILMI     155000  155000       96           UP
0/0         3       0   124 MSVC-3      SNAP     155000  155000       96           UP
0/0         4       0   125   MSVC      SNAP     155000  155000       96           UP
0/0         5       0   126   MSVC      SNAP     155000  155000       96           UP
0/0         6       0   127   MSVC      SNAP     155000  155000       96           UP
0/0         9       0   130   MSVC      SNAP     155000  155000       96           UP
0/0         10      0   131    SVC      SNAP     155000  155000       96           UP
0/0         11      0   132 MSVC-3      SNAP     155000  155000       96           UP
0/0         12      0   133 MSVC-1      SNAP     155000  155000       96           UP
0/0         13      0   134    SVC      SNAP     155000  155000       96           UP
0/0         14      0   135 MSVC-2      SNAP     155000  155000       96           UP
0/0         15      0   136 MSVC-2      SNAP     155000  155000       96           UP
```

The following is sample output from the **show atm vc** command for an IP multicast virtual circuit. The display shows the owner of the VC and leaves of the multipoint VC. This VC was opened by IP multicast. The three leaf routers' ATM addresses are included in the display. The VC is associated with IP group address 10.1.1.1.

```
Router# show atm vc 11
ATM0/0: VCD: 11, VPI: 0, VCI: 132
PeakRate: 155000, Average Rate: 155000, Burst Cells: 96
AAL5-LLC/SNAP, etype:0x0, Flags: 0x650, VCmode: 0xE000
OAM DISABLED
InARP DISABLED
InPkts: 0, OutPkts: 12, InBytes: 0, OutBytes: 496
InPRoc: 0, OutPRoc: 0, Broadcasts: 12
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
OAM cells received: 0
OAM cells sent: 0
Status: ACTIVE, TTL: 2, VC owner: IP Multicast (10.1.1.1)
interface =  ATM0/0, call locally initiated, call reference = 2
vcnum = 11, vpi = 0, vci = 132, state = Active
 aal5snap vc, multipoint call
Retry count: Current = 0, Max = 10
timer currently inactive, timer value = 00:00:00
Leaf Atm Nsap address: 47.009181000000000 2BA08E101.444444444444.02
Leaf Atm Nsap address: 47.009181000000000 2BA08E101.333333333333.02
Leaf Atm Nsap address: 47.009181000000000 2BA08E101.222222222222.02
```

The following is sample output from the **show atm vc** command where no VCD is specified and private VCs are present:

```
Router# show atm vc
AAL /         Peak   Avg.  Burst
Interface     VCD   VPI   VCI Type  Encapsulation  Kbps   Kbps  Cells Status
```

```
ATM1/0          1     0    40  PVC  AAL5-SNAP          0      0     0 ACTIVE
ATM1/0          2     0    41  PVC  AAL5-SNAP          0      0     0 ACTIVE
ATM1/0          3     0    42  PVC  AAL5-SNAP          0      0     0 ACTIVE
ATM1/0          4     0    43  PVC  AAL5-SNAP          0      0     0 ACTIVE
ATM1/0          5     0    44  PVC  AAL5-SNAP          0      0     0 ACTIVE
ATM1/0         15     1    32  PVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0         17     1    34  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0         26     1    43  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0         28     1    45  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0         29     1    46  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0         33     1    50  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
```

When you specify a VCD value and the VCD corresponds to that of a private VC on a control interface, the display output appears as follows:

```
Router# show atm vc 15
ATM1/0 33     1    50  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0: VCD: 15, VPI: 1, VCI: 32, etype:0x8, AAL5 - XTAGATM, Flags: 0xD38
PeakRate: 0, Average Rate: 0, Burst Cells: 0, VCmode: 0x0
XTagATM1, VCD: 1, VPI: 0, VCI: 32
OAM DISABLED, InARP DISABLED
InPkts: 38811, OutPkts: 38813, InBytes: 2911240, OutBytes: 2968834
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
OAM F5 cells sent: 0, OAM cells received: 0
Status: ACTIVE
```

The table below describes the fields shown in the displays.

Table 12: show atm vc Field Descriptions

Field	Description
Interface	Interface slot and port.
VCD/Name	Virtual circuit descriptor (virtual circuit number). The connection name is displayed if the virtual circuit (VC) was configured using the **pvc** command and the name was specified.
VPI	Virtual path identifier.
VCI	Virtual channel identifier.

Field	Description
Type	Type of VC, either PVC, SVC, TVC, or multipoint SVC (MSVC). • MSVC (with no -*x*) indicates that VCD is a leaf of some other router's multipoint VC. • MSVC-*x* indicates there are *x* leaf routers for that multipoint VC opened by the root. Type of PVC detected from PVC discovery, either PVC-D, PVC-L, or PVC-M. • PVC-D indicates a PVC created due to PVC discovery. • PVC-L indicates that the corresponding peer of this PVC could not be found on the switch. • PVC-M indicates that some or all of the quality of service (QoS) parameters of this PVC do not match those of the corresponding peer on the switch. • TVC indicates a Tag VC.
Encaps	Type of ATM adaptation layer (AAL) and encapsulation.
PeakRate	Kilobits per second sent at the peak rate.
Average Rate	Kilobits per second sent at the average rate.
Burst Cells	Value that equals the maximum number of ATM cells the VC can send at peak rate.
Status	Status of the VC connection. • UP indicates that the connection is enabled for data traffic. • DN indicates that the connection is down (not ready for data traffic). When the Status field is DN (down), a State field is shown. • IN indicates that the interface is down (inactive). • ACTIVE indicates that the interface is in use and active.
etype	Encapsulation type.
Flags	Bit mask describing VC information. The flag values are summed to result in the displayed value. 0x10000 ABR VC 0x20000 CES VC 0x40000 TVC 0x100 TEMP (automatically created) 0x200 MULTIPOINT 0x400 DEFAULT_RATE 0x800 DEFAULT_BURST 0x10 ACTIVE 0x20 PVC 0x40 SVC 0x0 AAL5-SNAP 0x1 AAL5-NLPID 0x2 AAL5-FRNLPID 0x3 AAL5-MUX 0x4 AAL3/4-SMDS 0x5 QSAAL 0x6 AAL5-ILMI 0x7 AAL5-LANE 0x8 AAL5-XTAGATM 0x9 CES-AAL1 0xA F4-OAM
VCmode	AIP-specific or NPM-specific register describing the usage of the VC. This register contains values such as rate queue, peak rate, and AAL mode, which are also displayed in other fields.

Field	Description
OAM frequency	Seconds between OAM loopback messages, or DISABLED if OAM is not in use on this VC.
InARP frequency	Minutes between Inverse Address Resolution Protocol (InARP) messages, or DISABLED if InARP is not in use on this VC.
virtual-access	Virtual access interface identifier.
virtual-template	Virtual template identifier.
InPkts	Total number of packets received on this VC. This number includes all fast-switched and process-switched packets.
OutPkts	Total number of packets sent on this VC. This number includes all fast-switched and process-switched packets.
InBytes	Total number of bytes received on this VC. This number includes all fast-switched and process-switched packets.
OutBytes	Total number of bytes sent on this VC. This number includes all fast-switched and process-switched packets.
InPRoc	Number of process-switched input packets.
OutPRoc	Number of process-switched output packets.
Broadcasts	Number of process-switched broadcast packets.
InFast	Number of fast-switched input packets.
OutFast	Number of fast-switched output packets.
InAS	Number of autonomous-switched or silicon-switched input packets.
VC TxRingLimit	Transmit Ring Limit for this VC.
VC Rx Limit	Receive Ring Limit for this VC.
Transmit priority	ATM service class transmit priority for this VC.
InCells	Number of incoming cells on this VC.
OutCells	Number of outgoing cells on this VC.
InPktDrops	A non-zero value for the InPktDrops of a VC counter suggests that the ATM interface is running out of packet buffers for an individual VC, or is exceeding the total number of VC buffers that can be shared by the VCs.
OutPktDrops	The PA-A3 driver increments the OutPktDrops counter when a VC fills its individual transmit buffer quota. The purpose of the quota is to prevent a consistently oversubscribed VC from grabbing all of the packet buffer resources and hindering other VCs from transmitting normal traffic within their traffic contracts.

Field	Description
InCellDrops	Number of incoming cells dropped on this VC.
OutCellDrops	Number of outgoing cells dropped on this VC.
InByteDrops	Number of incoming bytes that are dropped on this VC.
OutByteDrops	Number of outgoing bytes that are dropped on this VC.
CrcErrors	Number of cyclic redundancy check (CRC) errors on this VC.
SarTimeOuts	Number of segmentation and reassembly sublayer time-outs on this VC.
OverSizedSDUs	Number of over-sized service data units on this VC
LengthViolation	Number of length violations on this VC. A length violation occurs when a reassembled packet is dropped without checking the CRC.
CPIErrors	The Common Part Indicator error field is a one octet field in the AAL5 encapsulation of an ATM cell and must be set to 0. If it is received with some other value, it is flagged as an error by the interface. For example, this error may indicate data corruption.
Out CLP	Number of packets or cells where the Output Cell Loss Priority bit is set.
OutAS	Number of autonomous-switched or silicon-switched output packets.
OAM cells received	Number of OAM cells received on this VC.
OAM cells sent	Number of OAM cells sent on this VC.
TTL	Time to live in ATM hops across the VC.
VC owner	IP Multicast address of the group.

Related Commands

Command	Description
atm nsap-address	Sets the NSAP address for an ATM interface using SVC mode.
show xtagatm vc	Displays information about the VCs on the extended MPLS ATM interfaces.

show bridge-domain

To display bridge-domain information, use the **show bridge-domain** command in privileged EXEC mode.

show bridge-domain [{[*bridge-id*] [**c-mac**] [**mac** {**security** [{**address** | **last violation** | **statistics**}] | **static address** | **table** [{*mac-address* | **aging-time** | **count**}]}] | **split-horizon** [**group** {*group-number* | **all** | **none**}] | **stats**}]

Syntax Description

bridge-id	(Optional) Identifier for the bridge-domain instance. Integer in the range 1 to Platform_Upper_Bound, where Platform_Upper_Bound is a platform-specific upper limit.
c-mac	(Optional) Displays a specified customer bridge domain.
mac	(Optional) Displays MAC address data. **Note** The **mac** keyword is not supported on the Cisco ASR 1000 Series Aggregation Services Router.
security	(Optional) Displays MAC security information.
address	(Optional) Displays addresses. • When used with the **security** keyword, displays secure addresses on a specified service instance. • When used with the **static** keyword, displays static addresses in a specified bridge domain. **Note** The **address** keyword is not supported on the Cisco ASR 1000 Series Aggregation Services Router.
last	(Optional) Displays the last violation recorded on the specified bridge domain.
violation	(Optional) Displays information about the last violation recorded on the specified bridge domain.
statistics	(Optional) Displays the number of secured MAC addresses and related statistics.
static	(Optional) Displays static MAC information.
table	(Optional) Displays commands related to the MAC address table.
mac-address	(Optional) Displays the MAC address.
aging-time	(Optional) Displays the time, in minutes, that an entry remains before aging out of the MAC address table.
count	(Optional) Displays the total number of addresses in a bridge-domain table.
split-horizon	(Optional) Displays bridge-domain information for a split-horizon.
group	(Optional) Displays bridge-domain information for a split-horizon group.

group-number	(Optional) Number of a specific split-horizon group for bridge-domain information display.
all	(Optional) Selects all ports in split-horizon groups for bridge-domain information display.
none	(Optional) Selects ports that do not belong to any split-horizon group for bridge-domain information display.
stats	(Optional) Displays bridge-domain statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRD	This command was introduced.
12.2(33)SRE	This command was modified. The **address**, **aging-time**, **count**, **static**, and **table** keywords and the *mac-address* argument were added.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S to provide support for the Cisco ASR 903 Series Aggregation Services Router. This command was modified to provide support for Ethernet Flow Points (EFPs) on trunk ports (interfaces).
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S. The command was modified to display the MAC address limit for the bridge domain.

Usage Guidelines

This command is useful for system monitoring and troubleshooting.

This command is available on both linecards and route processors. To invoke this command on a linecard, log in to the linecard. To invoke this command on a route processor, use the **remote command module** command; for example, **remote command module16 bridge-domain 25**.

Note The **remote command** command is not supported on the Cisco ASR 1000 Series Aggregation Services Router.

Examples

The following is sample output of the **show bridge-domain** command. The output varies slightly by platform. The fields are self-explanatory.

```
Device# show bridge-domain 10

Bridge-domain 10 (2 ports in all)
State: UP                    Mac learning: Enabled
Aging-Timer: 300 second(s)
    GigabitEthernet0/2/2 service instance 10
    GigabitEthernet0/2/3 service instance 10
   MAC address    Policy Tag           Age Pseudoport[VC-lbl,egr-intf]
   0000.5200.010E fwd    dynamic    300 GigabitEthernet0/2/3.EFP10
   0000.5200.010C fwd    dynamic    300 GigabitEthernet0/2/3.EFP10
```

```
   0000.5200.0107 fwd    dynamic    299 GigabitEthernet0/2/3.EFP10
   0000.5200.0104 fwd    dynamic    300 GigabitEthernet0/2/3.EFP10
```

The following is sample output where the MAC address limit is displayed:

```
Device# show bridge-domain 100 mac address

Bridge-domain 100 (2 ports in all)
State: UP                    Mac learning: Enabled
Aging-Timer: 5 minute(s)
Maximum address limit: 10240      Current addresses: 300
    Ethernet0/0 service instance 100
    Maximum address limit: 200      Current addresses: 100
1 ports belonging to split-horizon group 1
    Ethernet0/0 service instance 101 (split-horizon group 1)
   Maximum address limit: 300      Current addresses: 150
  Software Bridging Info for Bridge Domain 100, contains 2 ports
   MAC address     Pseudoport
```

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

Table 13: show bridge-domain Field Descriptions

Field	Description
Maximum address limit	The maximum MAC addresses configured for the bridge domain.
Current addresses	The current number of MAC addresses learned for the bridge domain. **Note** This information may not display for all platforms.

The following example shows the sample output where information of the Ethernet over Generic Routing Encapsulation (GRE) for a specific bridge domain are displayed:

```
Device# show bridge-domain 10

Bridge-domain 10 (2 ports in all)
State: UP                    Mac learning: Enabled
Aging-Timer: 180 second(s)
    GigabitEthernet2/0/0 service instance 1
    Virtual-Ethernet1 service instance 1
 MAC address    Policy    Tag     Age Pseudoport
   0000.0000.0002 forward dynamic   177 Virtual-Ethernet1.EFP1 sGRE src:11.1.1.1 dst:1.1.1.2

   0000.0000.0001 forward dynamic 180  GigabitEthernet2/0/0.EFP1
```

Related Commands

Command	Description
clear bridge-domain	Clears bridge-domain attributes that are not needed.
remote command	Executes a Cisco 7600 Series Router command directly on the console or a specified module without having to log into the Cisco 7600 Series Router first.
show ethernet service instance	Displays information about Ethernet service instances.

Command	Description
show ethernet service interface	Displays interface-only information about Ethernet customer service instances.

show connection

To display the status of interworking connections, use the **show connection** command in privileged EXEC mode.

show connection[{**all***element* | **id** *startid*-[{*endid*}] | **name** *name* | **port** *port*}]

Syntax Description

all	(Optional) Displays information about all interworking connections.
element	(Optional) Displays information about the specified connection element.
id	(Optional) Displays information about the specified connection identifier.
startid	Starting connection ID number.
endid	(Optional) Ending connection ID number.
name *name*	(Optional) Displays information about the specified connection name.
port *port*	(Optional) Displays information about all connections on an interface. (In Cisco IOS Release 12.0S, only ATM, serial, and Fast Ethernet are shown.)

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(2)T	This command was introduced as show connect (FR-ATM).
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S and updated to show all ATM, serial, and Fast Ethernet interworking connections.
12.4(2)T	The command output was modified to add Segment 1 and Segment 2 fields for Segment state and channel ID.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(8)	This command was integrated into Cisco IOS Release 12.4(8).
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.
12.2SX	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.

Release	Modification
12.2(33)SB	This command was updated to display High-Level Data Link Control (HDLC) local switching connections.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example shows the local interworking connections on a router:

```
Device# show connection

ID   Name               Segment 1            Segment 2           State
=============================================================================
1    conn1          ATM 1/0/0 AAL5 0/100   ATM 2/0/0 AAL5 0/100   UP
2    conn2          ATM 2/0/0 AAL5 0/300   Serial0/1 16           UP
3    conn3          ATM 2/0/0 AAL5 0/400   FA 0/0.1 10            UP
4    conn4          ATM 1/0/0 CELL 0/500   ATM 2/0/0 CELL 0/500   UP
5    conn5          ATM 1/0/0 CELL 100     ATM 2/0/0 CELL 100     UP
```

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

Table 14: show connection Field Descriptions

Field	Description
ID	Arbitrary connection identifier assigned by the operating system.
Name	Name of the connection.
Segment 1 Segment 2	Information about the interworking segments: • Interface name and number. • Segment state, interface name and number, and channel ID. Segment state will displays nothing if the segment state is UP, "-" if the segment state is DOWN, and "***Card Removed***" if the segment state is DETACHED. • Type of encapsulation (if any) assigned to the interface. • Permanent virtual circuit (PVC) assigned to the ATM interface, data-link connection identifier (DLCI) assigned to the serial interface, or VLAN ID assigned to the Ethernet interface.
State	Status of the connection, which is one of the following: INVALID, UP, ADMIN UP, ADMIN DOWN, OPER DOWN, COMING UP, NOT VERIFIED, ERR.

Related Commands

Command	Description
connect (L2VPN local switching)	Connects two different or like interfaces on a router.
show atm pvc	Displays the status of ATM PVCs and SVCs.

Command	Description
show frame-relay pvc	Displays the status of Frame Relay interfaces.

show controllers vsi control-interface

Note Effective with Cisco IOS Release 12.4(20)T, the **show controllers vsi control-interface** is not available in Cisco IOS software.

To display information about an ATM interface configured with the **tag-control-protocol vsi** command to control an external switch (or if an interface is not specified, to display information about all Virtual Switch Interface [VSI] control interfaces), use the **show controllers vsi control-interface** command in user EXEC or privileged EXEC mode.

show controllers vsi control-interface [*interface*]

Syntax Description

interface	(Optional) Specifies the interface number.

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

The following is sample output from the **show controllers vsi control-interface** command:

```
Router# show controllers vsi control-interface
Interface:            ATM2/0        Connections:          14
```

The display shows the number of cross-connects currently on the switch that were established by the MPLS LSC through the VSI over the control interface.

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

Table 15: show controllers vsi control-interface Field Descriptions

Field	Description
Interface	The (Cisco IOS) interface name.
Connections	The number of cross connections currently on the switch.

Related Commands

Command	Description
tag-control-protocol vsi	Configures the use of VSI on a control port.

show controllers vsi descriptor

Note Effective with Cisco IOS Release 12.4(20)T, the **show controllers vsi descriptor** command is not available in Cisco IOS software.

To display information about a switch interface discovered by the Multiprotocol Label Switching (MPLS) Label Switch Controller (LSC) through a Virtual Switch Interface (VSI), or if no descriptor is specified, about all such discovered interfaces, use the **show controllers vsi descriptor** command in user EXEC or privileged EXEC mode.

show controllers vsi descriptor [*descriptor*]

Syntax Description

descriptor	(Optional) Physical descriptor. For the Cisco BPX switch, the physical descriptor has the following form: *>slot.port .>0*

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

Specify an interface by its (switch-supplied) physical descriptor.

Per-interface information includes the following:

- Interface name
- Physical descriptor
- Interface status
- Physical interface state (supplied by the switch)
- Acceptable VPI and VCI ranges
- Maximum cell rate
- Available cell rate (forward/backward)
- Available channels

Similar information is displayed when you enter the **show controllers xtagatm** privileged EXEC command. However, you must specify a Cisco IOS interface name instead of a physical descriptor.

Examples

The following is sample output from the **show controllers vsi descriptor** command:

```
Router# show controllers vsi descriptor 12.2.0
Phys desc: 12.2.0
Log intf:  0x000C0200 (0.12.2.0)
Interface: XTagATM0
IF status: up                  IFC state: ACTIVE
Min VPI:   1                   Maximum cell rate:  10000
Max VPI:   259                 Available channels: 2000
Min VCI:   32                  Available cell rate (forward):  10000
Max VCI:   65535               Available cell rate (backward): 10000
```

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

Table 16: show controllers vsi descriptor Field Descriptions

Field	Description
Phys desc	Physical descriptor. A string learned from the switch that identifies the interface.
Log intf	Logical interface ID. This 32-bit entity, learned from the switch, uniquely identifies the interface.
Interface	The (Cisco IOS) interface name.
IF status	Overall interface status. Can be “up,” “down,” or “administratively down.”
Min VPI	Minimum virtual path identifier. Indicates the low end of the VPI range configured on the switch.
Max VPI	Maximum virtual path identifier. Indicates the high end of the VPI range configured on the switch.
Min VCI	Minimum virtual path identifier. Indicates the high end of the VCI range configured on the switch.
Max VCI	Maximum virtual channel identifier. Indicates the high end of the VCI range configured on, or determined by, the switch.
IFC state	Operational state of the interface, according to the switch. Can be one of the following: • FAILED_EXT (that is, an external alarm) • FAILED_INT (indicates the inability of the MPLS LSC to communicate with the VSI slave controlling the interface, or another internal failure) • REMOVED (administratively removed from the switch)
Maximum cell rate	Maximum cell rate for the interface, which has been configured on the switch (in cells per second).
Available channels	Indicates the number of channels (endpoints) that are currently free to be used for cross-connects.
Available cell rate (forward)	Cell rate that is currently available in the forward (that is, ingress) direction for new cross-connects on the interface.

Field	Description
Available cell rate (backward)	Cell rate that is currently available in the backward (that is, egress) direction for new cross-connects on the interface.

Related Commands

Command	Description
show controllers xtagatm	Displays information about an extended MPLS ATM interface.

show controllers vsi session

Note Effective with Cisco IOS Release 12.4(20)T, the **show controllers vsi session** command is not available in Cisco IOS software.

To display information about all sessions with Virtual Switch Interface (VSI) subordinates, use the **show controllers vsi session** command in user EXEC or privileged EXEC mode.

show controllers vsi session [*session-number* [**interface** *interface*]]

Syntax Description

session-number	(Optional) Specifies the session number.
interface *interface*	(Optional) Specifies the VSI control interface.

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

If a session number and an interface are specified, detailed information on the individual session is presented. If the session number is specified, but the interface is omitted, detailed information on all sessions with that number is presented. (Only one session can contain a given number, because multiple control interfaces are not supported.)

Note A session consists of an exchange of VSI messages between the primary VSI (the LSC) and a VSI subordinate (an entity on the switch). There can be multiple VSI subordinates for a switch. On the BPX, each port or trunk card assumes the role of a VSI subordinate.

Examples

The following is sample output from the **show controllers vsi session** command:

```
Router# show controllers vsi session
Interface    Session  VCD    VPI/VCI    Switch/Slave Ids   Session State

ATM0/0       0        1      0/40       0/1                ESTABLISHED
ATM0/0       1        2      0/41       0/2                ESTABLISHED
ATM0/0       2        3      0/42       0/3                DISCOVERY
ATM0/0       3        4      0/43       0/4                RESYNC-STARTING
ATM0/0       4        5      0/44       0/5                RESYNC-STOPPING
ATM0/0       5        6      0/45       0/6                RESYNC-UNDERWAY
ATM0/0       6        7      0/46       0/7                UNKNOWN
```

```
ATM0/0       7        8      0/47       0/8               UNKNOWN
ATM0/0       8        9      0/48       0/9               CLOSING
ATM0/0       9        10     0/49       0/10              ESTABLISHED
ATM0/0       10       11     0/50       0/11              ESTABLISHED
ATM0/0       11       12     0/51       0/12              ESTABLISHED
```

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

Table 17: show controllers vsi session Field Descriptions

Field	Description
Interface	Control interface name.
Session	Session number (from 0 to <*n* -1>), where *n* is the number of sessions on the control interface.
VCD	Virtual circuit descriptor (virtual circuit number). Identifies the VC carrying the VSI protocol between the primary and the subordinate for this session.
VPI/VCI	Virtual path identifier or virtual channel identifier (for the VC used for this session).
Switch/Slave Ids	Switch and subordinate identifiers supplied by the switch.
Session State	Indicates the status of the session between the primary VC and the subordinate. • ESTABLISHED is the fully operational steady state. • UNKNOWN indicates that the subordinate is not responding. Other possible states include the following: • CONFIGURING • RESYNC-STARTING • RESYNC-UNDERWAY • RESYNC-ENDING • DISCOVERY • SHUTDOWN-STARTING • SHUTDOWN-ENDING • INACTIVE

In the following example, session number 9 is specified with the **show controllers vsi session** command:

```
Router# show controllers vsi session 9
Interface:            ATM1/0        Session number:       9
VCD:                  10            VPI/VCI:              0/49
Switch type:          BPX           Switch id:            0
Controller id:        1             Slave id:             10
Keepalive timer:      15            Powerup session id:   0x0000000A
Cfg/act retry timer:  8/8           Active session id:    0x0000000A
Max retries:          10            Ctrl port log intf:   0x000A0100
```

```
Trap window:          50            Max/actual cmd wndw:  21/21
Trap filter:          all           Max checksums:        19
Current VSI version:  1             Min/max VSI version:  1/1
Messages sent:        2502          Inter-slave timer:    4.000
Messages received:    2502          Messages outstanding: 0
```

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

Table 18: show controllers vsi session Field Descriptions

Field	Description
Interface	Name of the control interface on which this session is configured.
Session number	A number from 0 to <*n* -1>, where *n* is the number of subordinates. Configured on the MPLS LSC with the *slaves* option of the **tag-control-protocol vsi** command.
VCD	Virtual circuit descriptor (virtual circuit number). Identifies the VC that carries VSI protocol messages for this session.
VPI/VCI	Virtual path identifier or virtual channel identifier for the VC used for this session.
Switch type	Switch device (for example, the BPX).
Switch id	Switch identifier (supplied by the switch).
Controller id	Controller identifier. Configured on the LSC, and on the switch, with the **id** option of the **tag-control-protocol vsi** command.
Slave id	The subordinate identifier (supplied by the switch).
Keepalive timer	The primary VSI keepalive timeout period (in seconds). Configured on the MPLS LSC through the **keepalive** option of the **tag-control-protocol-vsi** command. If no valid message is received by the MPLS LSC within this time period, it sends a keepalive message to the subordinate.
Powerup session id	The session ID (supplied by the subordinate) used at powerup time.
Cfg/act retry timer	Configured and actual message retry timeout period (in seconds). If no response is received for a command sent by the primary VC within the actual retry timeout period, the message is re-sent. This applies to most message transmissions. The configured retry timeout value is specified through the **retry** option of the **tag-control-protocol vsi** command. The actual retry timeout value is the larger of the configured value and the minimum retry timeout value permitted by the switch.
Active session id	The session ID (supplied by the subordinate) for the currently active session.
Max retries	Maximum number of times that a particular command transmission will be retried by the primary VC. That is, a message may be sent up to <max_retries+1> times. Configured on the MPLS LSC through the **retry** option of the **tag-control-protocol vsi** command.
Ctrl port log intf	Logical interface identifier for the control port, as supplied by the switch.
Trap window	Maximum number of outstanding trap messages permitted by the primary VC. This is advertised, but not enforced, by the LSC.

Field	Description
Max/actual cmd wndw	Maximum command window is the maximum number of outstanding (that is, unacknowledged) commands that may be sent by the primary VC before waiting for acknowledgments. This number is communicated to the primary by the subordinate. The command window is the maximum number of outstanding commands that are permitted by the primary VC, before it waits for acknowledgments. This is always less than the maximum command window.
Trap filter	This is always "all" for the LSC, indicating that it wants to receive all traps from the subordinate. This is communicated to the subordinate by the primary server.
Max checksums	The maximum number of checksum blocks supported by the subordinate.
Current VSI version	VSI protocol version currently in use by the primary VC for this session.
Min/max VSI version	The minimum and maximum VSI versions supported by the subordinate, as last reported by the subordinate. If both are zero, the subordinate has not yet responded to the primary server.
Messages sent	Number of commands sent to the subordinate.
Inter-slave timer	Timeout value associated by the subordinate for messages it sends to other subordinates. On a VSI-controlled switch with a distributed subordinate implementation (such as the BPX), VSI messages may be sent between subordinates to complete their processing. For the MPLS LSC VSI implementation to function properly, the value of its retry timer is forced to be at least two times the value of the interslave timer. (See "Cfg/act retry timer" in this table.)
Messages received	Number of responses and traps received by the primary VC from the subordinate for this session.
Messages outstanding	The current number of outstanding messages (that is, commands sent by the primary VC for which responses have not yet been received).

Related Commands

Command	Description
tag-control-protocol vsi	Configures the use of VSI on a control port.

show controllers vsi status

Note Effective with Cisco IOS Release 12.4(20)T, the **show controllers vsi status** command is not available in Cisco IOS software.

To display a one-line summary of each Virtual Switch Interface (VSI)-controlled interface, use the **show controllers vsi status** command in user EXEC or in privileged EXEC mode .

show controllers vsi status

Syntax Description

This command has no arguments or keywords.

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

If an interface is discovered by the LSC, but no extended Multiprotocol Label Switching (MPLS) ATM interface is associated with it through the **extended-port** command, then the interface name is marked <unknown>, and interface status is marked n/a.

Examples

The following is sample output from the **show controllers vsi status** command:

```
Router# show controllers vsi status
Interface Name                  IF Status   IFC State  Physical Descriptor
switch control port                  n/a      ACTIVE  12.1.0
XTagATM0                              up      ACTIVE  12.2.0
XTagATM1                              up      ACTIVE  12.3.0
<unknown>                            n/a  FAILED-EXT  12.4.0
```

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

Table 19: show controllers vsi status Field Descriptions

Field	Description
Interface Name	The (Cisco IOS) interface name.
IF Status	Overall interface status. Can be “up,” “down,” or “administratively down.”

Field	Description
IFC State	The operational state of the interface, according to the switch. Can be one of the following: • FAILED-EXT (that is, an external alarm) • FAILED-INT (indicates the inability of the MPLS LSC to communicate with the VSI slave controlling the interface, or another internal failure) • REMOVED (administratively removed from the switch)
Physical Descriptor	A string learned from the switch that identifies the interface.

show controllers vsi traffic

Note Effective with Cisco IOS Release 12.4(20)T, the **show controllers vsi traffic** command is not available in Cisco IOS software.

To display traffic information about Virtual Switch Interface (VSI)-controlled interfaces, VSI sessions, or virtual circuits (VCs) on VSI-controlled interfaces, use the **show controllers vsi traffic** command in user EXEC or privileged EXEC mode.

show controllers vsi traffic {**descriptor** *descriptor* | **session** *session-number* | **vc** [**descriptor** *descriptor* [*vpi vci*]]}

Syntax Description

descriptor *descriptor*	Displays traffic statistics for the specified descriptor.
session *session-number*	Displays traffic statistics for the specified session.
vc	Displays traffic statistics for the specified VC.
descriptor descriptor *descriptor*	Specifies the name of the physical descriptor.
vpi	Virtual path identifier (0 to 4095).
vci	Virtual circuit identifier (0 to 65535).

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	The VPI range of values was extended to 4095.
12.4(20)T	This command was removed.

Usage Guidelines

If none of the keywords is specified, traffic for all interfaces is displayed. You can specify a single interface by its (switch-supplied) physical descriptor. For the BPX switch, the physical descriptor has the form

slot.port. 0

If a session number is specified, the output displays VSI protocol traffic by message type. The VC traffic display is also displayed by the **show xmplsatm vc cross-connect traffic descriptor** command.

Examples

The following is sample output from the **show controllers vsi traffic** command:

```
Router# show controllers vsi traffic
Phys desc: 10.1.0
```

```
Interface: switch control port
IF status: n/a
Rx cells: 304250             Rx cells discarded: 0
Tx cells: 361186             Tx cells discarded: 0
Rx header errors: 4294967254 Rx invalid addresses (per card): 80360
Last invalid address: 0/53

Phys desc: 10.2.0
Interface: XTagATM0
IF status: up
Rx cells: 202637             Rx cells discarded: 0
Tx cells: 194979             Tx cells discarded: 0
Rx header errors: 4294967258 Rx invalid addresses (per card): 80385
Last invalid address: 0/32

Phys desc: 10.3.0
Interface: XTagATM1
IF status: up
Rx cells: 182295             Rx cells discarded: 0
Tx cells: 136369             Tx cells discarded: 0
Rx header errors: 4294967262 Rx invalid addresses (per card): 80372
Last invalid address: 0/32
```

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

Table 20: show controllers vsi traffic Field Descriptions

Field	Description
Phys desc	Physical descriptor of the interface.
Interface	The Cisco (IOS) interface name.
Rx cells	Number of cells received on the interface.
Tx cells	Number of cells transmitted on the interface.
Rx cells discarded	Number of cells received on the interface that were discarded due to traffic management.
Tx cells discarded	Number of cells that could not be transmitted on the interface due to traffic management and which were therefore discarded.
Rx header errors	Number of cells that were discarded due to ATM header errors.
Rx invalid addresses	Number of cells received with an invalid address (that is, an unexpected VPI/VCI combination). With the Cisco BPX switch, this count is of all such cells received on all interfaces in the port group of this interface.
Last invalid address	Number of cells received on this interface with ATM cell header errors.

The following sample output is displayed when you enter the **show controllers vsi traffic session 9** command:

```
Router# show controllers vsi traffic session 9
                        Sent                                Received
Sw Get Cnfg Cmd:         3656       Sw Get Cnfg Rsp:         3656
Sw Cnfg Trap Rsp:        0          Sw Cnfg Trap:            0
Sw Set Cnfg Cmd:         1          Sw Set Cnfg Rsp:         1
```

```
Sw Start Resync Cmd:      1          Sw Start Resync Rsp:      1
Sw End Resync Cmd:        1          Sw End Resync Rsp:        1
Ifc Getmore Cnfg Cmd:     1          Ifc Getmore Cnfg Rsp:     1
Ifc Cnfg Trap Rsp:        4          Ifc Cnfg Trap:            4
Ifc Get Stats Cmd:        8          Ifc Get Stats Rsp:        8
Conn Cmt Cmd:             73         Conn Cmt Rsp:             73
Conn Del Cmd:             50         Conn Del Rsp:             0
Conn Get Stats Cmd:       0          Conn Get Stats Rsp:       0
Conn Cnfg Trap Rsp:       0          Conn Cnfg Trap:           0
Conn Bulk Clr Stats Cmd: 0           Conn Bulk Clr Stats Rsp: 0
Gen Err Rsp:              0          Gen Err Rsp:              0
unused:                   0          unused:                   0
unknown:                  0          unknown:                  0
TOTAL:                    3795       TOTAL:                    3795
```

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

Table 21: show controllers vsi traffic session Field Descriptions

Field	Description
Sw Get Cnfg Cmd	Number of VSI “get switch configuration command” messages sent.
Sw Cnfg Trap Rsp	Number of VSI “switch configuration asynchronous trap response” messages sent.
Sw Set Cnfg Cmd	Number of VSI “set switch configuration command” messages sent.
Sw Start Resync Cmd	Number of VSI “set resynchronization start command” messages sent.
Sw End Resync Cmd	Number of VSI “set resynchronization end command” messages sent.
Ifc Getmore Cnfg Cmd	Number of VSI “get more interfaces configuration command” messages sent.
Ifc Cnfg Trap Rsp	Number of VSI “interface configuration asynchronous trap response” messages sent.
Ifc Get Stats Cmd	Number of VSI “get interface statistics command” messages sent.
Conn Cmt Cmd	Number of VSI “set connection committed command” messages sent.
Conn Del Cmd	Number of VSI “delete connection command” messages sent.
Conn Get Stats Cmd	Number of VSI “get connection statistics command” messages sent.
Conn Cnfg Trap Rsp	Number of VSI “connection configuration asynchronous trap response” messages sent.
Conn Bulk Clr Stats Cmd	Number of VSI “bulk clear connection statistics command” messages sent.
Gen Err Rsp	Number of VSI “generic error response” messages sent or received.
Sw Get Cnfg Rsp	Number of VSI “get connection configuration command response” messages received.
Sw Cnfg Trap	Number of VSI “switch configuration asynchronous trap” messages received.
Sw Set Cnfg Rsp	Number of VSI “set switch configuration response” messages received.

Field	Description
Sw Start Resync Rsp	Number of VSI “set resynchronization start response” messages received.
Sw End Resync Rsp	Number of VSI “set resynchronization end response” messages received.
Ifc Getmore Cnfg Rsp	Number of VSI “get more interfaces configuration response” messages received.
Ifc Cnfg Trap	Number of VSI “interface configuration asynchronous trap” messages received.
Ifc Get Stats Rsp	Number of VSI “get interface statistics response” messages received.
Conn Cmt Rsp	Number of VSI “set connection committed response” messages received.
Conn Del Rsp	Number of VSI “delete connection response” messages received.
Conn Get Stats Rsp	Number of VSI “get connection statistics response” messages received.
Conn Cnfg Trap	Number of VSI “connection configuration asynchronous trap” messages received.
Conn Bulk Clr Stats Rsp	Number of VSI “bulk clear connection statistics response” messages received.
unused, unknown	“Unused” messages are those whose function codes are recognized as being part of the VSI protocol, but which are not used by the MPLS LSC and, consequently, are not expected to be received or sent. “Unknown” messages have function codes that the MPLS LSC does not recognize as part of the VSI protocol.
TOTAL	Total number of VSI messages sent or received.

show controllers xtagatm

Note Effective with Cisco IOS Release 12.4(20)T, the **show controllers xtagatm** command is not available in Cisco IOS software.

To display information about an extended Multiprotocol Label Switching (MPLS) ATM interface controlled through the Virtual Switch Interface (VSI) protocol (or, if an interface is not specified, to display information about all extended MPLS ATM interfaces controlled through the VSI protocol), use the **show controllers xtagatm** command in user EXEC or privileged EXEC mode.

show controllers xtagatm *if-number*

Syntax Description

if-number	Specifies the interface number.

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

Per-interface information includes the following:

- Interface name
- Physical descriptor
- Interface status
- Physical interface state (supplied by the switch)
- Acceptable VPI and VCI ranges
- Maximum cell rate
- Available cell rate (forward/backward)
- Available channels

Similar information appears if you enter the **show controllers vsi descriptor** command. However, you must specify an interface by its (switch-supplied) physical descriptor, instead of its Cisco IOS interface name. For the Cisco BPX switch, the physical descriptor has the form *slot.port.0*.

Examples

In this example, the sample output is from the **show controllers xtagatm** command specifying interface 0:

```
Router# show controllers xtagatm 0
Interface XTagATM0 is up
Hardware is Tag-Controlled ATM Port (on BPX switch BPX-VSI1)
Control interface ATM1/0 is up
Physical descriptor is 10.2.0
Logical interface 0x000A0200 (0.10.2.0)
Oper state ACTIVE, admin state UP
VPI range 1-255, VCI range 32-65535
VPI is not translated at end of link
Tag control VC need not be strictly in VPI/VCI range
Available channels: ingress 30, egress 30
Maximum cell rate: ingress 300000, egress 300000
Available cell rate: ingress 300000, egress 300000
Endpoints in use: ingress 7, egress 8, ingress/egress 1
Rx cells 134747
rx cells discarded 0, rx header errors 0
rx invalid addresses (per card): 52994
last invalid address 0/32
Tx cells 132564
tx cells discarded: 0
```

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

Table 22: show controllers xtagatm Field Descriptions

Field	Description
Interface XTagATM0 is up	Indicates the overall status of the interface. May be “up,” “down,” or “administratively down.”
Hardware is Tag-Controlled ATM Port	Indicates the hardware type. If the XTagATM was successfully associated with a switch port, a description of the form (on <switch_type> switch <name>) follows this field, where <switch_type> indicates the type of switch (for example, BPX), and the name is an identifying string learned from the switch. If the XTagATM interface was not bound to a switch interface (with the **extended-port** interface configuration command), then the label “Not bound to a control interface and switch port” appears. If the interface has been bound, but the target switch interface has not been discovered by the LSC, then the label “Bound to undiscovered switch port (id <number>)” appears, where <number> is the logical interface ID in hexadecimal notation.
Control interface ATM1/0 is up	Indicates that the XTagATM interface was bound (with the **extended-port** interface configuration command) to the primary VSI whose control interface is ATM1/0 and that this control interface is up.
Physical descriptor is...	A string identifying the interface that was learned from the switch.
Logical interface	This 32-bit entity, learned from the switch, uniquely identifies the interface. It appears in both hexadecimal and dotted quad notation.

Field	Description
Oper state	Operational state of the interface, according to the switch. Can be one of the following: • ACTIVE • FAILED_EXT (that is, an external alarm) • FAILED_INT (indicates the inability of the MPLS LSC to communicate with the VSI subordinate controlling the interface, or another internal failure) • REMOVED (administratively removed from the switch)
admin state	Administrative state of the interface, according to the switch--either “Up” or “Down.”
VPI range 1 to 255	Indicates the allowable VPI range for the interface that was configured on the switch.
VCI range 32 to 65535	Indicates the allowable VCI range for the interface that was configured on, or determined by, the switch.
LSC control VC need not be strictly in VPI or VCI range	Indicates that the label control VC does not need to be within the range specified by VPI range, but may be on VPI 0 instead.
Available channels	Indicates the number of channels (endpoints) that are currently free to be used for cross-connects.
Maximum cell rate	Maximum cell rate for the interface, which was configured on the switch.
Available cell rate	Cell rate that is currently available for new cross-connects on the interface.
Endpoints in use	Number of endpoints (channels) in use on the interface, broken down by anticipated traffic flow, as follows: • Ingress--Endpoints carry traffic into the switch • Egress--Endpoints carry traffic away from the switch • Ingress/egress--Endpoints carry traffic in both directions
Rx cells	Number of cells received on the interface.
rx cells discarded	Number of cells received on the interface that were discarded due to traffic management actions (rx header errors).
rx header errors	Number of cells received on the interface with cell header errors.
rx invalid addresses (per card)	Number of cells received with invalid addresses (that is, unexpected VPI or VCI.). On the BPX, this counter is maintained per port group (not per interface).
last invalid address	Address of the last cell received on the interface with an invalid address (for example, 0/32).

Field	Description
Tx cells	Number of cells sent from the interface.
tx cells discarded	Number of cells intended for transmission from the interface that were discarded due to traffic management actions.

Related Commands

Command	Description
show controllers vsi descriptor	Displays information about a switch interface discovered by the MPLS LSC through the VSI.

show interface pseudowire

To display information about the pseudowire interface, use the **show interface pseudowire** command in privileged EXEC mode.

show interface pseudowire *number*

Syntax Description

number	Interface pseudowire number.

Command Modes

Privileged EXEC (#)

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.

Examples

The following is sample output from the **show interface pseudowire** command. The output fields are self-explanatory.

```
Device# show interface pseudowire 100

pseudowire 100 is up
    Description: L2VPN Pseudowire
    MTU 1500 bytes, BW 1000000 Kbit
    Encapsulation: MPLS
                   Peer Address: 10.0.0.1, VC ID: 10
    RX
      0 unicast packets  0 multicast packets
      0 input packets  0 bit rate  0 packet rate
    TX
      0 unicast packets  0 multicast packets
      0 output packets  0 bits/sec  0 packets/sec
```

show interface tunnel configuration

To display the configuration of a mesh tunnel interface, use the **show interface tunnel configuration** command in privileged EXEC mode.

show interface tunnel *num* **configuration**

Syntax Description

num	Number of the mesh tunnel for which you want to display configuration 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.

Use this command to show the running configuration of the mesh tunnel interface.

Examples

The following command output shows the configuration of mesh tunnel interface 5:

```
Router# show interface tunnel 5 configuration
interface tunnel 5
 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 23: show interface tunnel configuration 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.
no ip directed-broadcast	Indicates that no IP broadcast addresses are used for the mesh tunnel interface.
no keepalive	Indicates that no keepalives are set for the mesh tunnel interface.

Field	Description
tunnel destination access-list 1	Indicates that access-list 1 is the access list that the template interface will use for obtaining the mesh tunnel interface destination address.
tunnel mode mpls traffic-eng	Indicates that the mode of the mesh tunnel 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
tunnel destination access-list	Specifies the access list that the template interface will use for obtaining the mesh tunnel interface destination address.

show interface virtual-ethernet

To display status and information about a virtual Ethernet interface, use the **show interface virtual-ethernet** command in user privileged EXEC mode.

show interface virtual-ethernet *num* [{**switchport** | **transport**}]

Syntax Description

num	The number of the virtual interface.
switchport	Show virtual Ethernet instance switchport information.
transport	Show virtual Ethernet instance transport information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following example shows transport information for virtual Ethernet interface 1:

```
Router# show interface virtual-ethernet 1 transport

VLAN Transport type for the V-E instance: VPLS Mesh
  11 VPLS domains provisioned for this V-E instance
  VFI names : VFI[45-55]_
```

The following example shows switchport information for virtual Ethernet interface 1:

```
Router# show interface virtual-ethernet 1 switchport
Name: VE1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: up
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Trunking VLANs Enabled: 100,200
```

Related Commands

Command	Description
interface virtual-ethernet	Creates a virtual Ethernet interface.

show interface xtagatm

Note Effective with Cisco IOS Release 12.4(20)T, the **show interface xtagatm** command is not available in Cisco IOS software.

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

if-number	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.
12.4(20)T	This command was removed.

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 ½55, rxload ½55
 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 ½55, rxload ½55
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
```

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

Table 24: 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).

Field	Description
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.
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.
n 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.

Field	Description
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.
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 terminate counts. Other input-related errors can also increment the count, so that this sum may not balance with other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus. A high number of CRCs is usually the result of traffic collisions or a station sending bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
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.

Field	Description
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.
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 l2vpn

To display Layer 2 Virtual Private Network (L2VPN) address family information from the Border Gateway Protocol (BGP) table, use the **show ip bgp l2vpn** command in user EXEC or privileged EXEC mode.

With BGP show Command Argument
show ip bgp l2vpn vpls {**all** | **neighbors***neighbor address* | **sso** | {**summary** | **internal**} | [{**summary** | [{**slow**}] | **ve-id** *id-value*}] | {**block-offset** | [{*value*}]} | **rd** {*route-distinguisher* | [{**ve-id** | {**block-offset** | [{*value*}]}}]}} [{*bgp-keyword*}]

With IP Prefix and Mask Length Syntax
show ip bgp l2vpn vpls {**all** | **rd** *route-distinguisher*} [*ip-prefix/length* [{[**bestpath**]}] [**longer-prefixes** [{[**injected**]}]] [{[**multipaths**]}] [{**shorter-prefixes** [{[*mask-length*]}]}] [{[**subnets**]}]]

With Network Address Syntax
show ip bgp l2vpn vpls {**all** | **rd** *route-distinguisher*} [*network-address* [{*mask* | **bestpath** | **multipaths**}] [**bestpath**] [**longer-prefixes** [**injected**]] [**multipaths**] [**shorter-prefixes** [*mask-length*]] [**subnets**]]

Syntax Description

vpls	Displays L2VPN address family database information for the Virtual Private LAN Service (VPLS) subsequent address family identifier (SAFI).
all	Displays the complete L2VPN database.
rd *route-distinguisher*	Displays prefixes that match the specified route distinguisher.
ve-id *id-value*	(Optional) Displays the target VPLS Endpoint (VE) ID and ID value.
summary	(Optional) Displays a summary of BGP neighbor status.
slow	(Optional) Displays a summary of slow-peer status.
block-offset *value*	Displays the target block-offset value.
bgp-keyword	(Optional) Argument representing a **show ip bgp** command keyword that can be added to this command. See the table below.
ip-prefix/length	(Optional) The IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
bestpath	(Optional) Displays the best path for the specified prefix.
longer-prefixes	(Optional) Displays the route and more specific routes.
injected	(Optional) Displays more specific routes that were injected because of the specified prefix.
multipaths	(Optional) Displays the multipaths for the specified prefix.
shorter-prefixes	(Optional) Displays the less specific routes.
mask-length	(Optional) The length of the mask as a number in the range from 0 to 32. Prefixes longer than the specified mask length are displayed.

subnets	(Optional) Displays the subnet routes for the specified prefix.
network-address	(Optional) The IP address of a network in the BGP routing table.
mask	(Optional) The mask of the network address, in dotted decimal format.

Command Default

If no arguments or keywords are specified, this command displays the complete L2VPN database.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE2.6	This command was integrated into Cisco IOS XE Release 2.6.
Cisco IOS XE3.8S	This command was modified. RFC4761 is fully supported in Cisco IOS XE Release 3.8S.

Usage Guidelines

The table below displays optional **show ip bgp** command keywords that can be configured with the **show ip bgp l2vpn** command. Replace the *bgp-keyword* argument with the appropriate keyword from the table. For more details about each command in its **show ip bgp** *bgp-keyword* form, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols,* Release 12.2.

Table 25: Optional show ip bgp Command Keywords and Descriptions

Keyword	Description
community	Displays routes that match a specified community.
community-list	Displays routes that match a specified community list.
dampening	Displays paths suppressed because of dampening (BGP route from peer is up and down).
extcommunity-list	Displays routes that match a specified extcommunity list.
filter-list	Displays routes that conform to the filter list.
inconsistent-as	Displays only routes that have inconsistent autonomous systems of origin.
neighbors	Displays details about TCP and BGP neighbor connections.
oer-paths	Displays all OER-managed path information.
paths [*regexp*]	Displays autonomous system path information. If the optional *regexp* argument is entered, the autonomous system paths that are displayed match the autonomous system path regular expression.
peer-group	Displays information about peer groups.

Keyword	Description
pending-prefixes	Displays prefixes that are pending deletion.
prefix-list	Displays routes that match a specified prefix list.
quote-regexp	Displays routes that match the quoted autonomous system path regular expression.
regexp	Displays routes that match the autonomous system path regular expression.
replication	Displays the replication status update groups.
route-map	Displays routes that match the specified route map.
rt-filter-list	Displays the specified inbound route target filter list.
summary	Displays a summary of BGP neighbor status.
update-group	Displays information on update groups.
internal	Displays information on prefixes maintained by BGP at standby RP.

Examples

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **all** keywords are used to display the complete L2VPN database:

```
Device# show ip bgp l2vpn vpls all

BGP table version is 5, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 45000:100
*> 45000:100:172.17.1.1/96
                    0.0.0.0                              32768 ?
*>i45000:100:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
Route Distinguisher: 45000:200
*> 45000:200:172.17.1.1/96
                    0.0.0.0                              32768 ?
*>i45000:200:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
```

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

Table 26: show ip bgp l2vpn vpls all Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is a historical entry. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session. • r—The table entry failed to install in the routing information base (RIB) table. • S—The table entry is Stale (old). This entry is useful in BGP graceful restart situations.
Origin codes	Origin of the entry. The origin code is displayed at the end of each line in the table. It can be one of the following values: • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
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.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** command in route-map configuration mode. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.
Route Distinguisher	Route distinguisher that identifies a set of routing and forwarding tables used in virtual private networks.

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **all** keywords are used to display information about all VPLS BGP signaling prefixes (including local generated and received from remote):

```
Device#show ip bgp l2vpn vpls all

BGP table version is 14743, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network               Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65000:1
*>i 65000:1:VEID-3:Blk-1/136
                      3.3.3.3                  0    100       0 ?
*> 65000:1:VEID-4:Blk-1/136
                      0.0.0.0                            32768 ?
*>i 65000:1:VEID-5:Blk-1/136
                      2.2.2.2                  0    100       0 ?
*>i 65000:1:VEID-6:Blk-1/136
                      4.4.4.4                  0    100       0 ?
Route Distinguisher: 65000:2
*> 65000:2:VEID-20:Blk-20/136
                      0.0.0.0                            32768 ?
*>i 65000:2:VEID-21:Blk-20/136
                      2.2.2.2                  0    100       0 ?
*>i 65000:2:VEID-22:Blk-20/136
                      3.3.3.3                  0    100       0 ?
*>i 65000:2:VEID-23:Blk-20/136
                      4.4.4.4                  0    100       0 ?
```

The following example shows output for the **show ip bgp l2vpn** command when the **vpls**, **all** and **summary** keywords are used to display information about the L2VPN VPLS address family:

```
Device# show ip bgp l2vpn vpls all summary

BGP router identifier 10.1.1.1, local AS number 65000
BGP table version is 14743, main routing table version
14743
6552 network entries using 1677312 bytes of memory
6552 path entries using 838656 bytes of memory
3276/3276 BGP path/bestpath attribute entries using
760032 bytes of memory
1638 BGP extended community entries using 65520 bytes of
memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3341520 total bytes of memory
BGP activity 9828/3276 prefixes, 9828/3276 paths, scan
interval 60 secs
Neighbor       V          AS  MsgRcvd  MsgSent  TblVer  InQ OutQ  Up/Down
State/PfxRcd
10.2.2.2       4        65000   90518   90507    14743   0     0  8w0d     1638
10.3.3.3       4        65000    4901    4895    14743   0     0  2d01h    1638
10.4.4.4       4        65000    4903    4895    14743   0     0  2d01h    1638
```

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **rd** *rd* keywords are used to display information about all VPLS BGP signaling prefixes with the specified rd, i.e. the same VPLS instance:

```
Device# show ip bgp l2vpn vpls rd 65000:3

BGP table version is 14743, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
```

```
             x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65000:3
*> 65000:3:VEID-30:Blk-30/136
                      0.0.0.0                              32768 ?
*>i 65000:3:VEID-31:Blk-30/136
                      2.2.2.2                  0  100        0 ?
*>i 65000:3:VEID-32:Blk-30/136
                      3.3.3.3                  0  100        0 ?
*>i 65000:3:VEID-33:Blk-30/136
                      4.4.4.4                  0  100        0 ?
```

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **rd** keywords are used to display the L2VPN information that matches the route distinguisher 45000:100. Note that the information displayed is a subset of the information displayed using the **all** keyword.

```
Device# show ip bgp l2vpn vpls rd 45000:100

BGP table version is 5, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 45000:100
*> 45000:100:172.17.1.1/96
                    0.0.0.0                            32768 ?
*>i45000:100:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
```

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **all** keywords are used to display information about an individual prefix:

```
Device# show ip bgp l2vpn vpls all ve-id 31 block 30

BGP routing table entry for 65000:3:VEID-31:Blk-30/136, version 11
Paths: (1 available, best #1, table L2VPN-VPLS-BGP-Table)
   Not advertised to any peer
   Refresh Epoch 2
   Local
     2.2.2.2 (metric 2) from 2.2.2.2 (2.2.2.2)
       Origin incomplete, metric 0, localpref 100, valid, internal, best
       AGI version(0), VE Block Size(10) Label Base(16596)
       Extended Community: RT:65000:3 L2VPN L2:0x0:MTU-1500
       rx pathid: 0, tx pathid: 0x0
                0    100      0 ?
```

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning information.
show bgp l2vpn vpls	Displays L2VPN VPLS address family information from the BGP table.

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 privileged EXEC mode.

show ip bgp labels

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
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.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to display eBGP labels associated with an Autonomous System Boundary Router (ASBR).

This command displays labels for BGP routes in the default table only. To display labels in the Virtual Private Network (VPN) routing and forwarding (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 an ASBR using BGP as a label distribution protocol:

```
Router# show ip bgp labels
Network          Next Hop         In Label/Out Label
10.3.0.0/16       0.0.0.0          imp-null/exp-null
10.15.15.15/32   10.15.15.15      18/exp-null
10.16.16.16/32   0.0.0.0          imp-null/exp-null
10.17.17.17/32   10.0.0.1         20/exp-null
10.18.18.18/32   10.0.0.1         24/31
10.18.18.18/32   10.0.0.1         24/33
```

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

Table 27: show ip bgp labels Field Descriptions

Field	Description
Network	Displays the network address from the eBGP table.
Next Hop	Specifies the eBGP 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 neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the **show ip bgp neighbors** command in user or privileged EXEC mode.

show ip bgp [{**ipv4** {**multicast** | **unicast**} | **vpnv4 all** | **vpnv6 unicast all**}] **neighbors** [{**slow** *ip-address* | *ipv6-address* [{**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **policy** [**detail**] | **received prefix-filter** | **received-routes** | **routes**}] | **include Fall over** }]

Syntax Description

ipv4	(Optional) Displays peers in the IPv4 address family.
multicast	(Optional) Specifies IPv4 multicast address prefixes.
unicast	(Optional) Specifies IPv4 unicast address prefixes.
vpnv4 all	(Optional) Displays peers in the VPNv4 address family.
vpnv6 unicast all	(Optional) Displays peers in the VPNv6 address family.
slow	(Optional) Displays information about dynamically configured slow peers.
ip-address	(Optional) IP address of the IPv4 neighbor. If this argument is omitted, information about all neighbors is displayed.
ipv6-address	(Optional) IP address of the IPv6 neighbor.
advertised-routes	(Optional) Displays all routes that have been advertised to neighbors.
dampened-routes	(Optional) Displays the dampened routes received from the specified neighbor.
flap-statistics	(Optional) Displays the flap statistics of the routes learned from the specified neighbor (for external BGP peers only).
paths *reg-exp*	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
policy	(Optional) Displays the policies applied to this neighbor per address family.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and autonomous system path filter lists.
received prefix-filter	(Optional) Displays the prefix list (outbound route filter [ORF]) sent from the specified neighbor.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the **received-routes** keyword.

include Fall over	(Optional) Displays all fallover with maximum-metric that is configured for the neighbor.

Command Default

The output of this command displays information for all neighbors.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Mainline and T Release	Modification
10.0	This command was introduced.
11.2	This command was modified. The **received-routes** keyword was added.
12.2(4)T	This command was modified. The **received** and **prefix-filter** keywords were added.
12.2(15)T	This command was modified. Support for the display of BGP graceful restart capability information was added.
12.3(7)T	This command was modified. The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.4(4)T	This command was modified. Support for the display of Bidirectional Forwarding Detection (BFD) information was added.
12.4(11)T	This command was modified. Support for the **policy** and **detail** keywords was added.
12.4(20)T	This command was modified. The output was modified to support BGP TCP path MTU discovery.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.

S Release	Modification
12.0(18)S	This command was modifed. The output was modified to display the no-prepend configuration option.
12.0(21)ST	This command was modifed. The output was modified to display Multiprotocol Label Switching (MPLS) label information.
12.0(22)S	This command was modified. Support for the display of BGP graceful restart capability information was added. Support for the Cisco 12000 series routers (Engine 0 and Engine 2) was also added.
12.0(25)S	This command was modified. The **policy** and **detail** keywords were added.
12.0(27)S	This command was modified. The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.

S Release	Modification
12.0(31)S	This command was modified. Support for the display of BFD information was added.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.2(18)SXE	This command was modified. Support for the display of BFD information 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 modified. The output was modified to support BGP TCP path Maximum Transmission Unit (MTU) discovery.
12.2(33)SRB	This command was modified. Support for the **policy** and **detail** keywords was added.
12.2(33)SXH	This command was modified. Support for displaying BGP dynamic neighbor information was added.
12.2(33)SRC	This command was modified. Support for displaying BGP graceful restart information was added.
12.2(33)SB	This command was modified. Support for displaying BFD and the BGP graceful restart per peer information was added, and support for the **policy** and **detail** keywords was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI1	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)SRE	This command was modified. Support for displaying BGP best external and BGP additional path features information was added. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The **slow** keyword was added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)S	This command was modified. The Layer 2 VPN address family is displayed if graceful restart or nonstop forwarding (NSF) is enabled.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.

S Release	Modification
15.2(4)S	This command was modified and implemented on the Cisco 7200 series router. The configured discard and treat-as-withdraw attributes are displayed, along with counts of incoming Updates with a matching discard attribute or treat-as-withdraw attribute, and number of times a malformed Update is treat-as-withdraw. The capabilities of the neighbor to send and receive additional paths that are advertised or received are added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Cisco IOS XE	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
Cisco IOS XE Release 3.1S	This command was modified. The **slow** keyword was added.
Cisco IOS XE Release 3.6S	This command was modified. Support for displaying BGP BFD multihop and C-bit information was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router and the output modified. The configured discard and treat-as-withdraw attributes are displayed, along with counts of incoming Updates with a matching discard attribute or treat-as-withdraw attribute, and number of times a malformed Update is treat-as-withdraw. The capabilities of the neighbor to send and receive additional paths that are advertised or received are added.
Cisco IOS XE Release 3.8S	This command was modified. In support of the BGP Multi-Cluster ID feature, the cluster ID of a neighbor is displayed if the neighbor is assigned a cluster.
Cisco IOS XE Gibraltar 16.10.1	BGP Peak Prefix Watermark was added to the command output.
Cisco IOS XE Release 17.1.1	This command was modified. The **include Fall over** keyword was added.

Usage Guidelines

Use the **show ip bgp neighbors** command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses

asplain—65538, for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Cisco IOS Releases 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and Later Releases

When BGP neighbors use multiple levels of peer templates, determining which policies are applied to the neighbor can be difficult.

In Cisco IOS Release 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and later releases, the **policy** and **detail** keywords were added to display the inherited policies and the policies configured directly on the specified neighbor. Inherited policies are policies that the neighbor inherits from a peer group or a peer policy template.

Examples

Example output is different for the various keywords available for the **show ip bgp neighbors** command. Examples using the various keywords appear in the following sections.

show ip bgp neighbors: Example

The following example shows output for the BGP neighbor at 10.108.50.2. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
Device# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
```

```
  1 update-group member
                                 Sent       Rcvd
  Prefix activity:               ----       ----
    Prefixes Current:               0          0
    Prefixes Total:                 0          0
    Implicit Withdraw:              0          0
    Explicit Withdraw:              0          0
    Used as bestpath:             n/a          0
    Used as multipath:            n/a          0
                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Total:                                0          0
  Number of NLRIs in the update sent: max 0, min 0
  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539
SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6
Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

The table below describes the significant fields shown in the display. Fields that are preceded by the asterisk character (*) are displayed only when the counter has a nonzero value.

Table 28: show ip bgp neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system number of the neighbor.
local AS 300 no-prepend (not shown in display)	Verifies that the local autonomous system number is not prepended to received external routes. This output supports the hiding of the local autonomous systems when a network administrator is migrating autonomous systems.
internal link	“internal link” is displayed for iBGP neighbors; “external link” is displayed for external BGP (eBGP) neighbors.
BGP version	BGP version being used to communicate with the remote router.

Field	Description
remote router ID	IP address of the neighbor.
BGP state	Finite state machine (FSM) stage of session negotiation.
up for	Time, in hh:mm:ss, that the underlying TCP connection has been in existence.
Last read	Time, in hh:mm:ss, since BGP last received a message from this neighbor.
last write	Time, in hh:mm:ss, since BGP last sent a message to this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor. "advertised and received" is displayed when a capability is successfully exchanged between two routers.
Route refresh	Status of the route refresh capability.
MPLS Label capability	Indicates that MPLS labels are both sent and received by the eBGP peer.
Graceful Restart Capability	Status of the graceful restart capability.
Address family IPv4 Unicast	IP Version 4 unicast-specific properties of this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.
Revd	Total number of received messages.
Opens	Number of open messages sent and received.
Notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.

Field	Description
For address family:	Address family to which the following fields refer.
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
neighbor version	Number used by the software to track prefixes that have been sent and those that need to be sent.
1 update-group member	Number of the update-group member for this address family.
Prefix activity	Prefix statistics for this address family.
Prefixes Current	Number of prefixes accepted for this address family.
Prefixes Total	Total number of received prefixes.
Implicit Withdraw	Number of times that a prefix has been withdrawn and readvertised.
Explicit Withdraw	Number of times that a prefix has been withdrawn because it is no longer feasible.
Used as bestpath	Number of received prefixes installed as best paths.
Used as multipath	Number of received prefixes installed as multipaths.
* Saved (soft-reconfig)	Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a nonzero value.
* History paths	This field is displayed only if the counter has a nonzero value.
* Invalid paths	Number of invalid paths. This field is displayed only if the counter has a nonzero value.
Local Policy Denied Prefixes	Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a nonzero value.
* route-map	Displays inbound and outbound route-map policy denials.
* filter-list	Displays inbound and outbound filter-list policy denials.
* prefix-list	Displays inbound and outbound prefix-list policy denials.
* Ext Community	Displays only outbound extended community policy denials.
* AS_PATH too long	Displays outbound AS_PATH length policy denials.
* AS_PATH loop	Displays outbound AS_PATH loop policy denials.
* AS_PATH confed info	Displays outbound confederation policy denials.
* AS_PATH contains AS 0	Displays outbound denials of autonomous system 0.

Field	Description
* NEXT_HOP Martian	Displays outbound martian denials.
* NEXT_HOP non-local	Displays outbound nonlocal next-hop denials.
* NEXT_HOP is us	Displays outbound next-hop-self denials.
* CLUSTER_LIST loop	Displays outbound cluster-list loop denials.
* ORIGINATOR loop	Displays outbound denials of local originated routes.
* unsuppress-map	Displays inbound denials due to an unsuppress map.
* advertise-map	Displays inbound denials due to an advertise map.
* VPN Imported prefix	Displays inbound denials of VPN prefixes.
* Well-known Community	Displays inbound denials of well-known communities.
* SOO loop	Displays inbound denials due to site-of-origin.
* Bestpath from this peer	Displays inbound denials because the best path came from the local router.
* Suppressed due to dampening	Displays inbound denials because the neighbor or link is in a dampening state.
* Bestpath from iBGP peer	Deploys inbound denials because the best path came from an iBGP neighbor.
* Incorrect RIB for CE	Deploys inbound denials due to RIB errors for a customer edge (CE) router.
* BGP distribute-list	Displays inbound denials due to a distribute list.
Number of NLRIs...	Number of network layer reachability attributes in updates.
Current session network count peaked...	Displays the peak number of networks observed in the current session.
Highest network count observed at...	Displays the peak number of networks observed since startup.
Connections established	Number of times a TCP and BGP connection has been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time, in hh:mm:ss, since this peering session was last reset. The reason for the reset is displayed on this line.
External BGP neighbor may be...	Indicates that the BGP time to live (TTL) security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.

Field	Description
unread input bytes	Number of bytes of packets still to be processed.
Connection is ECN Disabled	Explicit congestion notification status (enabled or disabled).
Local host: 10.108.50.1, Local port: 179	IP address of the local BGP speaker. BGP port number 179.
Foreign host: 10.108.50.2, Foreign port: 42698	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgment hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keepalive packets.
GiveUp	Number of times a packet is dropped due to no acknowledgment.
PmtuAger	Path MTU discovery timer.
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna:	Last transmission sequence number that has not been acknowledged.
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote neighbor.
irs:	Initial packet receive sequence number.
rcvnxt:	Last receive sequence number that has been locally acknowledged.
rcvwnd:	TCP window size of the local host.
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is higher than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.

Field	Description
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Shortest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Longest recorded round-trip timeout.
ACK hold:	Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value:	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.
Rcvd:	Number of received packets.
out of order:	Number of packets received out of sequence.
with data	Number of update packets sent with data.
total data bytes	Total amount of data received, in bytes.
Sent	Number of update packets sent.
Second Congestion	Number of update packets with data sent.
Datagrams: Rcvd	Number of update packets received from a neighbor.
retransmit	Number of packets retransmitted.
fastretransmit	Number of duplicate acknowledgments retransmitted for an out of order segment before the retransmission timer expires.
partialack	Number of retransmissions for partial acknowledgments (transmissions before or without subsequent acknowledgments).
Second Congestion	Number of second retransmissions sent due to congestion.

show ip bgp neighbors (4-Byte Autonomous System Numbers)

The following partial example shows output for several external BGP neighbors in autonomous systems with 4-byte autonomous system numbers, 65536 and 65550. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router# show ip bgp neighbors

BGP neighbor is 192.168.1.2,  remote AS 65536, external link
  BGP version 4, remote router ID 0.0.0.0
```

```
  BGP state = Idle
  Last read 02:03:38, last write 02:03:38, hold time is 120, keepalive interval is 70
seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds
.
.
.
BGP neighbor is 192.168.3.2,  remote AS 65550, external link
 Description: finance
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:48, last write 02:03:48, hold time is 120, keepalive interval is 70
seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds
```

show ip bgp neighbors advertised-routes

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
Device# show ip bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
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
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

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

Table 29: show ip bgp neighbors advertised-routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
local router ID	IP address of the local BGP speaker.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened and will not be advertised to BGP neighbors. • h—The table entry does not contain the best path based on historical information. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session.

Field	Description
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network.
Metric	If shown, this is the value of the interautonomous system metric. This field is not used frequently.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp neighbors check-control-plane-failure

The following is sample output from the **show ip bgp neighbors** command entered with the **check-control-plane-failure** option configured:

```
Device# show ip bgp neighbors 10.10.10.1

BGP neighbor is 10.10.10.1,  remote AS 10, internal link
 Fall over configured for session
 BFD is configured. BFD peer is Up. Using BFD to detect fast fallover (single-hop) with
c-bit check-control-plane-failure.
 Inherits from template cbit-tps for session parameters
  BGP version 4, remote router ID 10.7.7.7
  BGP state = Established, up for 00:03:55
  Last read 00:00:02, last write 00:00:21, hold time is 180, keepalive interval is 60 seconds

  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
```

show ip bgp neighbors paths

The following is sample output from the **show ip bgp neighbors** command entered with the **paths** keyword:

```
Device# show ip bgp neighbors 172.29.232.178 paths 10

Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

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

Table 30: show ip bgp neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	Autonomous system path for that route, followed by the origin code for that route.

show ip bgp neighbors received prefix-filter

The following example shows that a prefix list that filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```
Device# show ip bgp neighbors 192.168.20.72 received prefix-filter

Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

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

Table 31: show ip bgp neighbors received prefix-filter Field Descriptions

Field	Description
Address family	Address family mode in which the prefix filter is received.
ip prefix-list	Prefix list sent from the specified neighbor.

show ip bgp neighbors policy

The following sample output shows the policies applied to the neighbor at 192.168.1.2. The output displays both inherited policies and policies configured on the neighbor device. Inherited polices are policies that the neighbor inherits from a peer group or a peer-policy template.

```
Device# show ip bgp neighbors 192.168.1.2 policy

Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

Cisco IOS Release 12.0(31)S, 12.4(4)T, 12.2(18)SXE, and 12.2(33)SB

The following is sample output from the **show ip bgp neighbors** command that verifies that Bidirectional Forwarding Detection (BFD) is being used to detect fast fallover for the BGP neighbor that is a BFD peer:

```
Device# show ip bgp neighbors

BGP neighbor is 172.16.10.2,  remote AS 45000, external link
.
.
.
 Using BFD to detect fast fallover
```

Cisco IOS Release 12.2(33)SRA and 12.4(20)T

The following is sample output from the **show ip bgp neighbors** command that verifies that BGP TCP path maximum transmission unit (MTU) discovery is enabled for the BGP neighbor at 172.16.1.2:

```
Device# show ip bgp neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

Cisco IOS Release 12.2(33)SXH

The following is sample output from the **show ip bgp neighbors** command that verifies that the neighbor 192.168.3.2 is a member of the peer group group192 and belongs to the subnet range group 192.168.0.0/16, which shows that this BGP neighbor was dynamically created:

```
Device# show ip bgp neighbors 192.168.3.2

BGP neighbor is *192.168.3.2,  remote AS 50000, external link
 Member of peer-group group192 for session parameters
 Belongs to the subnet range group: 192.168.0.0/16
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:06:35
  Last read 00:00:33, last write 00:00:25, hold time is 180, keepalive intervals
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             7          7
    Route Refresh:          0          0
    Total:                  8          8
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
  group192 peer-group member
.
.
.
```

Cisco IOS Releases 12.2(33)SRC and 12.2(33)SB

The following is partial output from the **show ip bgp neighbors** command that verifies the status of the BGP graceful restart capability for the external BGP peer at 192.168.3.2. Graceful restart is shown as disabled for this BGP peer.

```
Device# show ip bgp neighbors 192.168.3.2

BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Inherits from template S2 for session parameters
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:01:41
  Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
.
```

```
.
.
Address tracking is enabled, the RIB does have a route to 192.168.3.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

Cisco IOS Release 15.1(1)S: Example

The following is partial output from the **show ip bgp neighbors** command. For this release, the display includes the Layer 2 VFN address family information if graceful restart or NSF is enabled.

```
Device# show ip bgp neighbors

Load for five secs: 2%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:49:17.034 GMT Wed Sep 22 2010
BGP neighbor is 10.1.1.3,  remote AS 2, internal link
  BGP version 4, remote router ID 10.1.1.3
  BGP state = Established, up for 00:14:32
  Last read 00:00:30, last write 00:00:43, hold time is 180, keepalive interval is 60 seconds

  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Address family L2VPN Vpls: advertised and received
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 120 seconds
      Address families advertised by peer:
        IPv4 Unicast (was not preserved), L2VPN Vpls (was not preserved)
    Multisession Capability:
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                4         16
    Keepalives:            16         16
    Route Refresh:          0          0
    Total:                 21         33
  Default minimum time between advertisement runs is 0 seconds
 For address family: IPv4 Unicast
  Session: 10.1.1.3
  BGP table version 34, neighbor version 34/0
  Output queue size : 0
  Index 1, Advertise bit 0
  1 update-group member
  Slow-peer detection is disabled
  Slow-peer split-update-group dynamic is disabled
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             2         11 (Consumes 572 bytes)
    Prefixes Total:               4         19
    Implicit Withdraw:            2          6
    Explicit Withdraw:            0          2
```

```
    Used as bestpath:             n/a          7
    Used as multipath:            n/a          0
                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    NEXT_HOP is us:                     n/a          1
    Bestpath from this peer:             20        n/a
    Bestpath from iBGP peer:              8        n/a
    Invalid Path:                        10        n/a
    Total:                               38          1
  Number of NLRIs in the update sent: max 2, min 0
  Last detected as dynamic slow peer: never
  Dynamic slow peer recovered: never
 For address family: L2VPN Vpls
  Session: 10.1.1.3
  BGP table version 8, neighbor version 8/0
  Output queue size : 0
  Index 1, Advertise bit 0
  1 update-group member
  Slow-peer detection is disabled
  Slow-peer split-update-group dynamic is disabled
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              1          1 (Consumes 68 bytes)
    Prefixes Total:                2          1
    Implicit Withdraw:             1          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          1
    Used as multipath:           n/a          0
                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Bestpath from this peer:              4        n/a
    Bestpath from iBGP peer:              1        n/a
    Invalid Path:                         2        n/a
    Total:                                7          0
  Number of NLRIs in the update sent: max 1, min 0
  Last detected as dynamic slow peer: never
  Dynamic slow peer recovered: never
  Address tracking is enabled, the RIB does have a route to 10.1.1.3
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is enabled, restart-time 120 seconds, stalepath-time 360 seconds
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Mininum incoming TTL 0, Outgoing TTL 255
Local host: 10.1.1.1, Local port: 179
Foreign host: 10.1.1.3, Foreign port: 48485
Connection tableid (VRF): 0
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0xE750C):
Timer          Starts    Wakeups            Next
Retrans            18          0             0x0
TimeWait            0          0             0x0
AckHold            22         20             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
Linger              0          0             0x0
iss: 3196633674  snduna: 3196634254  sndnxt: 3196634254     sndwnd:  15805
irs: 1633793063  rcvnxt: 1633794411  rcvwnd:      15037  delrcvwnd:   1347
SRTT: 273 ms, RTTO: 490 ms, RTV: 217 ms, KRTT: 0 ms
minRTT: 2 ms, maxRTT: 300 ms, ACK hold: 200 ms
```

```
Status Flags: passive open, gen tcbs
Option Flags: nagle, path mtu capable
Datagrams (max data segment is 1436 bytes):
Rcvd: 42 (out of order: 0), with data: 24, total data bytes: 1347
Sent: 40 (retransmit: 0 fastretransmit: 0),with data: 19, total data bytes: 579
```

BGP Attribute Filter and Enhanced Attribute Error Handling

The following is sample output from the **show ip bgp neighbors** command that indicates the discard attribute values and treat-as-withdraw attribute values configured. It also provides a count of received Updates matching a treat-as-withdraw attribute, a count of received Updates matching a discard attribute, and a count of received malformed Updates that are treat-as-withdraw.

```
Device# show ip bgp vpnv4 all neighbors 10.0.103.1

BGP neighbor is 10.0.103.1,  remote AS 100, internal link
 Path-attribute treat-as-withdraw inbound
 Path-attribute treat-as-withdraw value 128
 Path-attribute treat-as-withdraw 128 in: count 2
 Path-attribute discard 128 inbound
 Path-attribute discard 128 in: count 2

       Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    MALFORM treat as withdraw:            0          1
    Total:                                0          1
```

BGP Additional Paths

The following output indicates that the neighbor is capable of advertising additional paths and sending additional paths it receives. It is also capable of receiving additional paths and advertised paths.

```
Device# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is 60 seconds

  Neighbor capabilities:
    Additional paths Send: advertised and received
    Additional paths Receive: advertised and received
    Route refresh: advertised and received(old & new)
    Graceful Restart Capabilty: advertised and received
    Address family IPv4 Unicast: advertised and received
```

BGP—Multiple Cluster IDs

In the following output, the cluster ID of the neighbor is displayed. (The vertical bar and letter “i” for “include” cause the device to display only lines that include the user's input after the “i”, in this case, “cluster-id.”) The cluster ID displayed is the one directly configured through a neighbor or a template.

```
Device# show ip bgp neighbors 192.168.2.2 | i cluster-id
```

```
 Configured with the cluster-id 192.168.15.6
```

BGP Peak Prefix Watermark

The following sample output shows the peak watermarks and their timestamps displayed for the peak number of route entries per neighbor bases:

```
Device# show ip bgp ipv4 unicast neighbors 11.11.11.11

BGP neighbor is 11.11.11.11, remote AS 1, internal link
BGP version 4, remote router ID 0.0.0.0
BGP state = Idle, down for 00:01:43
Neighbor sessions:
0 active, is not multisession capable (disabled)
Stateful switchover support enabled: NO
Do log neighbor state changes (via global configuration)
Default minimum time between advertisement runs is 0 seconds
For address family: IPv4 Unicast
BGP table version 27, neighbor version 1/27
Output queue size : 0
Index 0, Advertise bit 0

Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled
    Sent Rcvd
Prefix activity:      ---- ----
 Prefixes Current:              0    0
 Prefixes Total:                0    0
 Implicit Withdraw:             0    0
 Explicit Withdraw:             0    0
 Used as bestpath:            n/a    0
 Used as multipath:           n/a    0
 Used as secondary:           n/a    0
                              Outbound Inbound
Local Policy Denied Prefixes: -------- -------
 Total:                                0       0
Number of NLRIs in the update sent: max 2, min 0
Current session network count peaked at 20 entries at 00:00:23 Aug 8 2018 PST (00:01:29.156
ago).
Highest network count observed at 20 entries at 23:55:32 Aug 7 2018 PST (00:06:20.156
ago).
Last detected as dynamic slow peer: never
Dynamic slow peer recovered: never
Refresh Epoch: 1
Last Sent Refresh Start-of-rib: never
Last Sent Refresh End-of-rib: never
Last Received Refresh Start-of-rib: never
Last Received Refresh End-of-rib: never
                                  Sent Rcvd
Refresh activity:                 ---- ----
 Refresh Start-of-RIB                1    0
 Refresh End-of-RIB                  0    0
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.

Command	Description
bgp enhanced-error	Restores the default behavior of treating Update messages that have a malformed attribute as withdrawn, or includes iBGP peers in the Enhanced Attribute Error Handling feature.
neighbor path-attribute discard	Configures the device to discard unwanted Update messages from the specified neighbor that contain a specified path attribute.
neighbor path-attribute treat-as-withdraw	Configures the device to withdraw from the specified neighbor unwanted Update messages that contain a specified attribute.
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
neighbor send-label explicit-null	Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.
router bgp	Configures the BGP routing process.

show ip bgp vpnv4

To display VPN Version 4 (VPNv4) 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*} [{[{*ip-prefix*/*length* [{*mask* | **bestpath** | **multipaths**}] | *network-address* [{*mask* | **bestpath** | **longer-prefixes** | **multipaths** | **shorter-prefixes** | **subnets**}]}] | **cidr-only** | **cluster-ids** | **community** | **community-list** | **dampening** | **extcommunity-list** *extcommunity-list-name* | **filter-list** | **inconsistency nexthop-label** | **inconsistent-as** | **labels** | **neighbors** [{{*ip-addressipv6-address*} [{**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** | **policy** [**detail**] | **received** | **received-routes** | **routes**}] | **slow**}] | **nexthops** | **oer-paths** | **path-attribute** {**discard** | **unknown**} | **paths** [*line*] | **peer-group** | **pending-prefixes** | **prefix-list** *prefix-list-name* | **quote-regexp** | **regexp** | **replication** [*update-group-index*] [*update-group-member-address*] | **rib-failure** | **route-map** *route-map-name* | **summary** | **update-group** | **update-source** | **version** {*version-number* | **recent** *offset-value*}}]

Syntax Description

all	Displays the complete VPNv4 database.
rd *route-distinguisher*	Displays Network Layer Reachability Information (NLRI) prefixes that match the named route distinguisher.
vrf *vrf-name*	Displays NLRI prefixes associated with the named VPN routing and forwarding (VRF) instance.
ip-prefix/length	(Optional) 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.
network-address	(Optional) IP address of a network in the BGP routing table.
mask	(Optional) Mask of the network address, in dotted decimal format.
cidr-only	(Optional) Displays only routes that have nonclassful netmasks.
cluster-ids	(Optional) Displays configured cluster IDs.
community	(Optional) Displays routes that match this community.
community-list	(Optional) Displays routes that match this community list.
dampening	(Optional) Displays paths suppressed because of dampening (BGP route from peer is up and down).
extcommunity-list *extended-community-list-name*	(Optional) Displays routes that match the extended community list.
filter-list	(Optional) Displays routes that conform to the filter list.
inconsistency nexthop-label	(Optional) Displays all inconsistent paths.

inconsistent-as	(Optional) Displays only routes that have inconsistent autonomous systems of origin.
labels	(Optional) Displays incoming and outgoing BGP labels for each NLRI prefix.
neighbors	(Optional) Displays details about TCP and BGP neighbor connections.
ip-address	(Optional) Displays information about the neighbor at this IPv4 address.
ipv6-address	(Optional) Displays information about the neighbor at this IPv6 address.
advertised-routes	(Optional) Displays advertised routes from the specified neighbor.
dampened-routes	(Optional) Displays dampened routes from the specified neighbor.
flap-statistics	(Optional) Displays flap statistics about the specified neighbor.
paths	(Optional) Displays path information.
line	(Optional) A regular expression to match the BGP autonomous system paths.
policy [detail]	(Optional) Displays configured policies for the specified neighbor.
slow	(Optional) Displays BGP slow peer information.
nexthops	(Optional) Displays nexthop address table.
oer-paths	(Optional) Displays all OER-controlled paths.
path-attribute	(Optional) Displays path-attribute-specific information.
discard	(Optional) Displays prefixes with discarded path attribute.
unknown	(Optional) Displays prefixes with unknown path attribute.
paths	(Optional) Displays path information.
line	(Optional) A regular expression to match the BGP autonomous system paths.
peer-group	(Optional) Displays information about peer groups.
pending-prefixes	(Optional) Displays prefixes that are pending deletion.
prefix-list *prefix-list*	(Optional) Displays routes that match the prefix list.
quote-regexp	(Optional) Displays routes that match the autonomous system path regular expression.
regexp	(Optional) Displays routes that match the autonomous system path regular expression.
replication	(Optional) Displays replication status of update group(s).

rib-failure	(Optional) Displays BGP routes that failed to install in the VRF table.
route-map	(Optional) Displays routes that match the route map.
summary	(Optional) Displays BGP neighbor status.
update-group	(Optional) Displays information on update groups.
update-source	(Optional) Displays update source interface table.
version	(Optional) Displays prefixes with matching version numbers.
version-number	(Optional) If the **version** keyword is specified, either a *version-number* or the **recent** keyword and an *offset-value* are required.
recent *offset-value*	(Optional) Displays prefixes with matching version numbers.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	This command was modified. 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	This command was modified. The **tags** keyword was replaced by the **labels** keyword to conform to the MPLS guidelines.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
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(27)S	This command was modified. The output of the **show ip bgp vpnv4 all labels** command was enhanced to display explicit-null label information.
12.3	This command was modified. The **rib-failure** keyword was added for VRFs.
12.2(22)S	This command was modified. The output of the **show ip bgp vpnv4 vrf** *vrf-name* **labels** command was modified so that directly connected VRF networks no longer display as aggregate; no label appears instead.
12.2(25)S	This command was updated to display MPLS VPN nonstop forwarding information.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router. The display output was modified to indicate whether BGP nonstop routing (NSR) with stateful switchover (SSO) is enabled and the reason the last BGP lost SSO capability.

Release	Modification
12.2(33)SRA	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.
12.2(31)SB2	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.
12.2(33)SXH	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID. **Note** In Cisco IOS Release 12.2(33)SXH, the command output does not display on the standby Route Processor in NSF/SSO mode.
12.4(20)T	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.
15.0(1)M	This command was modified. The output was modified to support the BGP Event-Based VPN Import feature.
12.2(33)SRE	This command was modified. The command output was modified to support the BGP Event-Based VPN Import, BGP best external, and BGP additional path features.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was implemented on the Cisco 7200 series router and the output was modified to display unknown attributes and discarded attributes associated with a prefix.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router and the output modified to display unknown attributes and discarded attributes associated with a prefix.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

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 all summary** command displays BGP neighbor status. The **show ip bgp vpnv4 all labels** command displays explicit-null label information.

Examples

The following example shows all available VPNv4 information in a BGP routing table:

```
Router# show ip bgp vpnv4 all
```

```
BGP table version is 18, local router ID is 10.14.14.14
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)
*>i10.6.6.6/32      10.0.0.21               11    100      0 ?
*> 10.7.7.7/32      10.150.0.2              11         32768 ?
*>i10.69.0.0/30     10.0.0.21                0    100      0 ?
*> 10.150.0.0/24    0.0.0.0                  0         32768 ?
```

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

Table 32: show ip bgp vpnv4 all 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)
   10.0.0.0         10.20.0.60      34/nolabel
   10.0.0.0         10.20.0.60      35/nolabel
   10.0.0.0         10.20.0.60      26/nolabel
                    10.20.0.60      26/nolabel
   10.0.0.0         10.15.0.15      nolabel/26
```

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

Table 33: 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 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf test1)
*> 10.1.1.1/32      192.168.1.1              0             0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 10.2.2.2/32      192.168.1.1                            0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 172.16.1.0/24    192.168.1.1              0             0 100 i
* i                 10.4.4.4                 0    100      0 100 i
r> 192.168.1.0      192.168.1.1              0             0 100 i
rbi                 10.4.4.4                 0    100      0 100 i
*> 192.168.3.0      192.168.1.1                            0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
```

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

Table 34: 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 192.168.9.0 that include multipaths, best path, and a recursive-via-host flag:

```
Router# show ip bgp vpnv4 vrf vpn1 192.168.9.0 255.255.255.0

BGP routing table entry for 100:1:192.168.9.0/24, version 44
Paths: (2 available, best #2, table test1)
  Additional-path
  Advertised to update-groups:
     2
  100, imported path from 400:1:192.168.9.0/24
    10.8.8.8 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.8.8.8, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out nolabel/17
  100, imported path from 300:1:192.168.9.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
```

```
mpls labels in/out nolabel/17
```

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

Table 35: show ip bgp vpnv4 all network-address Field Descriptions

Field	Description
BGP routing table entry for ... 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.
Multipath	Indicates the maximum paths configured (iBGP or eBGP).
Advertised to non peer-group peers	IP address of the BGP peers to which the specified route is advertised.
10.22.7.8 (metric 11) from 10.11.3.4 (10.0.0.8)	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 internal if the path is learned via iBGP. The field is external 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 this path is advertised to neighbors.
Extended Community	Route Target value associated with the specified route.
Originator	The router ID of the router from which the route originated 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 xyz rib-failure

Network            Next Hop                      RIB-failure   RIB-NH Matches
Route Distinguisher: 2:2 (default for vrf bar)
10.1.1.2/32        10.100.100.100      Higher admin distance              No
10.111.111.112/32  10.9.9.9            Higher admin distance             Yes
```

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

Table 36: show ip bgp vpnv4 vrf rib-failure 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 the Routing Information Base (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 the **bgp suppress-inactive** command is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or that the next hop recurses down to the same adjacency as the BGP next hop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that the **bgp suppress-inactive** command is not configured for the address family being used.

The following example shows the information displayed on the active and standby Route Processors when they are configured for NSF/SSO: MPLS VPN.

Note In Cisco IOS Release 12.2(33)SXH, the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature incurred various infrastructure changes. The result of those changes affects the output of this command on the standby Route Processor (RP). In Cisco IOS Release 12.2(33)SXH, the standby RP does not display any output from the **show ip bgp vpnv4** command.

```
Router# show ip bgp vpnv4 all labels

Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)
```

```
Route Distinguisher: 609:1 (vpn0)
10.13.13.13/32  0.0.0.0    18/aggregate(vpn0)

Router# show ip bgp vpnv4 vrf vpn1 labels

Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)


Router# show ip bgp vpnv4 all labels

Network       Masklen   In label
Route Distinguisher: 100:1
10.12.12.12   /32       16
10.0.0.0      /8        17
Route Distinguisher: 609:1
10.13.13.13   /32       18

Router# show ip bgp vpnv4 vrf vpn1 labels

Network        Masklen   In label
Route Distinguisher: 100:1
10.12.12.12    /32       16
10.0.0.0       /8        17
```

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

Table 37: show ip bgp vpnv4 labels Field Descriptions

Field	Description
Network	The network address from the BGP table.
Next Hop	The BGP next-hop address.
In label	The label (if any) assigned by this router.
Out label	The label assigned by the BGP next-hop router.
Masklen	The mask length of the network address.

The following example displays output, including the explicit-null label, from the **show ip bgp vpnv4 all labels** command on a CSC-PE router:

```
Router# show ip bgp vpnv4 all labels

   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   10.0.0.0/24       10.0.0.0        19/aggregate(v1)
   10.0.0.1/32       10.0.0.0        20/nolabel
   10.1.1.1/32       10.0.0.0        21/aggregate(v1)
   10.10.10.10/32    10.0.0.1        25/exp-null

   10.168.100.100/32
                     10.0.0.1        23/exp-null
   10.168.101.101/32
```

```
                10.0.0.1         22/exp-null
```

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

Table 38: show ip bgp vpnv4 all labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.

The following example displays separate router IDs for each VRF in the output from an image in Cisco IOS Release 12.2(31)SB2, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, Cisco IOS XE Release 2.1, and later releases with the Per-VRF Assignment of BGP Router ID feature configured. The router ID is shown next to the VRF name.

```
Router# show ip bgp vpnv4 all

BGP table version is 5, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 192.168.4.0      0.0.0.0                  0         32768 ?
Route Distinguisher: 42:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
*> 192.168.5.0      0.0.0.0                  0         32768 ?
```

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

Table 39: show ip bgp vpnv4 all (VRF Router ID) Field Descriptions

Field	Description
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.
vrf	Name of the VRF.
VRF Router ID	Router ID for the VRF.

In the following example, the BGP Event-Based VPN Import feature is configured in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured, but the **strict** keyword is not included, then a safe import path selection policy is in effect. When a path is imported as the best available path (when the best path or multipaths are not eligible for import), the imported path includes the wording “imported safety path,” as shown in the output.

```
Router# show ip bgp vpnv4 all 172.17.0.0
```

```
BGP routing table entry for 45000:1:172.17.0.0/16, version 10
Paths: (1 available, best #1, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2, imported safety path from 50000:2:172.17.0.0/16
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 200, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
```

In the following example, BGP Event-Based VPN Import feature configuration information is shown for Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured with the **all** keyword, any path that matches an RD of the specified VRF will be imported, even though the path does not match the Route Targets (RT) imported by the specified VRF. In this situation, the imported path is marked as "not-in-vrf" as shown in the output. Note that on the net for vrf-A, this path is not the best path because any paths that are not in the VRFs appear less attractive than paths in the VRF.

```
Router# show ip bgp vpnv4 all 172.17.0.0

BBGP routing table entry for 45000:1:172.17.0.0/16, version 11
Paths: (2 available, best #2, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2
     10.0.101.2 from 10.0.101.2 (10.0.101.2)
       Origin IGP, metric 100, localpref 100, valid, internal, not-in-vrf
       Extended Community: RT:45000:200
       mpls labels in/out nolabel/16
   2
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 50, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
mpls labels in/out nolabel/16
```

In the following example, the unknown attributes and discarded attributes associated with the prefix are displayed.

```
Device# show ip bgp vpnv4 all 10.0.0.0/8

BGP routing table entry for 100:200:10.0.0.0/8, version 0
Paths: (1 available, no best path)
  Not advertised to any peer
  Refresh Epoch 1
  Local
    10.0.103.1 from 10.0.103.1 (10.0.103.1)
      Origin IGP, localpref 100, valid, internal
      Extended Community: RT:1:100
      Connector Attribute: count=1
       type 1 len 12 value 22:22:10.0.101.22
      mpls labels in/out nolabel/16
      unknown transitive attribute: flag E0 type 129 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 140 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 120 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
```

```
      discarded unknown attribute: flag C0 type 128 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
```

The following example is based on the BGP—VPN Distinguisher Attribute feature. The output displays an Extended Community attribute, which is the VPN distinguisher (VD) of 104:1.

```
Device# show ip bgp vpnv4 unicast all 1.4.1.0/24

BGP routing table entry for 104:1:1.4.1.0/24, version 28
Paths: (1 available, best #1, no table)
   Advertised to update-groups:
      1
   Refresh Epoch 1
   1001
     19.0.101.1 from 19.0.101.1 (19.0.101.1)
       Origin IGP, localpref 100, valid, external, best
       Extended Community: VD:104:1
       mpls labels in/out nolabel/16
       rx pathid: 0, tx pathid: 0x0
```

The following example includes “allow-policy” in the output, indicating that the BGP—Support for iBGP Local-AS feature was configured for the specified neighbor by configuring the **neighbor allow-policy** command.

```
Device# show ip bgp vpnv4 all neighbors 192.168.3.3 policy

Neighbor: 192.168.3.3, Address-Family: VPNv4 Unicast
Locally configured policies:
 route-map pe33 out
 route-reflector-client
 allow-policy
 send-community both
```

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
neighbor allow-policy	Allows iBGP policies to be configured for the specified neighbor.
set extcommunity vpn-distinguisher	Sets a VPN distinguisher attribute to routes that pass a route map.
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** *pathname* | **identifier** *number*}] [**detail**]

Syntax Description

name *pathname*	(Optional) Displays the pathname of the explicit path.
identifier *number*	(Optional) Displays the number of the explicit path. The range is 1 to 65535.
detail	(Optional) Displays, in the long form, information about the configured IP explicit paths.

Command Default

If you enter the command without entering an optional keyword, all configured IP explicit paths are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	The command output was enhanced to display SLRG-related information.
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 2.3	This command was integrated into Cisco IOS XE Release 2.3.

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 10.3.28.3
    2: next-address 10.3.27.3
```

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

Table 40: show ip explicit-paths Field Descriptions

Field	Description
PATH	Pathname 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.
index	Inserts or modifies a path entry at a specific index.
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 multicast mpls vif

To display the virtual interfaces (VIFs) that are created on the Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) tailend router, use the **show ip multicast mpls vif** command in privileged EXEC mode.

show ip multicast mpls vif

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows information about the virtual interfaces:

```
Router# show ip multicast mpls vif
Interface   Next-hop             Application     Ref-Count   Table / VRF name
 Lspvif0     10.1.0.1             Traffic-eng      1           default
 Lspvif4     10.2.0.1             Traffic-eng      1           default
```

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

Table 41: show ip multicast mpls vif Field Descriptions

Field	Description
Interface	The name of the virtual interface
Next-hop	For P2MP TE, the source address of the TE P2MP tunnel. Only one label switched path (LSP) VIF is created for all TE P2MP tunnels that have the same source address.
Application	The name of the multicast application that creates the VIF.
Table/VRF name	The multicast virtual routing and forwarding (VRF) table used.

Related Commands

Command	Description
show ip mroute	Displays IP multicast traffic.

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.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 ip ospf database opaque-area** command:

```
Router# show ip ospf database opaque-area
OSPF Router with ID (10.3.3.3) (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: 10.0.0.0
  Opaque Type: 1
  Opaque ID: 0
  Advertising Router: 172.16.8.8
  LS Seq Number: 80000004
  Checksum: 0xD423
  Length: 132
  Fragment number : 0

    MPLS TE router ID: 172.16.8.8

    Link connected to Point-to-Point network
      Link ID : 10.2.2.2
      Interface Address : 192.168.1.1
```

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

Table 42: show ip ospf database opaque-area Field Descriptions

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

process-id	(Optional) Process ID. Includes information only for the specified routing process.
interface	(Optional) Defines the interface for which MPLS LDP-IGP synchronization information is displayed.

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.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

This command shows MPLS LDP-IGP synchronization information for specified interfaces or OSPF processes. If you do not specify an argument, information is displayed for each interface that was configured for MPLS LDP-IGP synchronization.

Examples

The following is sample output from 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 msecs
  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 msecs
  Holddown timer is not running
  Interface is up
```

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

Table 43: 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 MPLS LDP-IGP synchronization was enabled on this interface.
Holddown timer	Indicates whether the hold-down 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 the status of the MPLS LDP-IGP synchronization process.

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 Default

No default behavior or values.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 ip ospf mpls traffic-eng** command:

```
Router# show ip ospf mpls traffic-eng link
OSPF Router with ID (10.0.0.1) (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 :172.16.0.1
```

```
  Neighbor Address :172.16.0.2
  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 :192.168.1.2
  Interface Address :192.168.1.1
  Neighbor Address :192.168.1.2
  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
```

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

Table 44: 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** command in the interface configuration mode.
Maximum reservable bandwidth	Bandwidth available for traffic engineering on this link. This value is set in the **ip rsvp** command in the interface configuration mode.
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 and forwarding (VRF) instance, use the **show ip protocols vrf** command in user EXEC or privileged EXEC mode.

show ip protocols vrf vrf-name [**summary**]

Syntax Description

vrf-name	Name assigned to a VRF.
summary	Optional. Displays the routing protocol information in summary format.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	The **summary** keyword was added. EIGRP VRF support was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
12.2SX	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

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
```

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

Table 45: 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

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

show ip route [{*ip-address* [{**repair-paths** | **next-hop-override** [**dhcp**] | *mask* [**longer-prefixes**]}] | *protocol* [*process-id*] | **list** [{*access-list-number access-list-name*}] | **static download** | **update-queue**}]

Syntax Description

ip-address	(Optional) IP address for which routing information should be displayed.
repair-paths	(Optional) Displays the repair paths.
next-hop-override	(Optional) Displays the Next Hop Resolution Protocol (NHRP) next-hop overrides that are associated with a particular route and the corresponding default next hops.
dhcp	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.
mask	(Optional) Subnet mask.
longer-prefixes	(Optional) Displays output for longer prefix entries.
protocol	(Optional) The name of a routing protocol or the keyword **connected**, **mobile**, **static**, or **summary**. If you specify a routing protocol, use one of the following keywords: **bgp**, **eigrp**, **hello**, **isis**, **odr**, **ospf**, **nhrp**, or **rip**.
process-id	(Optional) Number used to identify a process of the specified protocol.
list	(Optional) Filters output by an access list name or number.
access-list-number	(Optional) Access list number.
access-list-name	(Optional) Access list name.
static	(Optional) Displays static routes.
download	(Optional) Displays routes installed using the authentication, authorization, and accounting (AAA) route download function. This keyword is used only when AAA is configured.
update-queue	(Optional) Displays Routing Information Base (RIB) queue updates.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.2	This command was introduced.

Release	Modification
10.0	This command was modified. The “D—EIGRP, EX—EIGRP, N1—SPF NSSA external type 1 route” and “N2—OSPF NSSA external type 2 route” codes were included in the command output.
10.3	This command was modified. The *process-id* argument was added.
11.0	This command was modified. The **longer-prefixes** keyword was added.
11.1	This command was modified. The “U—per-user static route” code was included in the command output.
11.2	This command was modified. The “o—on-demand routing” code was included in the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA, and the **update-queue** keyword was added.
11.3	This command was modified. The command output was enhanced to display the origin of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
12.0(1)T	This command was modified. The “M—mobile” code was included in the command output.
12.0(3)T	This command was modified. The “P—periodic downloaded static route” code was included in the command output.
12.0(4)T	This command was modified. The “ia—IS-IS” code was included in the command output.
12.2(2)T	This command was modified. The command output was enhanced to display information on multipaths to the specified network.
12.2(13)T	This command was modified. The *egp* and *igrp* arguments were removed because the Exterior Gateway Protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) were no longer available in Cisco software.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3(2)T	This command was modified. The command output was enhanced to display route tag information.
12.3(8)T	This command was modified. The command output was enhanced to display static routes using DHCP.

Release	Modification
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRE	This command was modified. The **dhcp** and **repair-paths** keywords were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5. The **next-hop-override** and **nhrp** keywords were added.
15.2(2)S	This command was modified. The command output was enhanced to display route tag values in dotted decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to display route tag values in dotted decimal format.
15.2(4)S	This command was implemented on the Cisco 7200 series router.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Examples

The following is sample output from the **show ip route** command when an IP address is not specified:

```
Device# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is 10.119.254.240 to network 10.140.0.0
O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E    10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E    10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

The following sample output from the **show ip route** command includes routes learned from IS-IS Level 2:

```
Device# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is not set
     10.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C       10.89.64.0 255.255.255.0 is possibly down,
          routing via 10.0.0.0, Ethernet0
i L2    10.89.67.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
i L2    10.89.66.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
```

The following is sample output from the **show ip route** *ip-address mask* **longer-prefixes** command. When this keyword is included, the address-mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed. The logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared with 10.0.0.0. Any destinations that fall into that range are displayed in the output.

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

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

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

The following sample outputs from the **show ip route** command display all downloaded static routes. A “p” indicates that these routes were installed using the AAA route download function.

```
Device# show ip route

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

Gateway of last resort is 172.16.17.1 to network 10.0.0.0

        172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1 10.0.0.0/8 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1

Device# show ip route static

     172.16.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.16.1.1/32 is directly connected, BRI0
P       172.16.4.0/8 [1/0] via 10.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.16.114.65, Ethernet0
S    10.0.0.0/8 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.114.201/32 is directly connected, BRI0
S       172.16.114.205/32 is directly connected, BRI0
S       172.16.114.174/32 is directly connected, BRI0
S       172.16.114.12/32 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
P    10.1.0.0/16 is directly connected, BRI0
P    10.2.2.0/24 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.16.114.65, Ethernet0
S    172.16.0.0/16 [1/0] via 172.16.114.65, Ethernet0
```

The following sample output from the **show ip route static download** command displays all active and inactive routes installed using the AAA route download function:

```
Device# show ip route static download

Connectivity: A - Active, I - Inactive

A     10.10.0.0 255.0.0.0 BRI0
A     10.11.0.0 255.0.0.0 BRI0
A     10.12.0.0 255.0.0.0 BRI0
A     10.13.0.0 255.0.0.0 BRI0
I     10.20.0.0 255.0.0.0 172.21.1.1
I     10.22.0.0 255.0.0.0 Serial0
I     10.30.0.0 255.0.0.0 Serial0
I     10.31.0.0 255.0.0.0 Serial1
I     10.32.0.0 255.0.0.0 Serial1
A     10.34.0.0 255.0.0.0 192.168.1.1
A     10.36.1.1 255.255.255.255 BRI0 200 name remote1
I     10.38.1.9 255.255.255.0 192.168.69.1
```

The following sample outputs from the **show ip route nhrp** command display shortcut switching on the tunnel interface:

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
Gateway of last resort is not set
10.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Tunnel0
C       172.16.22.0 is directly connected, Ethernet1/0
H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
     10.11.0.0/24 is subnetted, 1 subnets
C       10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route nhrp

H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
```

The following are sample outputs from the **show ip route** command when the **next-hop-override** keyword is used. When this keyword is included, the NHRP next-hop overrides that are associated with a particular route and the corresponding default next hops are displayed.

```
================================================================
1) Initial configuration
================================================================

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
```

```
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback1
10.10.10.0/24        attached             Tunnel0  <<<<<<<<
10.11.11.0/24        attached             Ethernet0/0
172.16.0.0/12          drop
.
.
.
================================================================
2) Add a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.1.1.1
   interface = Tunnel0
================================================================

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets

S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
```

```
      10.0.0.0/24 is subnetted, 1 subnets

S        10.10.10.0 is directly connected, Tunnel0
                    [NHO][1/0] via 10.1.1.1, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24

10.10.10.0/24       10.1.1.1             Tunnel0

10.11.11.0/24       attached            Ethernet0/0
10.12.0.0/16 drop
.
.
.
================================================================
3) Delete a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.11.1.1
   interface = Tunnel0
================================================================

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
```

```
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24

10.10.10.0/24        attached             Tunnel0
10.11.11.0/24        attached             Ethernet0/0
10.120.0.0/16 drop
.
.
.
```

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

Table 46: show ip route Field Descriptions

Field	Description
Codes (Protocol)	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—Connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • i—IS-IS derived • ia—IS-IS • L—Local • M—Mobile • o—On-demand routing • O—Open Shortest Path First (OSPF) derived • P—Periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—Static • U—Per-user static route • +—Replicated route

Field	Description
Codes (Type)	Type of route. It can be one of the following values: • *—Indicates the last path used when a packet was forwarded. This information is specific to nonfast-switched packets. • E1—OSPF external type 1 route • E2—OSPF external type 2 route • IA—OSPF interarea route • L1—IS-IS Level 1 route • L2—IS-IS Level 2 route • N1—OSPF not-so-stubby area (NSSA) external type 1 route • N2—OSPF NSSA external type 2 route
10.110.0.0	Indicates the address of the remote network.
[160/5]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next device to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

The following is sample output from the **show ip route** command when an IP address is specified:

```
Device# show ip route 10.0.0.1

Routing entry for 10.0.0.1/32
    Known via "isis", distance 115, metric 20, type level-1
    Redistributing via isis
    Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
    Routing Descriptor Blocks:
    * 10.22.22.2, from 10.191.255.247, via Serial2/3
       Route metric is 20, traffic share count is 1
       10.191.255.251, from 10.191.255.247, via Fddi1/0
       Route metric is 20, traffic share count is 1
```

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

The preceding example shows the output from the **show ip route** command for an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next-hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine the origin of a particular IP route in your network. In the preceding example, the route to 10.0.0.1/32 was originated by a device with IP address 10.191.255.247.

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

Table 47: show ip route with IP Address Field Descriptions

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	Indicates the IP address of the router that is the next hop to the remote network and the interface on which the last update arrived.
Routing Descriptor Blocks	Displays the next-hop IP address followed by the information source.
Route metric	This value is the best metric for this Routing Descriptor Block.
traffic share count	Indicates the number of packets transmitted over various routes.

The following sample output from the **show ip route** command displays the tag applied to the route 10.22.0.0/16. You must specify an IP prefix to see the tag value. The fields in the display are self-explanatory.

```
Device# show ip route 10.22.0.0

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

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.16.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate. The fields in the display are self-explanatory.

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.0.19.14 to network 0.0.0.0
10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
```

```
  172.16.0.0/32 is subnetted, 1 subnets
S 172.16.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0
S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

The following sample output from the **show ip route repair-paths** command shows repair paths marked with the tag [RPR]. The fields in the display are self-explanatory:

```
Device# show ip route repair-paths

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 3 subnets
C        10.1.1.1 is directly connected, Loopback0
B        10.2.2.2 [200/0] via 172.16.1.2, 00:31:07
                  [RPR][200/0] via 192.168.1.2, 00:31:07
B        10.9.9.9 [20/0] via 192.168.1.2, 00:29:45
                  [RPR][20/0] via 192.168.3.2, 00:29:45
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Serial2/0
L        192.168.1.1/32 is directly connected, Serial2/0
B     192.168.3.0/24 [200/0] via 172.16.1.2, 00:31:07
                     [RPR][200/0] via 192.168.1.2, 00:31:07
B     192.168.9.0/24 [20/0] via 192.168.1.2, 00:29:45
                     [RPR][20/0] via 192.168.3.2, 00:29:45
B     192.168.13.0/24 [20/0] via 192.168.1.2, 00:29:45
                      [RPR][20/0] via 192.168.3.2, 00:29:45

Device# show ip route repair-paths 10.9.9.9

>Routing entry for 10.9.9.9/32
>  Known via "bgp 100", distance 20, metric 0
>  Tag 10, type external
>  Last update from 192.168.1.2 00:44:52 ago
>  Routing Descriptor Blocks:
>  * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
>    [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
```

Related Commands

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

show ip route vrf

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

show ip route vrf {*vrf-name* | *****} [{**connected** | *protocol* [{*as-number*}] | **list** [{*list-number*}] | **profile** | **static** | **summary** | [{*ip-prefixip-address*}] [{*mask* | **longer-prefixes**}] | **repair-paths** | **dhcp** | **supernets-only** | **tag** {*tag-value* | *tag-value-dotted-decimal* [{*mask*}]}}]

Syntax Description

vrf-name or *	Name of the VRF. Use the asterisk (*) wildcard to include all VRF's.
connected	(Optional) Displays all connected routes in a VRF.
protocol	(Optional) Routing protocol. To specify a routing protocol, use one of the following keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**.
as-number	(Optional) Autonomous system number.
list *number*	(Optional) Specifies the IP access list to be displayed.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
ip-prefix	(Optional) Network for which routing information is displayed.
ip-address	(Optional) Address for which routing information is displayed.
mask	(Optional) Network mask.
longer-prefixes	(Optional) Displays longer prefix entries.
repair-paths	(Optional) Displays repair paths.
dhcp	(Optional) Displays routes added by the DHCP server.
supernets-only	(Optional) Displays only supernet entries.
tag	(Optional) Displays information about route tags in the VRF table.
tag-value	(Optional) Route tag values as a plain decimals.
tag-value-dotted-decimal	(Optional) Route tag values as a dotted decimals.
mask	(Optional) Route tag wildcard mask.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	This command was modified. The *ip-prefix* argument was added. The command output was enhanced to display information on multipaths to the specified network.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was modified. Support for Enhanced Interior Gateway Routing Protocol (EIGRP) VRFs was added.
12.2(15)T	This command was modified. Support for EIGRP VRFs was added.
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. The output was enhanced to display remote label information and corresponding Multiprotocol Label Switching (MPLS) flags for prefixes that have remote labels stored in the Routing Information Base (RIB).
12.2(33)SRE	This command was modified. The **repair-paths**, **dhcp**, and **supernets-only** keywords were added. Support for the Border Gateway Protocol (BGP) Best External and BGP Additional Path features was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.2(2)S	This command was modified. The **tag** keyword and *tag-value*, *tag-value-dotted-decimal*, and *mask* arguments were added to enable the display of route tags as plain or dotted decimals in the command output.
Cisco IOS XE Release 3.6S	This command was modified. The **tag** keyword and *tag-value*, *tag-value-dotted-decimal*, and *mask* arguments were added to enable the display of route tags as plain or dotted decimals in the command output.
15.2(4)S	This command was implemented on the Cisco 7200 series router.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
IOS XE Gibraltar 16.12.1	Extended use of asterisk (*) wildcard for *vrf-name* to work with the **summary** keyword.

Examples

The following sample output displays the IP routing table associated with the VRF named vrf1:

```
Device# 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    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, Ethernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

This following sample output shows BGP entries in the IP routing table associated with the VRF named vrf1:

```
Device# show ip route vrf vrf1 bgp

B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B  10.0.0.0/8 [20/0] via 10.0.0.1, 03:44:12
B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14
```

The following sample output displays the IP routing table associated with a VRF named PATH:

```
Device# 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:
  * 10.22.7.8 (Default-IP-Routing-Table), from 10.11.3.4, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.1.9 (Default-IP-Routing-Table), from 10.11.1.2, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.6.10 (Default-IP-Routing-Table), from 10.11.6.7, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.4.10 (Default-IP-Routing-Table), from 10.11.4.5, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.5.10 (Default-IP-Routing-Table), from 10.11.5.6, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
```

The following sample output from the **show ip route vrf** *vrf-name* **tag** command displays route tag information for routes associated with vrf1. The route tags in the sample output are displayed in dotted decimal format.

```
Device# show ip route vrf vrf1 tag 5

Routing Table: vrf1
Routing entry for 10.0.0.1/24
  Known via "static", distance 1, metric 0 (connected)
  Tag 0.0.0.5
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 0, traffic share count is 1
      Route tag 0.0.0.5
```

The following sample outputs from the **show ip route vrf** command include recursive-via-host and recursive-via-connected flags:

```
Device# show ip route vrf v2 10.2.2.2

Routing Table: v2
Routing entry for 10.2.2.2/32
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:15:54 ago
  Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:15:54 ago, recursive-via-conn
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: none

Device# show ip route vrf v2 10.2.2.2

Routing Table: v2
Routing entry for 10.2.2.2/32
  Known via "bgp 10", distance 200, metric 0
  Tag 100, type internal
  Last update from 10.3.3.3 00:18:11 ago
  Routing Descriptor Blocks:
  * 10.3.3.3 (default), from 10.5.5.5, 00:18:11 ago, recursive-via-host
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: 16
      MPLS Flags: MPLS Required
```

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

Table 48: 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	Metric used to reach the destination network.
Tag	Integer used to tag the route.
type	Indicates whether the route is an L1 type or L2 type of route.
Last update from 10.22.5.10	Indicates the IP address of the device that is the next hop to the remote network and identifies the interface on which the last update arrived.
00:01:07 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.

Field	Description
10.22.6.10, from 10.11.6.7, 00:01:07 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	Indicates the number of packets transmitted over various routes.
AS Hops	Number of hops to the destination or to the device where the route first enters internal BGP (iBGP).

The following is sample output from the **show ip route vrf** command on devices using the Cisco IOS Software Modularity for Layer 3 VPNs feature. The output includes remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the RIB if BGP is the label distribution protocol.

```
Device# show ip route vrf v2 10.2.2.2

Routing entry for 10.2.2.2/32
  Known via "bgp 1", distance 200, metric 0, type internal
  Redistributing via ospf 2
  Advertised by ospf 2 subnets
  Last update from 10.0.0.4 00:22:59 ago
  Routing Descriptor Blocks:
  * 10.0.0.4 (Default-IP-Routing-Table), from 10.0.0.31, 00:22:59 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 1300
      MPLS Flags: MPLS Required
```

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

Table 49: show ip route vrf Field Descriptions

Field	Description
MPLS label	Displays the BGP prefix from the BGP peer. The output shows one of the following values: • A label value (16–1048575). • A reserved label value, such as explicit-null or implicit-null. • The word “none” if no label is received from the peer. The MPLS label field is not displayed if any of the following conditions is true: • BGP is not the Label Distribution Protocol (LDP). However, Open Shortest Path First (OSPF) prefixes learned via sham links display an MPLS label. • MPLS is not supported. • The prefix is imported from another VRF, where the prefix was an Interior Gateway Protocol (IGP) prefix and LDP provided the remote label for it.

Field	Description
MPLS Flags	Name of the MPLS flag. One of the following MPLS flags is displayed: • MPLS Required—Indicates that packets are forwarded to this prefix because of the presence of the MPLS label stack. If MPLS is disabled on the outgoing interface, the packets are dropped. • No Global—Indicates that MPLS packets for this prefix are forwarded from the VRF interface and not from the interface in the global table. VRF interfaces prevent loops in scenarios that use iBGP multipaths. • NSF—Indicates that the prefix is from a nonstop forwarding (NSF)-aware neighbor. If the routing information temporarily disappears due to a disruption in the control plane, packets for this prefix are preserved.

The following sample output from the **show ip route vrf** command shows repair paths in the routing table. The fields in the display are self-explanatory.

```
Device> show ip route vrf test1 repair-paths 192.168.3.0

Routing Table: test1
Routing entry for 192.168.3.0/24
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:49:39 ago
  Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:49:39 ago, recursive-via-conn
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: none
    [RPR]10.4.4.4 (default), from 10.5.5.5, 00:49:39 ago, recursive-via-host
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: 29
MPLS Flags: MPLS Required, No Global
```

Using wildcard for VRF name

This example uses the asterisk (*) wildcard for *vrf-name*, with the **summary** keyword. All VRF's are included, in this case default, blue, and red.

```
Device#show ip route vrf * summary
IP routing table name is default (0x0)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
application     0           0           0           0           0
connected       0           2           0           192         624
static          1           1           0           192         624
internal        1                                               672
Total           2           3           0           384         1920

IP routing table name is blue (0x2)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
```

```
application     0           0           0           0           0
connected       0           0           0           0           0
static          0           0           0           0           0
internal        0                                               40
Total           0           0           0           0           40

IP routing table name is red (0x5)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
application     0           0           0           0           0
connected       0           0           0           0           0
static          0           0           0           0           0
internal        0                                               40
Total           0           0           0           0           40
```

Related Commands

Command	Description
show ip cache	Displays the Cisco Express 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 **showiprsvpfastbw-protect** command in user EXEC or privileged EXEC mode.

show ip rsvp fast bw-protect [**detail**] [**filter** [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]]

Syntax Description

detail	(Optional) Specifies additional receiver information.
filter	(Optional) Specifies a subset of the receivers to display .
destination *ip-address*	(Optional) Specifies the destination IP address of the receiver.
hostname	(Optional) Specifies the hostname of the receiver.
dst-port *port-number*	(Optional) Specifies the destination port number. Valid destination port numbers must be in the range from 0 to 65535.
source *ip-address*	(Optional) Specifies the source IP address of the receiver.
src-port *port-number*	(Optional) Specifies the source port number. Valid source port numbers must be in the range from 0 to 65535.

Command Default

The backup bandwidth protection and backup tunnel status information is not displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **showiprsvpfastbw-protect** command:

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

Primary          Protect  BW         Backup
Tunnel           I/F      BPS:Type   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
```

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

Table 50: 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 the following: • S--Subpool • G--Global pool
Backup Tunnel:Label	Identification of the backup tunnel.
State	Status of backup tunnel. Valid values are the following: • 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 the following: • 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 **showiprsvpfastdetail**command in user EXEC or privileged EXEC mode.

show ip rsvp fast detail [**filter** [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]]

Syntax Description

filter	(Optional) Specifies a subset of the receivers to display .
destination *ip-address*	(Optional) Specifies the destination IP address of the receiver.
hostname	(Optional) Specifies the hostname of the receiver.
dst-port *port-number*	(Optional) Specifies the destination port number. Valid destination port numbers must be in the range from 0 to 65535.
source *ip-address*	(Optional) Specifies the source IP address of the receiver.
src-port *port-number*	(Optional) Specifies the source port number. Valid source port numbers must be in the range from 0 to 65535.

Command Default

Specific information for RSVP categories is not displayed.

Command Modes

User EXEC (>)
Privileged 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.
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 **showiprsvpfastdetail** command:

```
Router# show ip rsvp fast detail

PATH:
  Tun Dest:   10.0.0.7  Tun ID: 500  Ext Tun ID: 10.0.0.5
  Tun Sender: 10.0.0.5  LSP ID: 8
  Path refreshes:
    sent:     to   NHOP 10.5.6.6 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)
  10.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.5.6 (Strict IPv4 Prefix, 8 bytes, /32)
  10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
ERO: (outgoing)
  10.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
  10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.7 (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: 10.5.6.5  LSP ID: 8
    Bkup FilerSpec:
      Tun Sender: 10.5.6.5, 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
```

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

Table 51: show ip rsvp fast detail Field Descriptions

Field	Description
Tun Dest	IP address of the receiver.
Tun 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 label-switched path (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 Unit	Minimum policed units, in bytes.
Max Pkt Size	Maximum packet size, in bytes.

Field	Description
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 point of local repair (PLR) for an LSP, there are three possible states: • 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: • 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).
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 or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) 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 or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) 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	Protection Switch Byte (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.

Field	Description
Status	For FRR LSPs, valid values are as follows: • 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 hello

To display hello status and statistics for Fast Reroute, reroute (hello state timer), and graceful restart, use the **showiprsvphello** command in user EXEC or privileged EXEC mode.

show ip rsvp hello

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The command output was modified to include graceful restart, reroute (hello state timer), and Fast Reroute information.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	The command output was modified to show whether graceful restart is configured and full mode was added.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	The command output was modified to include Bidirectional Forwarding Detection (BFD) protocol information.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following is sample output from the **showiprsvphello** command:

```
Router# show ip rsvp hello
Hello:
 RSVP Hello for Fast-Reroute/Reroute: Enabled
  Statistics: Disabled
 BFD for Fast-Reroute/Reroute: Enabled
 RSVP Hello for Graceful Restart: Disabled
```

The table below describes the significant fields shown in the display. The fields describe the processes for which hello is enabled or disabled.

Table 52: show ip rsvp hello Field Descriptions

Field	Description
RSVP Hello for Fast-Reroute/Reroute	Status of Fast-Reroute/Reroute: • Disabled--Fast reroute and reroute (hello for state timer) are not activated (disabled). • Enabled--Fast reroute and reroute (hello for state timer) are activated (enabled).
Statistics	Status of hello statistics: • Disabled--Hello statistics are not configured. • Enabled--Statistics are configured. Hello packets are time-stamped when they arrive in the hello input queue for the purpose of recording the time required until they are processed. • Shutdown--Hello statistics are configured but not operational. The input queue is too long (that is, more than 10,000 packets are queued).
BFD for Fast-Reroute/Reroute	Status of BFD for Fast-Reroute/Reroute: • Disabled--BFD is not configured. • Enabled--BFD is configured.
Graceful Restart	Restart capability: • Disabled--Restart capability is not activated. • Enabled--Restart capability is activated for a router (full mode) or its neighbor (help-neighbor).

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables hello globally on the router.
ip rsvp signalling hello statistics	Enables hello statistics on the router.
show ip rsvp hello statistics	Displays how long hello packets have been in the hello input queue.

show ip rsvp hello bfd nbr

To display information about all Multiprotocol Label Switching (MPLS) traffic engineering (TE) clients that use the Bidirectional Forwarding Detection (BFD) protocol, use the **show ip rsvp hello bfd nbr** command in user EXEC or privileged EXEC mode.

show ip rsvp hello bfd nbr

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

The command output is the same as the **show ip rsvp hello bfd nbr summary** command output.

Examples

The following is sample output from the **show ip rsvp hello bfd nbr** command.

```
Router# show ip rsvp hello bfd nbr
Client  Neighbor    I/F     State  LostCnt  LSPs
FRR     10.0.0.6    Gi9/47  Up     0        1
```

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

Table 53: show ip rsvp hello bfd nbr Field Descriptions

Field	Description
Client	MPLS TE feature that is using the BFD protocol.
Neighbor	IP address of the next-hop (that is, the neighbor).
I/F	Outbound (egress) interface name.
State	Status of the BFD session (Up, Down, or Lost).
LostCnt	Number of times that the BFD session is lost (dropped) on this interface.
LSPs	Number of label-switched paths (LSPs) that BFD is protecting on this interface.

Related Commands

Command	Description
clear ip rsvp hello bfd	Globally resets to zero the number of times that the BFD protocol was dropped on an interface or the number of times that a link was down.
ip rsvp signalling hello bfd (configuration)	Enables the BFD protocol globally on the router for MPLS TE link and node protection.
ip rsvp signalling hello bfd (interface)	Enables the BFD protocol on an interface for MPLS TE link and node protection.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

show ip rsvp hello bfd nbr detail

To display detailed information about all Multiprotocol Label Switching (MPLS) traffic engineering (TE) clients that use the Bidirectional Forwarding Detection (BFD) protocol, use the **show ip rsvp hello bfd nbr detail** command in user EXEC or privileged EXEC mode.

show ip rsvp hello bfd nbr detail

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Examples

The following is sample output from the **show ip rsvp hello bfd nbr detail** command:

```
Router# show ip rsvp hello bfd nbr detail
 Hello Client Neighbors
 Remote addr 10.0.0.6, Local addr  10.0.0.7
  Type: Active
  I/F: Gi9/47
  State: Up (for 00:09:41)
  Clients: FRR
  LSPs protecting: 1 (frr: 1, hst upstream: 0 hst downstream: 0)
  Communication with neighbor lost: 0
```

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

Table 54: show ip rsvp hello bfd nbr detail Field Descriptions

Field	Description
Remote addr	IP address of the next hop interface.
Local addr	IP address of the outbound interface.
Type	Type of signaling that is in effect (Active or Passive).
I/F	Interface name.
State	Status of the BFD session (Up, Down, or Lost).
Clients	Software that is using the BFD protocol.

Field	Description
LSPs protecting	Number of label switched paths (LSPs) that the BFD protocol is protecting.
Communication with neighbor lost	Number of times the BFD protocol detected that a link was down.

Related Commands

Command	Description
clear ip rsvp hello bfd	Globally resets to zero the number of times that the BFD protocol was dropped on an interface or the number of times that a link was down.
ip rsvp signalling hello bfd (configuration)	Enables the BFD protocol globally on the router for MPLS TE link and node protection.
ip rsvp signalling hello bfd (interface)	Enables the BFD protocol on an interface for MPLS TE link and node protection.
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

show ip rsvp hello bfd nbr summary

To display summarized information about all Multiprotocol Label Switching (MPLS) traffic engineering (TE) clients that use the Bidirectional Forwarding Detection (BFD) protocol, use the **show ip rsvp hello bfd nbr summary** command in user EXEC or privileged EXEC mode.

show ip rsvp hello bfd nbr summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

The command output is the same as the **show ip rsvp hello bfd nbr** command output.

Examples

The following is sample output from the **show ip rsvp hello bfd nbr summary** command.

```
Router# show ip rsvp hello bfd nbr summary

Client  Neighbor   I/F     State  LostCnt  LSPs
FRR     10.0.0.6   Gi9/47  Up     0        1
```

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

Table 55: show ip rsvp hello bfd nbr summary Field Descriptions

Field	Description
Client	MPLS TE feature that uses the BFD protocol.
Neighbor	IP address of the next hop (that is, the neighbor).
I/F	Interface type and slot or port.
State	Status of the BFD session (Up, Down, or Lost).
LostCnt	Number of times that the BFD session is lost (dropped) on this interface.
LSPs	Number of label switched paths (LSPs) that BFD is protecting on this interface.

Related Commands

Command	Description
clear ip rsvp hello bfd	Globally resets to zero the number of times that the BFD protocol was dropped on an interface or the number of times that a link was down.
ip rsvp signalling hello bfd (configuration)	Enables the BFD protocol globally on the router for MPLS TE link and node protection.
ip rsvp signalling hello bfd (interface)	Enables the BFD protocol globally on an interface for MPLS TE link and node protection.
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.

show ip rsvp hello instance detail

To display detailed information about a hello instance, use the **showiprsvphelloinstancedetail**command in user EXEC or privileged EXEC mode.

show ip rsvp hello instance detail [**filter destination** *ip-address*]

Syntax Description

filter destination *ip-address*	(Optional) IP address of the neighbor node.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The command output was modified to include graceful restart, hello state timer (reroute), and fast reroute information.
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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **showiprsvphelloinstancedetail** command to display information about the processes (clients) currently configured.

Examples

The following is sample output from the **showiprsvphelloinstancedetail** command:

```
Router# show ip rsvp hello instance detail
Neighbor 10.0.0.3  Source  10.0.0.2
    Type: Active    (sending requests)
    I/F:  Serial2/0
    State:   Up        (for 2d19h2d19h)
    Clients: ReRoute
    LSPs protecting: 1
    Missed acks: 4, IP DSCP: 0x30
    Refresh Interval (msec)
      Configured: 6000
      Statistics: (from 40722 samples)
        Min:      6000
        Max:      6064
        Average:  6000
        Waverage: 6000 (Weight = 0.8)
        Current:  6000
    Last sent Src_instance: 0xE617C847
    Last recv nbr's Src_instance: 0xFEC28E95
    Counters:
```

```
    Communication with neighbor lost:
      Num times:                    0
      Reasons:
        Missed acks:                0
        Bad Src_Inst received:      0
        Bad Dst_Inst received:      0
        I/F went down:              0
        Neighbor disabled Hello:    0
    Msgs Received:   55590
         Sent:       55854
         Suppressed: 521
Neighbor 10.0.0.8 Source  10.0.0.7
  Type: Passive   (responding to requests)
  I/F:  Serial2/1
  Last sent Src_instance: 0xF7A80A52
  Last recv nbr's Src_instance: 0xD2F1B7F7
  Counters:
    Msgs Received:   199442
         Sent:       199442
```

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

Table 56: show ip rsvp hello instance detail Field Descriptions

Field	Description
Neighbor	IP address of the adjacent node.
Source	IP address of the node that is sending the hello message.
Type	Values are Active (node is sending a request) and Passive (node is responding to a request).
I/F	Interface from which hellos are sent for this instance. Any means that the hellos can be sent out any interface.
State	Status of communication. Values are as follows: • Up--Node is communicating with its neighbor. • Lost--Communication has been lost. • Init--Communication is being established.
Clients	Clients that created this hello instance; they include graceful restart, ReRoute (hello state timer), and Fast Reroute.
LSPs protecting	Number of LSPs that are being protected by this hello instance.
Missed acks	Number of times that communication was lost due to missed acknowledgments (ACKs).
IP DSCP	IP differentiated services code point (DSCP) value used in the hello IP header.
Refresh Interval (msec)	The frequency (in milliseconds) with which a node generates a hello message containing a Hello Request object for each neighbor whose status is being tracked.
Configured	Configured refresh interval.

Field	Description
Statistics	Refresh interval statistics from a specified number of samples (packets).
Min	Minimum refresh interval.
Max	Maximum refresh interval.
Average	Average refresh interval.
Waverage	Weighted average refresh interval.
Current	Current refresh interval.
Last sent Src_instance	The last source instance sent to a neighbor.
Last recv nbr's Src_instance	The last source instance field value received from a neighbor. (0 means none received.)
Counters	Incremental information relating to communication with a neighbor.
Num times	Total number of times that communication with a neighbor was lost.
Reasons	Subsequent fields designate why communication with a neighbor was lost.
Missed acks	Number of times that communication was lost due to missed ACKs.
Bad Src_Inst received	Number of times that communication was lost due to bad source instance fields.
Bad Dst_Inst received	Number of times that communication was lost due to bad destination instance fields.
I/F went down	Number of times that the interface became unoperational.
Neighbor disabled Hello	Number of times that a neighbor disabled hello messages.
Msgs Received	Number of messages that were received.
Sent	Number of messages that were sent.
Suppressed	Number of messages that were suppressed due to optimization.

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables hello globally on the router.
ip rsvp signalling hello statistics	Enables hello statistics on the router.
show ip rsvp hello	Displays hello status and statistics for Fast reroute, reroute (hello state timer), and graceful restart.
show ip rsvp hello instance summary	Displays summary information about a hello instance.

show ip rsvp hello instance summary

To display summary information about a hello instance, use the **showiprsvphelloinstancesummary** command in user EXEC or privileged EXEC mode.

show ip rsvp hello instance summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The command output was modified to include graceful restart, reroute (hello state timer), and fast reroute information.
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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following is sample output from the **showiprsvphelloinstancesummary** command:

```
Router# show ip rsvp hello instance summary
Active Instances:
  Client  Neighbor        I/F        State      LostCnt  LSPs Interval
  RR      10.0.0.3        Se2/0      Up               0     1 6000
  GR      10.1.1.1        Any        Up              13     1 10000
  GR      10.1.1.5        Any        Lost             0     1 10000
  GR      10.2.2.1        Any        Init             1     0 5000
Passive Instances:
  Neighbor        I/F
  10.0.0.1        Se2/1
Active = Actively tracking neighbor state on behalf of clients:
         RR = ReRoute, FRR = Fast ReRoute, or GR = Graceful Restart
Passive = Responding to hello requests from neighbor
```

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

Table 57: show ip rsvp hello instance summary Field Descriptions

Field	Description
Active Instances	Active nodes that are sending hello requests.

Field	Description
Client	Clients on behalf of which hellos are sent; they include GR (graceful restart), RR (reroute = hello state timer), and FRR (Fast Reroute).
Neighbor	IP address of the adjacent node. For graceful restart, this is the neighbor router's ID; for Fast Reroute and hello state timer (reroute), this is one of the neighbor's interface addresses.
I/F	Interface from which hellos are sent for this instance. Any means that the hellos can be sent out any interface.
State	Status of communication. Values are as follows: • Up--Node is communicating with its neighbor. • Lost--Communication has been lost. • Init--Communication is being established.
LostCnt	Number of times that communication was lost with the neighbor.
LSPs	Number of label-switched paths (LSPs) protected by this hello instance.
Interval	Hello refresh interval in milliseconds.
Passive Instances	Passive nodes that are responding to hello requests.
Neighbor	IP address of adjacent node. For graceful restart, this is the neighbor router's ID; for Fast Reroute and hello state timer (reroute), this is one of the neighbor's interface addresses.
I/F	Interface from which hellos are sent for this instance. Any means that the hellos can be sent out any interface.

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables hello globally on the router.
ip rsvp signalling hello statistics	Enables hello statistics on the router.
show ip rsvp hello	Displays hello status and statistics for fast reroute, reroute (hello state timer), and graceful restart.
show ip rsvp hello instance detail	Displays detailed information about a hello instance.

show ip rsvp hello statistics

To display how long hello packets have been in the Hello input queue, use the **showiprsvphellostatistics**command in privileged EXEC mode.

show ip rsvp hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Information about how long hello packets have been in the Hello input queue is not displayed.

Command Modes

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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T

Usage Guidelines

You can use this command to determine if the Hello refresh interval is too small. If the interval is too small, communication may falsely be declared as lost.

Examples

The following is sample output from the **showiprsvphellostatistics** command:

```
Router# show ip rsvp hello statistics

Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:4
    Current length: 0 (max:500)
  Number of samples taken: 2398525
```

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

Table 58: show ip rsvp hello statistics Field Descriptions

Field	Description
Status	Indicator of whether Hello has been enabled globally on the router.

Field	Description
Current	Amount of time, in milliseconds, that the current hello packet has been in the Hello input queue.
Average	Average amount of time, in milliseconds, that hello packets are in the Hello input queue.
Max	Maximum amount of time, in milliseconds, that hello packets have been in the Hello input queue.
Current length	Current amount of time, in milliseconds, that hello packets have been in the Hello input queue.
Number of samples taken	Number of packets for which these statistics were compiled.

Related Commands

Command	Description
clear ip rsvp hello instance statistics	Clears Hello statistics for an instance.
clear ip rsvp hello statistics	Globally clears Hello statistics.
ip rsvp signalling hello refresh interval	Configures the Hello request interval.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.

show ip rsvp high-availability database

To display contents of Resource Reservation Protocol (RSVP) high availability (HA) read and write databases used in traffic engineering (TE), use the **show ip rsvp high-availability database** command in user EXEC or privileged EXEC mode.

show ip rsvp high-availability database {**hello** | **if-autotun** | **link-management** {**interfaces** [{**fixed** | **variable**}] | **system**} | **lsp** [{**filter** [{**destination** *ip-address*}] | [{**lsp-id** *lsp-id*}] | [{**source** *ip-address*}] | [{**tunnel-id** *tunnel-id*}]}] | **lsp-head** [**filter** *number*] | **summary**}

Syntax Description

hello	Displays information about hello entries in read and write databases.
if-autotun	Displays information about TE HA autotunnel interface entries in read and write databases.
link-management	Displays information about link-management entries in the read and write databases.
interfaces	Displays information about link-management interfaces in the read and write databases.
fixed	(Optional) Displays information about link-management fixed interfaces in the read and write databases.
variable	(Optional) Displays information about link-management variable interfaces in the read and write databases.
system	Displays information about the link-management system in the read and write databases.
lsp	Displays information about label switched path (LSP) entries in the read and write databases.
filter destination *ip-address*	(Optional) Displays filtered information on the IP address of the destination (tunnel tail).
filter lsp-id *lsp-id*	(Optional) Displays filtered information on a specific LSP ID designated by a number from 0 to 65535.
filter source *ip-address*	(Optional) Displays filtered information on the IP address of the source (tunnel head).
filter tunnel-id *tunnel-id*	(Optional) Displays filtered information on a specific tunnel ID designated by a number from 0 to 65535.
lsp-head	Displays information about LSP-head entries in the read and write databases.
filter *number*	(Optional) Displays filtered information on a specific LSP-head router designated by a number from 0 to 65535.
summary	Displays cumulative information about entries in read and write databases.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.2(33)SRB	The command output was modified to display the result of a loose hop expansion performed on the router.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC. The command output was modified to include path protection information specified by the **lsp-head** keyword.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. The command output was modified to distinguish database-entry information for point-to-point (P2P) tunnels from that for point-to-multipoint (P2MP) tunnels and to display error database information.
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)S	This command was modified. The **if-autotun** keyword was added. The output for the **show ip rsvp high-availability database lsp**, the **show ip rsvp high-availability database lsp-head**, and the **show ip rsvp high-availability database summary** commands was enhanced to display checkpoint information for MPLS TE autotunnel and automesh stateful switchover (SSO) tunnels.
Cisco IOS XE Release 3.6S	This command was modified. The **if-autotun** keyword was added. The output for the **show ip rsvp high-availability database lsp**, the **show ip rsvp high-availability database lsp-head**, and the **show ip rsvp high-availability database summary** commands was enhanced to display checkpoint information for MPLS TE autotunnel and automesh stateful switchover (SSO) tunnels.

Usage Guidelines

Use the **show ip rsvp high-availability database** command to display information about entries in the read and write databases.

Use the **show ip rsvp high-availability database lsp** command to display loose hop information. A loose hop expansion can be performed on a router when the router processes the explicit router object (ERO) for an incoming path message. After the router removes all local IP addresses from the incoming ERO, it finds the next hop. If the ERO specifies that the next hop is loose instead of strict, the router consults the TE topology database and routing to determine the next hop and output interface to forward the path message. The result of the calculation is a list of hops; the list is placed in the outgoing ERO and checkpointed with the LSP data as the loose hop information.

In Cisco IOS Release 15.0(1)S and later releases, the **show ip rsvp high-availability database lsp** command displays sub-LSP information. If any sub-LSP, whether P2MP or P2P, fails to recover after a stateful switchover

(SSO), the failure is noted in an error database for troubleshooting. You can use the **show ip rsvp high-availability database lsp** command to display error database entries.

You can use the **show ip rsvp high-availability database lsp-head** command only on a headend router; this command gives no information on other routers

Examples

Hello Example on an Active RP

The following is sample output from the **show ip rsvp high-availability database hello** command on an active Route Processor (RP):

```
Router# show ip rsvp high-availability database hello

HELLO WRITE DB
   Header:
     State: Checkpointed     Action: Add
     Seq #: 1                Flags: 0x0
   Data:
     Last sent Src_instance: 0xDE435865
HELLO READ DB
```

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

Table 59: show ip rsvp high-availability database hello—Active RP Field Descriptions

Field	Description
HELLO WRITE DB	Storage area for active RP hello data consisting of checkpointed RSVP-TE information that is sent to the standby RP when it becomes the active RP and needs to recover LSPs. This field is blank on a standby RP.
Header	Header information.
State	Status of an entry. Values are as follows: • Ack-Pending—Entries have been sent but not acknowledged. • Checkpointed—Entries have been sent and acknowledged by the standby RP. • Send-Pending—Entries are waiting to be sent.
Action	Action taken. Values are as follows: • Add—Adding an item to the standby RP. • Delete—Deleting an item from the standby RP. This is a temporary action that takes place while the active RP awaits an acknowledgment (ack) of the delete operation. • Modify—Modifying an item on the standby RP. • Remove—Removing an item from the standby RP.
Seq #	Number used by the active and standby RPs to synchronize message acknowledgments (acks) and negative acknowledgments (nacks) to sent messages.

Field	Description
Flags	Attribute used to identify or track data.
Data	Information about the last transmission.
Last sent Src_instance	Last sent source instance identifier.
HELLO READ DB	Storage area for standby RP hello data. This field is blank on an active RP, except when it is in recovery mode.

Hello Example on a Standby RP

The following is sample output from the **show ip rsvp high-availability database hello** on a standby RP:

```
Router# show ip rsvp high-availability database hello

HELLO WRITE DB
HELLO READ DB
   Header:
     State: Checkpointed     Action: Add
     Seq #: 1                Flags: 0x0
   Data:
     Last sent Src_instance: 0xDE435865
```

These fields are the same as those for the active RP described in the table except they are now in the read database for the standby RP.

Autotunnel Interfaces Example on an Active RP

The following is sample output from the **show ip rsvp high-availability database if-autotun** command on an active RP.

```
Router# show ip rsvp high-availability database if-autotun
IF_AUTOTUN WRITE DB

  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
    Tunnel ID: 1000 (if_handle: 85), prot_if_handle: 14
    template_unit: n/a, dest: 22.22.22.22, flags=0x0

  Header:
    State: Checkpointed     Action: Add
    Seq #: 61               Flags: 0x0
  Data:
    Tunnel ID: 2000 (if_handle: 86), prot_if_handle: 14
    template_unit: n/a, dest: 22.22.22.22, flags=0x1

  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
    Tunnel ID: 3000 (if_handle: 87), prot_if_handle: 0
    template_unit: 1, dest: 22.22.22.22, flags=0x2
```

```
  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
    Tunnel ID: 3001 (if_handle: 88), prot_if_handle: 0
    template_unit: 1, dest: 172.16.255.128, flags=0x2

  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
    Tunnel ID: 3002 (if_handle: 89), prot_if_handle: 0
    template_unit: 1, dest: 200.0.0.0, flags=0x2
```

```
IF_AUTOTUN READ DB
```

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

Table 60: show ip rsvp high-availability database if-autotun—Active RP Field Descriptions

Field	Description
IF_AUTOTUN WRITE DB	Storage area for active RP autotunnel interface information. This field is blank on a standby RP.
Header	Header information.
State	Status of an entry. Values are as follows: • Ack-Pending—Entries have been sent but not acknowledged. • Checkpointed—Entries have been sent and acknowledged by the standby RP. • Send-Pending—Entries are still waiting to be sent.
Action	Action taken. Values are as follows: • Add—Adding an item to the standby RP. • Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation. • Modify—Modifying an item on the standby RP. • Remove—Removing an item from the standby RP.
Seq #	Number used by the active and standby RPs to synchronize message acks and nacks to sent messages.
Flags	Attributes used to identify or track data.
Data	Information about the last transmission.

Field	Description
Tunnel ID	Tunnel identifier.
if_handle	Internal number representing the autotunnel interface. For the same tunnel ID, this if_handle value should always be the same for the record in the Standby READ DB as in the Active WRITE DB.
prot_if_handle	For autotunnel mesh tunnels, this value should always be zero. For autotunnel primary tunnels, this is an internal number representing the egress interface of the autotunnel primary. For autotunnel backup tunnels, this is an internal number representing the interface that the backup is protecting. In all three cases, for the same tunnel ID, this value should always be the same for the record in the Standby READ DB as in the Active WRITE DB.
template_unit	For autotunnel mesh, this represents the auto-template interface number that the mesh tunnel was created from. For autotunnel primary and backup, this should be "n/a."
dest	Destination IP address of the autotunnel.
flags	Encodings have these values: • 0 = autotunnel primary • 1 = autotunnel backup • 2 = autotunnel mesh
IF_AUTOTUN READ DB	Storage area for standby RP autotunnel interface information. This field is blank on an active RP.

The fields for a standby RP are the same as those described in the table except that they are now in the interface autotunnel read database instead of the interface autotunnel write database that is used by an active RP.

Link-Management Interfaces Example on an Active RP

The following is sample output from the **show ip rsvp high-availability database link-management interfaces** command on an active RP:

```
Router# show ip rsvp high-availability database link-management interfaces

TE LINK WRITE DB
Flooding Protocol: ospf  IGP Area ID: 0  Link ID: 0 (GigabitEthernet3/2)
  Header:
    State: Checkpointed     Action: Add
    Seq #: 4                Flags: 0x0
  Data:
```

```
Ifnumber: 5  Link Valid Flags: 0x193B
Link Subnet Type: Broadcast
Local Intfc ID: 0  Neighbor Intf ID: 0
Link IP Address: 172.16.3.1
Neighbor IGP System ID: 172.16.3.2  Neighbor IP Address: 10.0.0.0
IGP Metric: 1  TE Metric: 1
Physical Bandwidth: 1000000 kbits/sec
Res. Global BW: 3000 kbits/sec
Res. Sub BW: 0 kbits/sec
Upstream::
                        Global Pool   Sub Pool
                        -----------   ----------
Reservable Bandwidth[0]:           0            0 kbits/sec
Reservable Bandwidth[1]:           0            0 kbits/sec
Reservable Bandwidth[2]:           0            0 kbits/sec
Reservable Bandwidth[3]:           0            0 kbits/sec
Reservable Bandwidth[4]:           0            0 kbits/sec
Reservable Bandwidth[5]:           0            0 kbits/sec
Reservable Bandwidth[6]:           0            0 kbits/sec
Reservable Bandwidth[7]:           0            0 kbits/sec
Downstream::
                        Global Pool   Sub Pool
                        -----------   ----------
Reservable Bandwidth[0]:        3000            0 kbits/sec
Reservable Bandwidth[1]:        3000            0 kbits/sec
Reservable Bandwidth[2]:        3000            0 kbits/sec
Reservable Bandwidth[3]:        3000            0 kbits/sec
Reservable Bandwidth[4]:        3000            0 kbits/sec
Reservable Bandwidth[5]:        3000            0 kbits/sec
Reservable Bandwidth[6]:        3000            0 kbits/sec
Reservable Bandwidth[7]:        2900            0 kbits/sec
Affinity Bits: 0x0
Protection Type: Capability 0,  Working Priority 0
Number of TLVs: 0
```

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

Table 61: show ip rsvp high-availability database link-management interfaces—Active RP Field Descriptions

Field	Description
TE LINK WRITE DB	Storage area for active TE RP link data. This field is blank on a standby RP.
Flooding Protocol	Protocol that is flooding information for this area. OSPF = Open Shortest Path First.
IGP Area ID	Interior Gateway Protocol (IGP) identifier for the area being flooded.
Link ID	Link identifier and interface for the area being flooded.
Header	Header information.
State	Status of an entry. Values are as follows: • Ack-Pending—Entries have been sent but not acknowledged. • Checkpointed—Entries have been sent and acknowledged by the standby RP. • Send-Pending—Entries are waiting to be sent.

Field	Description
Action	Action taken. Values are as follows: • Add—Adding an item to the standby RP. • Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation. • Modify—Modifying an item on the standby RP. • Remove—Removing an item from the standby RP.
Seq #	Number used by the active and standby RPs to synchronize message acks and nacks to sent messages.
Flags	Attribute used to identify or track data.
Data	Information about the last transmission.
Ifnumber	Interface number.
Link Valid Flags	Attributes used to identify or track links.
Link Subnet Type	Subnet type of the link. Values are as follows: • Broadcast—Data for multiple recipients. • Nonbroadcast Multiaccess--A network in which data is transmitted directly from one computer to another over a virtual circuit or across a switching fabric. • Point-to-Multipoint—Unidirectional connection in which a single source end system (known as a root node) connects to multiple destination end systems (known as leaves). • Point-to-Point—Unidirectional or bidirectional connection between two end systems. • Unknown subnet type—Subnet type not identified.
Local Intfc ID	Local interface identifier.
Neighbor Intf ID	Neighbor’s interface identifier.
Link IP Address	IP address of the link.
Neighbor IGP System ID	Neighbor system identifier configured using IGP.
Neighbor IP Address	Neighbor’s IP address.
IGP Metric	Metric value for the TE link configured using IGP.
TE Metric	Metric value for the TE link configured using Multiprotocol Label Switching (MPLS) TE.
Physical Bandwidth	Link bandwidth capacity in kilobits per second (kb/s).

Field	Description
Res. Global BW	Amount of reservable global pool bandwidth (in kb/s) on this link.
Res. Sub BW	Amount of reservable subpool bandwidth (in kb/s) on this link.
Upstream	Header for the following section of bandwidth values.
Global Pool	Global pool bandwidth (in kb/s) on this link.
Sub Pool	Subpool bandwidth (in kb/s) on this link.
Reservable Bandwidth [1]	Amount of bandwidth (in kb/s) available for reservations in the global TE topology and subpools.
Downstream	Header for the following section of bandwidth values.
Affinity Bits	Link attributes required in tunnels.
Protection Type	LSPs protected by fast reroute (FRR). • Capability = LSPs capable of using FRR. • Working Priority = LSPs actually using FRR.
Number of TLVs	Number of type, length, values (TLVs).

The fields for a standby RP are the same as those described in the table except that they are now in the TE link read database instead of the TE link write database that is used by an active RP.

Link-Management System Example on an Active RP

The following is sample output from the **show ip rsvp high-availability database link-management system** command on an active RP:

```
Router# show ip rsvp high-availability database link-management system

TE SYSTEM WRITE DB
Flooding Protocol: OSPF  IGP Area ID: 0
  Header:
    State: Checkpointed     Action: Modify
    Seq #: 4                Flags: 0x0
  Data:
    LM Flood Data::
      LSA Valid flags: 0x0  Node LSA flag: 0x0
      IGP System ID: 172.16.3.1  MPLS TE Router ID: 10.0.0.3
      Flooded links: 1  TLV length: 0 (bytes)
      Fragment id: 0
TE SYSTEM READ DB
```

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

Table 62: show ip rsvp high-availability database link-management system—Active RP Field Descriptions

Field	Description
TE SYSTEM WRITE DB	Storage area for active TE RP system data. This field is blank on a standby RP.
Flooding Protocol	Protocol that is flooding information for this area. OSPF = Open Shortest Path First.
IGP Area ID	IGP identifier for the area being flooded.
Header	Header information.
State	Status of an entry. Values are as follows: • Ack-Pending—Entries have been sent but not acknowledged. • Checkpointed—Entries have been sent and acknowledged by the standby RP. • Send-Pending—Entries are waiting to be sent.
Action	Action taken. Values are as follows: • Add—Adding an item to the standby RP. • Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation. • Modify—Modifying an item on the standby RP. • Remove—Removing an item from the standby RP.
Seq #	Number used by the active and standby RPs to synchronize message acks and nacks to messages sent.
Flags	Attribute used to identify or track data.
Data	Information about the last transmission.
LM Flood Data	Link management (LM) flood data.
LSA Valid flags	Link-state advertisement (LSA) attributes.
Node LSA flag	LSA attributes used by a router.
IGP System ID	Identification (IP address) that IGP flooding uses in this area to identify this node.
MPLS TE Router ID	MPLS TE router identifier (IP address).
Flooded links	Number of flooded links.
TLV length	TLV length in bytes.
Fragment id	Fragment identifier for this link.

Field	Description
TE SYSTEM READ DB	Storage area for standby TE RP system data. This field is blank on a standby RP.

The fields for a standby RP are the same as those described in the table except that they are now in the TE system read database instead of the TE system write database that is used by an active RP.

LSP Example on an Active RP for a P2P Tunnel

The following is sample output from the **show ip rsvp high-availability database lsp** command on an active RP for a P2P tunnel:

```
Router# show ip rsvp high-availability database lsp

Tun ID: 0   LSP ID: 10   (P2P)
  SubGrp ID:   -
  SubGrp Orig: -
  Dest:   10.3.0.1
  Sender: 10.1.0.1     Ext. Tun ID: 10.1.0.1
  Header:
    State: Checkpointed     Action: Add
    Seq #: 2                Flags: 0x0
  Data:
    PathSet ID: -
    Lspvif if_num: -
    InLabel: -
    Out I/F: Se2/0
    Next-Hop: 10.1.3.2
    OutLabel: 16
    Loose hop info: None (0)
```

LSP Example on an Active RP for a P2MP Tunnel

The following is sample output from the **show ip rsvp high-availability database lsp** command on an active RP for a P2MP tunnel:

```
Router# show ip rsvp high-availability database lsp

Tun ID: 1   LSP ID: 127   (P2MP)
  SubGrp ID:   1
  SubGrp Orig: 10.1.0.1
  Dest:   10.2.0.1
  Sender: 10.1.0.1     Ext. Tun ID: 10.1.0.1
  Header:
    State: Checkpointed     Action: Add
    Seq #: 30               Flags: 0x0
  Data:
    PathSet ID: 0x1A000003
    Lspvif if_num: 35 (Lspvif0)
    InLabel: 19
    Out I/F: None
    Next-Hop: -
    OutLabel: -
    Loose hop info: None (0)
```

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

Table 63: show ip rsvp high-availability database lsp—Active RP Field Descriptions

Field	Description
P2P/P2MP	Tunnel type.
Subgrp ID	Subgroup identifier (valid only for P2MP TE LSPs).
Subgrp Orig	Subgroup origin IP address (valid only for P2MP TE LSPs).
Lspvif if_num	Interface number of the LSPVIF (valid only for P2MP TE tailends).
PathSet ID	Path set identifier (valid only for P2MP TE LSPs)
LSP WRITE DB	Storage area for active RP LSP data. This field is blank on a standby RP.
Tun ID	Tunnel identifier.
LSP ID	LSP identifier.
Dest	Tunnel destination IP address.
Sender	Tunnel sender IP address.
Ext. Tun ID	Extended tunnel identifier; usually set to 0 or the sender's IP address.
Header	Header information.
State	Status of an entry. Values are as follows: • Ack-Pending—Entries have been sent, but not acknowledged. • Checkpointed—Entries have been sent and acknowledged by the standby RP. • Send-Pending—Entries are waiting to be sent.
Action	Action taken. Values are as follows: • Add—Adding an item to the standby RP. • Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation. • Modify—Modifying an item on the standby RP. • Remove—Removing an item from the standby RP.
Seq #	Number used by the active and standby RPs to synchronize message acks and nacks to messages sent.
Flags	Attribute used to identify or track data.
Data	Information about the last transmission.
InLabel	Incoming label identifier.
Out I/F	Outgoing interface.

Field	Description
Next-Hop	Next hop IP address.
OutLabel	Outgoing label identifier.
Loose hop info	Lists the loose hop expansions performed on the router, or specifies None.
LSP READ DB	Storage area for standby RP LSP data. This field is blank on an active RP.

The fields for a standby RP are the same as those described in the table except that they are now in the LSP read database instead of the LSP write database that is used by an active RP.

LSP-Head Example on an Active RP for a P2P Tunnel

The following is sample output from the **show ip rsvp high-availability database lsp-head** command on an active RP for a P2P tunnel:

```
Router# show ip rsvp high-availability database lsp-head

LSP_HEAD WRITE DB
  Tun ID: 0  (P2P)
  Header:
    State: Checkpointed     Action: Add
    Seq #: 2                Flags: 0x0
  Data:
    lsp_id: 10, bandwidth: 5, thead_flags: 0x1, popt: 1
    feature flags: none
    output_if_num: 11, output_nhop: 10.1.3.2
    RRR path setup info
      Destination: 10.3.0.1, Id: 10.3.0.1 Router Node (ospf) flag:0x0
      IGP: ospf, IGP area: 0, Number of hops: 3, metric: 128
      Hop 0: 10.1.3.2, Id: 10.2.0.1 Router Node (ospf), flag:0x0
      Hop 1: 10.2.3.3, Id: 10.3.0.1 Router Node (ospf), flag:0x0
      Hop 2: 10.3.0.1, Id: 10.3.0.1 Router Node (ospf), flag:0x0
```

LSP-Head Example on an Active RP for a P2MP Tunnel

The following is sample output from the **show ip rsvp high-availability database lsp-head** command on an active RP for a P2MP tunnel:

```
Router# show ip rsvp high-availability database lsp-head

LSP_HEAD WRITE DB
Tun ID: 1  (P2MP)
  Destination: 10.2.0.1
  Header:
    State: Checkpointed     Action: Add
    Seq #: 3                Flags: 0x0
  Data:
    lsp_id: 11, bandwidth: 100, thead_flags: 0x1, popt: 1
    Subgrp_id: 1
    feature flags: none
    output_if_num: 3, output_nhop: 10.1.2.2
    RRR path setup info
      Destination: 10.2.0.1, Id: 10.2.0.1 Router Node (ospf) flag:0x0
```

```
IGP: ospf, IGP area: 0, Number of hops: 3, metric: 10
Hop 0: 10.1.2.1, Id: 10.1.0.1 Router Node (ospf), flag:0x0
Hop 1: 10.1.2.2, Id: 10.2.0.1 Router Node (ospf), flag:0x0
Hop 2: 10.2.0.1, Id: 10.2.0.1 Router Node (ospf), flag:0x0
```

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

Table 64: show ip rsvp high-availability database lsp-head—Active RP Field Descriptions

Field	Description
LSP_HEAD WRITE DB	Storage area for active RP LSP-head data. This field is blank on a standby RP.
P2P/P2MP	Tunnel type.
Tun ID	Tunnel identifier.
Header	Header information.
State	Status of an entry. Values are as follows: • Ack-Pending—Entries have been sent, but not acknowledged. • Checkpointed—Entries have been sent and acknowledged by the standby RP. • Send-Pending—Entries are waiting to be sent.
Action	Action taken. Values are as follows: • Add—Adding an item to the standby RP. • Delete—Deleting an item from the standby RP. This is a temporary action that takes place while the active RP awaits an ack of the delete operation. • Modify—Modifying an item on the standby RP. • Remove—Removing an item from the standby RP.
Seq #	Number used by the active and standby RPs to synchronize message acks and nacks to messages sent.
Flags	Attribute used to identify or track data.
Data	Information about the last transmission.
lsp_id	LSP identifier.
bandwidth	Bandwidth on the LSP (in kb/s).
thead_flags	Tunnel head attribute used to identify or track data.
popt	Parsing option number.

Field	Description
feature_flags	Indicates whether the LSP being used to forward traffic is the secondary LSP using the path protection path option. Valid values are as follows: • none • path protection active
output_if_num	Output interface number.
output_nhop	Output next hop IP address.
RRR path setup info	Routing with Resource Reservation (RRR) path information.
Destination	Destination IP address.
Id	IP address and protocol of the routing node. Values are as follows: • ISIS = Intermediate System-to-Intermediate System • OSPF = Open Shortest Path First
flag	Attribute used to track data.
IGP	Interior Gateway Protocol. OSPF = Open Shortest Path First.
IGP area	IGP area identifier.
Number of hops	Number of connections or routers.
metric	Routing cost.
Hop	Hop's number and IP address.
LSP_HEAD READ DB	Storage area for standby RP LSP-head data. This field is blank on an active RP.

The fields for a standby RP are the same as those described in the table except that they are now in the LSP_head read database instead of the LSP_head write database that is used by an active RP.

Summary Example on an Active RP

The following is sample output from the **show ip rsvp high-availability database summary** command on an active RP:

```
Router# show ip rsvp high-availability database summary

Write DB:
  Send-Pending:     0
  Ack-Pending :     0
  Checkpointed:    10
  Total       :    10
Read DB:
  Total       :     0
```

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

Table 65: show ip rsvp high-availability database summary—Active RP Field Descriptions

Field	Description
Write DB	Storage area for active RP summary data. This field is blank on a standby RP.
Send-Pending	Entries are waiting to be sent.
Ack-Pending	Entries have been sent, but are waiting to be acknowledged.
Checkpointed	Entries have been sent and acknowledged.
Total	Total number of entries in the write database.
Total	Total number of entries in the read database.

Summary Example on a Standby RP

The following is sample output from the **show ip rsvp high-availability database summary** command on a standby RP:

```
Router# show ip rsvp high-availability database summary

Write DB:
  Send-Pending:     0
  Ack-Pending :     0
  Checkpointed:     0
  Total       :     0
Read DB:
  Total       :    10
```

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

Table 66: show ip rsvp high-availability database summary—Standby RP Field Descriptions

Field	Description
Write DB	Storage area for active RP summary data.
Send-Pending	Entries are waiting to be sent.
Ack-Pending	Entries have been sent but are waiting to be acknowledged.
Checkpointed	Entries have been sent and acknowledged.
Total	Total number of entries in the write database.
Total	Total number of entries in the read database.

Related Commands

Command	Description
show ip rsvp high-availability counters	Displays all RSVP HA counters that are being maintained by an RP.

Command	Description
show ip rsvp high-availability summary	Displays summary information for an RSVP HA RP.

show ip rsvp host

To display specific information for a Resource Reservation Protocol (RSVP) host, use the **showiprsvphost** command in user EXEC or privileged EXEC mode.

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

Syntax Description

senders	RSVP-related sender information currently in the database.
receivers	RSVP-related receiver information currently in the database.
hostname	(Optional) Hostname of the source or destination.
group-address	(Optional) IP address of the source or destination.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.4(6)T	This command was modified. The command output was modified to display RSVP identity information when configured.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use the **showiprsvphost** command to display static RSVP senders and receivers. If a router has any local host receivers or senders that have RSVP identities configured, the application IDs that they use are also displayed.

Examples

In the following example from the**showiprsvphostsenders**command, no RSVP identities are configured for the local sender:

```
Router# show ip rsvp host senders
To            From          Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.3 192.168.104.1 UDP 1     1                           10K
  Mode(s): Host CLI
```

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

Table 67: show ip rsvp host senders (No RSVP Identities Configured) Field Descriptions

Field	Description
To	IP address of the receiver.

Field	Description
From	IP address of the sender.
Pro	Protocol code. IP protocol such as TCP or UDP.
DPort	Destination port number. Code 1 indicates an IP protocol such as TCP or UDP.
Sport	Source port number. Code 1 indicates an IP protocol such as TCP or UDP.
Prev Hop	IP address of the previous hop. Blank means no previous hop.
I/F	Interface of the previous hop.
BPS	Reservation rate, in bits per second (bps).
Mode(s)	Any of the following strings: • Host--The router is acting as the host system or RSVP endpoint for this reservation. • LSP-Tunnel--The reservation is for a traffic engineering (TE) tunnel. • MIB--The reservation was created via an Simple Network Management Protocol (SNMP) SET directive from a remote management station. • CLI--The reservation was created via a local RSVP command. • Host CLI--A combination of the host and command line interface (CLI) strings meaning that the static sender being displayed was created by the **iprsvpsender-host** command.

In the following example from the**showiprsvphostsenders**command, an RSVP identity is configured for the local sender:

```
Router# show ip rsvp host senders
To              From            Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.3 192.168.104.1 UDP 1     1                           10K
  Mode(s): Host CLI
  Identity: voice100
    Locator: GUID=www.cisco.com,APP=voice,VER=100.0
    ID Type: Application
```

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

Table 68: show ip rsvp host senders (RSVP Identity Configured) Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. IP protocol such as TCP or UDP.
DPort	Destination port number. Code 1 indicates IP protocol such as TCP or UDP.
Sport	Source port number. Code 1 indicates IP protocol such as TCP or UDP.

Field	Description
Prev Hop	IP address of the previous hop. Blank means no previous hop.
I/F	Interface of the previous hop.
BPS	Reservation rate in bits per second (bps).
Mode(s)	Any of the following strings: • CLI--The reservation was created via a local RSVP command. • Host--The router is acting as the host system or RSVP endpoint for this reservation. • Host CLI--A combination of the host and CLI strings meaning that the static sender being displayed was created by the **iprsvpsender-host** command. • LSP-Tunnel--The reservation is for a Traffic Engineering (TE) tunnel. • MIB--The reservation was created via an SNMP SET directive from a remote management station.
Identity	The alias string for the RSVP application ID.
Locator	The application ID that is being signaled in the RSVP PATH message for this statically-configured sender.
ID Type	Types of identities. RSVP defines two types: application IDs (Application) and user IDs (User). Cisco IOS software and Cisco IOS XE software support application IDs only.

Related Commands

Command	Description
ip rsvp sender-host	Enables a router to simulate a host generating an RSVP PATH message.

show ip rsvp interface detail

To display the hello configuration for all interface types, use the **show ip rsvp interface detail**command in user EXEC or privileged EXEC mode.

show ip rsvp interface detail [*type number*]

Syntax Description

type number	(Optional) The type and number of the interface for which you want to display the hello configuration.

Command Default

The hello configuration for all interfaces is 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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
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 the source address used in the PHOP address field.
15.1(2)T	This command was modified. The output was updated to display the overhead percent.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

To display the hello configuration for a specific interface, use the **show ip rsvp interface detail** command with the *type* and *number* arguments.

Examples

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

```
Router# show ip rsvp interface detail GigabitEthernet 9/47
Tu0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 10K bits/sec
     Max. allowed (total): 75K bits/sec
```

```
  Max. allowed (per flow): 75K bits/sec
  Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
  Set aside by policy (total): 0 bits/sec
Admission Control:
  Header Compression methods supported:
    rtp (36 bytes-saved), udp (20 bytes-saved)
  Tunnel IP Overhead percent:
    4
  Tunnel Bandwidth considered:
    Yes
Traffic Control:
  RSVP Data Packet Classification is ON via CEF callbacks
Signalling:
  DSCP value used in RSVP msgs: 0x3F
  Number of refresh intervals to enforce blockade state: 4
Authentication: disabled
  Key chain:   <none>
  Type:        md5
  Window size: 1
  Challenge:   disabled
Hello Extension:
  State: Disabled
```

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

Table 69: show ip rsvp interface detail Field Descriptions

Field	Description
RSVP	Status of the Resource Reservation Protocol (RSVP) (Enabled or Disabled).
Interface State	Status of the interface (Up or Down).
Curr allocated	Amount of bandwidth (in bits per second [b/s]) currently allocated.
Max. allowed (total)	Total maximum amount of bandwidth (in b/s) allowed.
Max. allowed (per flow)	Maximum amount of bandwidth (in b/s) allowed per flow.
Max. allowed for LSP tunnels using sub-pools	Maximum amount of bandwidth permitted for the label switched path (LSP) tunnels that obtain their bandwidth from subpools.
Tunnel IP Overhead percent	Overhead percent to override the RSVP bandwidth manually.
Tunnel Bandwidth considered	Indicates if the tunnel bandwidth is considered.
DSCP value used in RSVP msgs	Differentiated services code point (DSCP) value in the RSVP messages.

show ip traffic-engineering

To display information about the traffic engineering configuration and metric information associated with it, use the **show ip traffic-engineering** command in privileged EXEC mode.

show ip traffic-engineering [**metrics** [**detail**]]

Syntax Description

metrics	(Optional) Displays metric information associated with traffic engineering.
detail	(Optional) Displays information in long form.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
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 goal of the loop prevention algorithm is that traffic should not be sent down the tunnel if there is a possibility that, after leaving the tunnel, steady state routing will route the traffic back to the head of the tunnel.

The strategy of the loop prevention algorithm is to compare the Layer 3 routing distance to the egress from the tunnel tailend and tunnel headend. The loop check passes only if the tunnel tail is closer to the egress than the tunnel head is.

The loop prevention algorithm allows you to use the tunnel for a route if one the following cases applies:

- Given that the two ends of the tunnel are routing to the egress using the same dynamic protocol in the same area, the Layer 3 routing distance from the tailend to the egress is less than the Layer 3 routing distance from the headend to the egress.
- The route to the egress is directly connected at the tunnel tailend router, but not at the tunnel headend router.
- The egress is unreachable from the tunnel headend router, but is reachable from the tunnel tailend router.

The loop prevention algorithm prevents you from using the tunnel for a given egress in all other cases, in particular, the following cases:

- The routers at the ends of the tunnel get their route to the egress from different dynamic routing protocols.
- The routing protocols at the two ends of the tunnel route to the egress through different areas.
- The two ends each use a static route to the egress.
- The tunnel headend router’s route to the egress is a connected route.
- The egress is unreachable from the tunnel tailend router.

Devices request metrics via an LDP adjacency. The display output shows detailed metric information.

The metric information includes a metric type (shown as routing_protocol/routing_protocol_subtype) and a metric value.

The routing protocol is as follows:

- Open Shortest Path First (OSPF)
- Intermediate System to Intermediate System (IS-IS)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Connected
- Static
- Other (some other routing protocol)

The routing protocol subtype is specific to each routing protocol.

Examples

The following is sample output from the **show ip traffic-engineering metrics detail** command:

```
Router# show ip traffic-engineering metrics detail
Metrics requested BY this device
 Prefix 43.0.0.1/32
  TDP id 2.2.2.2:0, metric: connected/0
    type request, flags metric-received, rev 6, refcnt 1
  TDP id 4.4.4.4:0, metric: ospf-300/2
    type request, flags metric-received, rev 7, refcnt 1
 Prefix 44.0.0.0/8
  TDP id 18.18.18.18:0, metric: connected/0
    type request, flags metric-received, rev 1, refcnt 1
Metrics requested FROM this device
 Prefix 36.0.0.0/8
  TDP id 18.18.18.18:0, metric: connected/0
    type advertise, flags none, rev 1, refcnt 1
```

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

Table 70: show ip traffic-engineering metrics detail Field Descriptions

Field	Description
Prefix	Destination network and mask.
TDP id	The LDP identifier of the LDP peer device at the other end of the tunnel. The LDP peer device advertises these metrics to this neighbor.
metric	The routing protocol and metric within that protocol for the prefix in question.
type	For metrics being requested by this device, the type is either “request” or “release.” For metrics being requested from this device, the type is “advertise.”
flags	For metrics being requested by this device, “metric-received” indicates that the other end has responded with a metric value. For metrics being requested from this device, response-pending indicates that the metric value has not yet been sent to the requester.

Field	Description
rev	An internal identifier for the metric request or advertisement. The rev number is assigned when the request/advertisement is created. The rev number is updated if the local information for the metric changes.
refcnt	For a metric of type request, the number of traffic engineering routes interested in this metric value. Otherwise, refcnt is 1.

Related Commands

Command	Description
traffic-engineering filter	Specifies a filter with a given number and properties.
traffic-engineering route	Configures a route for a specified filter, through a specified tunnel.

show ip traffic-engineering configuration

To display information about configured traffic engineering filters and routes, use the **show ip traffic-engineering configuration** command in privileged EXEC mode.

show ip traffic-engineering configuration [*interface*] [*filter-number*] [**detail**]

Syntax Description

interface	(Optional) Specifies an interface for which to display traffic engineering information.
filter-number	(Optional) A decimal value representing the number of the filter to display.
detail	(Optional) Displays command output in long form.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
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 sample output can show all filters or can be limited by interface, filter number, or both.

Examples

The following is sample output from the **show ip traffic-engineering configuration detail** command:

```
Router# show ip traffic-engineering configuration detail
Traffic Engineering Configuration
    Filter 5: egress 44.0.0.0/8, local metric: ospf-0/1
        Tunnel5 route installed
          interface up, preference 1
          loop check on, passing, remote metric: connected/0
    Filter 6: egress 43.0.0.1/32, local metric: ospf-300/3
        Tunnel7 route installed
          interface up, preference 50
          loop check on, passing, remote metric: ospf-300/2
        Tunnel6 route not installed
          interface up, preference 75
          loop check on, passing, remote metric: connected/0
```

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

Table 71: show ip traffic-engineering configuration detail Field Descriptions

Field	Description
Filter	The configured filter identifier for the traffic engineering route.
egress	The prefix/mask configured with the filter local metric.

Field	Description
local metric	The routing protocol and metric value of the local LSR for the egress prefix/mask.
Tunnel5	The tunnel for the traffic engineering route.
route installed/not installed	Indicates whether the route is installed in the forwarding tables (typically CEF and label interface up/down).
interface	Indicates whether the tunnel interface for the traffic engineering route is up or down. The traffic engineering route is not installed if the tunnel interface is down.
preference	The configured administrative preference for the traffic engineering route.
loop check	Indicates whether the loop check has been configured on or off.
passing/failing	If the loop check is configured on, indicates whether the check is passing. The traffic engineering route is not installed if the loop check is configured on and is failing.
remote metric	The routing protocol and the metric within that protocol for the prefix in question, as seen by the LSR that is advertising the metric. As part of the loop check, a comparison is made between the remote metric and the local metric.

Related Commands

Command	Description
show ip traffic-engineering routes	Displays information about the requested filters configured for traffic engineering.

show ip traffic-engineering routes through show mpls memory

show ip traffic-engineering routes

To display information about the requested filters configured for traffic engineering, use the **show ip traffic-engineering routes** command in privileged EXEC mode.

show ip traffic-engineering routes [*filter-number*] [**detail**]

Syntax Description

filter-number	(Optional) A decimal value representing the number of the filter to display.
detail	(Optional) Display of command output in long form.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
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

Requests can be limited to a specific filter.

Examples

The following is sample output from the **show ip traffic-engineering routes** command:

```
Router# show ip traffic-engineering routes
Installed traffic engineering routes:
Codes: T - traffic engineered route
T    43.0.0.1/32 (not override of routing table entry)
               is directly connected, 00:06:35, Tunnel7
T    44.0.0.0/8 (override of routing table entry)
              is directly connected, 01:12:39, Tunnel5
```

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

Table 72: show ip traffic-engineering routes Field Descriptions

Field	Description
T	Traffic engineering route.
43.0.0.1/32 (not override of routing table entry) is directly connected	Prefix/mask being routed. The routing table does not contain an entry for this prefix/mask.
00:06:35	The time since the route was installed (hours:minutes:seconds).
Tunnel7	The LSP tunnel for the route.

Related Commands

Command	Description
show ip traffic-engineering configuration	Displays information about configured traffic engineering filters and routes.

show ip vrf

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

show ip vrf [{**brief** | **detail** | **interfaces** | **id**}] [*vrf-name*]

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.
vrf-name	(Optional) Name assigned to a VRF.

Command Default

When you do not specify keywords or arguments, the command shows concise information about all configured VRFs.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(17)ST	This command was modified. The id keyword was added. The 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 Virtual access interface (VAI).
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.
12.2SX	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

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.

When you use the **show ip vrf** command, interface and subinterface names are truncated in the output. For example, GigabitEthernet3/1/0.100 is displayed as Gi3/1/0.100.

Examples

Cisco IOS T Train, Cisco IOS SB Train, Cisco IOS B Train, and Cisco IOS SX Train

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          Interfaces
  v1                                20:20               Gi0/2.4294967291
                                                        Gi0/2.4294967293
                                                        Gi0/2.4294967294
                                                        Gi0/2.4294967295
  vpn152-1                          152:1               Lo1
```

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

Table 73: show ip vrf Field Descriptions

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

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 vpn152-1
VRF vpn152-1; default RD 152:1; default VPNID <not set>
VRF Table ID = 2
  Interfaces:
    Lo1
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:152:1
  Import VPN route-target communities
    RT:152:1
  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 74: show ip vrf detail Field Descriptions

Field	Description
default VPNID	Specifies the VPN ID that uniquely identifies every VPN in the network.

Field	Description
VRF Table ID	Uniquely identifies the VRF routing table.
Interfaces	Specifies the network interfaces.
Export VPN route-target communities	Specifies VPN route-target export communities.
Import VPN route-target communities	Specifies VPN route-target import communities.
VRF label distribution protocol	MPLS label distribution protocol in the VRF context. This is required when VRF is configured for Carrier Supporting Carrier (CSC). This could be LDP (enabled via the **mpls ip** command on the VRF interface) or BGP (enabled via the **send-label** command in the router bgp VRF address-family configuration mode).

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

```
Router# show ip vrf interfaces
Interface              IP-Address      VRF                              Protocol
Gi0/2.4294967291       unassigned      v1                               down
Gi0/2.4294967293       unassigned      v1                               down
Gi0/2.4294967294       unassigned      v1                               down
Gi0/2.4294967295       unassigned      v1                               down
Lo1                    10.1.1.1        vpn152-1                         up
```

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

Table 75: 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.

Cisco IOS SR Train

The following example displays output from the **show ip vrf detail** command. The information shown is for a VRF named vpn1.

```
Router# show ip vrf detail vpn1
VRF vpn1 (VRF Id = 1); default RD 1:1; default VPNID <not set>
 Interfaces:
 Lo1                     Lo99                    Et0/0
VRF Table ID = 1
 Export VPN route-target communities
 RT:1:1
 Import VPN route-target communities
  RT:1:1                  RT:2:1
No import route-map
```

```
No export route-map
 VRF label distribution protocol: not configured
 VRF label allocation mode: per-prefix
```

The table above and the table below describe the significant fields shown in the display.

Table 76: show ip vrf detail Field Descriptions

Field	Description
VRF ID	Uniquely identifies the VRF within the router.
VRF label allocation mode	Indicates the type of label mode used based on the route types.

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)	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 ipv6 cef vrf

To display the Cisco Express Forwarding Forwarding Information Base (FIB) associated with an IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **show ipv6 cef vrf**command in user EXEC or privileged EXEC mode.

show ipv6 cef vrf [{*vrf-name* | ***** | **internal**}]

Syntax Description

vrf-name	(Optional) Name assigned to the VRF.
*****	(Optional) All VRFs are displayed.
internal	(Optional) Only internal data is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
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.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use the **show ipv6 cef vrf** command to display content of the IPv6 FIB for the specified VRF.

Examples

The following is sample output from a Cisco Express Forwarding FIB associated with a VRF named cisco1:

```
Router# show ipv6 cef vrf cisco1
 2001:8::/64
  attached to FastEthernet0/0
 2001:8::3/128
  receive
 2002:8::/64
  nexthop 10.1.1.2 POS4/0 label 22 19
 2010::/64
  nexthop 2001:8::1 FastEthernet0/0
 2012::/64
  attached to Loopback1
 2012::1/128
  receive
```

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

Table 77: show ipv6 cef vrf Field Descriptions

Field	Description
2001:8::/64	Specifies the network prefix.
attached to FastEthernet0/0	Specifies the VRF interface.
nexthop 10.1.1.2 POS4/0 label 22 19	Specifies the BGP next hop address.

show ipv6 route vrf

To display IPv6 routing table information associated with a VPN routing and forwarding (VRF) instance, use the **show ipv6 route vrf** command in user EXEC or privileged EXEC mode.

show ipv6 route vrf {*vrf-namevrf-number*}[**tag** {*tag-value* | *tag-value-dotted-decimal* [{*mask*}]}]

Syntax Description

vrf-name	Name assigned to the VRF.
vrf-number	Hexadecimal number assigned to the VRF.
tag	(Optional) Displays information about route tags in the VRF table.
tag-value	(Optional) Displays route tag value in plain decimals.
tag-value-dotted-decimal	(Optional) Displays route tag values in dotted decimals.
mask	(Optional) Route tag wildcard mask.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.2(2)S	This command was integrated into Cisco IOS Release 15.2(2)S. The **tag** keyword and the *tag-value*, *tag-value-dotted-decimal*, and *mask* arguments were added to enable the display of route tags as plain decimals or dotted decimals in the command output.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S. The **tag** keyword and the *tag-value*, *tag-value-dotted-decimal*, and *mask* arguments were added to enable the display of route tags as plain decimals or dotted decimals in the command output.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following sample output from the **show ipv6 route vrf** command displays information about the IPv6 routing table associated with VRF1:

```
Device# show ipv6 route vrf VRF1
```

```
IPv6 Routing Table VRF1 - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
C   2001:DB8:4::2/48 [0/0]
     via ::, FastEthernet0/0
L   2001:DB8:4::3/48 [0/0]
     via ::, FastEthernet0/0
B   2001:DB8:4::4/48 [200/0]
     via ::FFFF:192.168.1.4,
B   2001:DB8:4::5/48 [20/1]
     via 2001:8::1,
C   2001:DB8:4::6/48 [0/0]
     via ::, Loopback1
L   2001:DB8:4::7/48 [0/0]
     via ::, Loopback1
```

The following sample output from the **show ip route vrf** *vrf-name* **tag** command displays information about tagged IPv6 routes in vrf1:

```
Device# show ipv6 route vrf vrf1 tag 0.0.0.6

IPv6 Routing Table - vrf1 - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
Routing entry for 2001::/32
  Known via "static", distance 1, metric 0
  Tag 0.0.0.6
  Route count is 1/1, share count 0
  Routing paths:
    directly connected via Null0
      Last updated 00:00:23 ago
```

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

Table 78: show ipv6 route vrf Field Descriptions

Field	Description
Codes	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—Connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • I—IS-IS derived • L—Local • O—Open Shortest Path First (OSPF) derived • P—Periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—Static • U—Per-user static route
via ::, FastEthernet0/0	Indicates how the route was derived.
Tag	Identifies the tag associated with the remote network.

show isis database verbose

To display details about the Intermediate System-to-Intermediate System (IS-IS) link-state 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.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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.
12.2SX	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 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.6S	This command was modified. Support was added for administrative tags in IPv6 prefixes.

Examples

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

```
Device# 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:   10.5.5.5
  IP Address:  172.16.39.5
  Metric:10         IP 172.16.39.0/24
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
```

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

Table 79: show isis database verbose Field Descriptions

Field	Description
LSPID	Link-state packet (LSP) identifier. The first six octets form the System ID of the router that originated the LSP. 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 Open Shortest Path First (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. 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.
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	Hostname of the node.

Field	Description
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, or b/s).
Reservable BW	Amount of reservable bandwidth on this link, in b/s.
BW Unreserved	Amount of bandwidth that is available for reservation, in b/s.

The following example includes a route tag:

```
Device# 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 172.16.170.0/24
  Metric: 10     IP 10.0.3.0/24
  Metric: 10     IP 10.0.3.3/30
  Metric: 10     IS-Extended dasher.02172.19.170.0/24
  Metric: 20     IP-Interarea 10.1.1.1/32
    Route Admin Tag: 60
  Metric: 20     IP-Interarea 192.168.0.6/32
    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 ldp

To display synchronization and autoconfiguration information about interfaces belonging to Intermediate System-to-Intermediate System (IS-IS) processes, use the **show isis mpls ldp** command in privileged EXEC mode.

show isis [*process-tag*] **mpls ldp** [**interface** *interface*]

Syntax Description

process-tag	(Optional) Process ID. Displays information only for the specified routing process.
interface *interface*	(Optional) Defines the interface for which Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization and LDP autoconfiguration information will be displayed.

Command Modes

Privileged EXEC

Command History

Release	Modifications
12.0(32)SY	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

This command shows Multiprotocol Label Switching (MPLS) LDP synchronization and autoconfiguration information for interfaces that are running IS-IS processes. If you do not specify a keyword or argument, information appears for each interface that is configured for MPLS LDP synchronization and autoconfiguration. MPLS LDP synchronization and autoconfiguration for IS-IS is supported only in Cisco IOS Release 12.0(32)SY.

Examples

In the following example, interface POS0/2 is running IS-IS. Autoconfiguration is enabled. Synchronization is configured.

```
Router# show isis mpls ldp

Interface: POS0/2; ISIS tag null enabled
 ISIS is UP on interface
 AUTOCONFIG Information :
   LDP enabled: YES
 SYNC Information :
   Required: YES
   Achieved: YES
   IGP Delay: NO
   Holddown time: Infinite
   State: SYNC achieved
```

This command returns information for interfaces that are configured for IS-IS, which are indicated by the message “ISIS is UP” on the interface.

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

Table 80: show isis mpls ldp Field Descriptions

Field	Description
AUTOCONFIG Information	LDP enabled--Indicates whether LDP autoconfiguration is enabled on this interface. Value is YES or NO.
SYNC Information	Provides synchronization information. • Required--Indicates whether synchronization is required on the interface. • Achieved--Indicates whether synchronization was achieved with LDP. If IS-IS was configured on an interface but synchronization is not achieved, the Achieved field indicates NO. The Required field still indicates YES. • IGP Delay--Indicates whether the IS-IS process must wait for synchronization with LDP before bringing up the interface adjacency. • Holddown time--Valid values are Finite or Infinite. The finite value is equal to the hold-down delay that you configured using the **mpls ldp igp sync holddown** command. If this field indicates Infinite, hold-down time was not configured. Therefore, IS-IS waits until synchronization is achieved before bringing adjacency UP. The Holddown time field is significant only if the IGP Delay field indicates YES. • State--Indicates information about the state of synchronization on the interface. If synchronization is achieved, the output shows the following: • SYNC achieved--Synchronization was required and has been achieved. If synchronization is not achieved, the output shows one of the following: • • Holding down until SYNC--No hold-down timer was configured, so IS-IS continues to hold down adjacency until synchronization is achieved. • Holding down with timer--A hold-down timer was configured and IS-IS is holding down adjacency until the timer, indicated in the IGP Delay field, expires. • Maximum metric in effect--Although synchronization was not achieved, the IGP brought up adjacency with the maximum metric.

Related Commands

Command	Description
mpls ldp autoconfig	Globally enables LDP autoconfiguration on all interfaces that belong to an OSPF or IS-IS process.
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process or an IS-IS process.

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.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 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  172.16.1.2        PO1/0/0   Up     level-1
04:52:37  0000.0024.0004.02  10.0.0.0          Et0/2     Up     level-1
```

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

Table 81: 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.

Field	Description
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.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 isis mpls traffic-eng advertisements** command:

```
Router# show isis mpls traffic-eng advertisements
System ID:dtp-5.00
  Router ID:10.5.5.5
  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
```

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

Table 82: 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.
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 downstream-tree

To display the Multiprotocol Label Switching (MPLS) traffic engineering Intermediate System-to-Intermediate System (IS-IS) children list for a specific node, use the **show isis mpls traffic-eng downstream-tree** command in privileged EXEC mode.

show isis mpls traffic-eng downstream-tree *system-id* [{**level-1** | **level-2**}]

Syntax Description

system-id	Displays the traffic engineering downstream tree information for the specified system ID as either a hostname or in the MAC address format.
level-1	(Optional) Displays the traffic engineering downstream tree information for the Level 1 database.
level-2	(Optional) Displays the traffic engineering downstream tree information for the Level 2 database.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(24)S	This command was introduced in a release earlier than Cisco IOS Release 12.0(24)S.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
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)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS 2.1 XE	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show isis mpls traffic-eng downstream-tree** command. The fields are self-explanatory.

```
Router# show isis mpls traffic-eng downstream-tree
cr2.amsterdam1
System cr2.amsterdam1.00  with metric 5
   MPLS TE-tunnel Children List
        15   ar5.hilversum1.00
        15   ar5.zwolle1.00
        15   ar5.tilburg1.00
        15   ar5.wageningen.00
        15   ar5.groningen1.00
        15   ar5.enschede1.00
        15   ar5.nijmegen1.00
        15   cr1.amsterdam1.00
         1   cr1.amsterdam1.00
        25   ar5.denhaag1.00
        25   ar5.delft1.00
        25   ar5.leiden1.00
        25   ar5.rotterdam1.00
```

```
25   ar5.amsterdam1.00
25   ar5.eindhoven1.00
25   ar5.maastricht.00
```

Related Commands

Command	Description
show isis mpls traff9c-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 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.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 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         10.2.2.2       -3       Relative
                    Tunnel1021    10000        10.2.2.2       11       Absolute
tomklong-route.00   Tunnel1031    10000        172.17.3.3       -1       Relative
                    Tunnel1032    10000        172.17.3.3
```

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

Table 83: 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.

Field	Description
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.

show issu clients

To display a list of the current In Service Software Upgrade (ISSU) clients--that is, the network applications and protocols supported by ISSU--use the **show issu clients**command in user EXEC or privileged EXEC mode.

show issu clients

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

This command lists all ISSU clients currently operating in the network, along with their Client ID numbers and the number of entities each client contains.

You should enter this command before you enter the **issu runversion** command, because if a client (application or protocol) that needs to continue operating in the network does not appear in the displayed list, you will know not to continue the software upgrade (because proceeding further with ISSU would then halt the operation of that application or protocol).

Examples

The following example shows a client list displayed by entering this command:

```
Router# show issu clients
Client_ID = 2,  Client_Name = ISSU Proto client,  Entity_Count = 1
Client_ID = 3,  Client_Name = ISSU RF,  Entity_Count = 1
Client_ID = 4,  Client_Name = ISSU CF client,  Entity_Count = 1
Client_ID = 5,  Client_Name = ISSU Network RF client,  Entity_Count = 1
Client_ID = 7,  Client_Name = ISSU CONFIG SYNC,  Entity_Count = 1
Client_ID = 8,  Client_Name = ISSU ifIndex sync,  Entity_Count = 1
Client_ID = 9,  Client_Name = ISSU IPC client,  Entity_Count = 1
Client_ID = 10,  Client_Name = ISSU IPC Server client,  Entity_Count = 1
Client_ID = 11,  Client_Name = ISSU Red Mode Client,  Entity_Count = 1
Client_ID = 12,  Client_Name = ISSU EHSA services client,  Entity_Count = 1
Client_ID = 100,  Client_Name = ISSU rfs client,  Entity_Count = 1
Client_ID = 110,  Client_Name = ISSU ifs client,  Entity_Count = 1
Client_ID = 1001,  Client_Name = OC3POS-6,  Entity_Count = 4
Client_ID = 1002,  Client_Name = C10K ATM,  Entity_Count = 1
Client_ID = 1003,  Client_Name = C10K CHSTM1,  Entity_Count = 1
Client_ID = 1004,  Client_Name = C10K CT3,  Entity_Count = 1
Client_ID = 1005,  Client_Name = C10K GE,  Entity_Count = 1
Client_ID = 1006,  Client_Name = C10K ET,  Entity_Count = 1
Client_ID = 1007,  Client_Name = C10K CHE1T1,  Entity_Count = 1
Client_ID = 1009,  Client_Name = C10K MFE,  Entity_Count = 1
Client_ID = 1010,  Client_Name = C10K APS,  Entity_Count = 1
Client_ID = 1013,  Client_Name = C10K CARD OIR,  Entity_Count = 1
Client_ID = 2002,  Client_Name = CEF Push ISSU client,  Entity_Count = 1
```

```
Client_ID = 2003,  Client_Name = ISSU XDR client,  Entity_Count = 1
Client_ID = 2004,  Client_Name = ISSU SNMP client,  Entity_Count = 1
Client_ID = 2005,  Client_Name = ISSU HDLC Client,  Entity_Count = 1
Client_ID = 2006,  Client_Name = ISSU QoS client,  Entity_Count = 1
Client_ID = 2007,  Client_Name = ISSU LSD Label Mgr HA Client,  Entity_Count = 1
Client_ID = 2008,  Client_Name = ISSU Tableid Client,  Entity_Count = 1
Client_ID = 2009,  Client_Name = ISSU MPLS VPN Client,  Entity_Count = 1
Client_ID = 2010,  Client_Name = ARP HA,  Entity_Count = 1
Client_ID = 2011,  Client_Name = ISSU LDP Client,  Entity_Count = 1
Client_ID = 2012,  Client_Name = ISSU HSRP Client,  Entity_Count = 1
Client_ID = 2013,  Client_Name = ISSU ATM Client,  Entity_Count = 1
Client_ID = 2014,  Client_Name = ISSU FR Client,  Entity_Count = 1
Client_ID = 2015,  Client_Name = ISSU REDSSOC client,  Entity_Count = 1
Client_ID = 2019,  Client_Name = ISSU TCP client,  Entity_Count = 1
Client_ID = 2020,  Client_Name = ISSU BGP client,  Entity_Count = 1
Client_ID = 2021,  Client_Name = XDR Int Priority ISSU client,  Entity_Count = 1
Client_ID = 2022,  Client_Name = XDR Proc Priority ISSU client,  Entity_Count = 1
Client_ID = 2023,  Client_Name = FIB HWIDB ISSU client,  Entity_Count = 1
Client_ID = 2024,  Client_Name = FIB IDB ISSU client,  Entity_Count = 1
Client_ID = 2025,  Client_Name = FIB HW subblock ISSU client,  Entity_Count = 1
Client_ID = 2026,  Client_Name = FIB SW subblock ISSU client,  Entity_Count = 1
Client_ID = 2027,  Client_Name = Adjacency ISSU client,  Entity_Count = 1
Client_ID = 2028,  Client_Name = FIB IPV4 ISSU client,  Entity_Count = 1
Client_ID = 2030,  Client_Name = MFI Pull ISSU client,  Entity_Count = 1
Client_ID = 2031,  Client_Name = MFI Push ISSU client,  Entity_Count = 1
Client_ID = 2051,  Client_Name = ISSU CCM Client,  Entity_Count = 1
Client_ID = 2052,  Client_Name = ISSU PPP SIP CCM Client,  Entity_Count = 1
Client_ID = 2054,  Client_Name = ISSU process client,  Entity_Count = 1
Base Clients:
 Client_Name = ISSU Proto client
 Client_Name = ISSU RF
 Client_Name = ISSU CF client
 Client_Name = ISSU Network RF client
 Client_Name = ISSU CONFIG SYNC
 Client_Name = ISSU ifIndex sync
 Client_Name = ISSU IPC client
 Client_Name = ISSU IPC Server client
 Client_Name = ISSU Red Mode Client
 Client_Name = ISSU EHSA services client
```

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

Table 84: show issu clients Field Descriptions

Field	Description
Client_ID	The identification number used by ISSU for that client.

Field	Description
Client_Name	A character string describing the client. "Base Clients" are a subset, which includes: • Inter-Process Communications (IPC) • Redundancy Framework (RF) • Checkpoint Facility (CF) • Cisco Express Forwarding • Network RF (for IDB stateful switchover) • EHSA Services (including ifIndex) • Configuration Synchronization.
Entity_Count	The number of entities within this client. An entity is a logical group of sessions with some common attributes.

Related Commands

Command	Description
show issu message types	Displays the formats, versions, and size of ISSU messages supported by a particular client.
show issu negotiated	Displays results of a negotiation that occurred concerning message versions or client capabilities.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status is compatible for the impending software upgrade.

show issu entities

To display information about entities within one or more In Service Software Upgrade (ISSU) clients, use the **show issu entities**command in user EXEC or privileged EXEC mode.

show issu entities [*client-id*]

Syntax Description

client-id	(Optional) The identification number of a single ISSU client.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

An entity is a logical group of sessions that possess some common attributes. Enter a Client_ID if you are interested in seeing information only about one client's entities. If a Client_ID is not specified, the command will display all ISSU clients' entities known to the device.

If you are not sure of the precise Client_ID number to enter for the client you are interested in, use the **show issu clients** command to display the current list of clients with their names and ID numbers.

Examples

The following example shows detailed information about the entities within the virtual routing and forwarding (VRF) ("Table ID") client:

```
Router# show issu entities 2008
Client_ID = 2008 :
      Entity_ID = 1,  Entity_Name = Tableid Entity :
         MsgType MsgGroup CapType CapEntry CapGroup
          Count    Count   Count   count    Count
   2   2   1   2   2
```

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

Table 85: show issu entities Field Descriptions

Field	Description
Client_ID	The identification number used by ISSU for the specified client.
Entity_ID	The identification number used by ISSU for each entity within this client.
Entity_Name	A character string describing the entity.
MsgType Count	The number of message types within the identified entity.
MsgGroup Count	The number of message groups within the identified entity. A message group is a list of message types.

Field	Description
CapType Count	The number of capability types within the identified entity.
CapEntry Count	The number of capability entries within the identified entity. A capability entry is a list of all mutually dependent capability types within a particular client session and, optionally, other capability types belonging to that client session.
CapGroup Count	The number of capability groups within the identified entity. A capability group is a list of capability entries given in priority sequence.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients--that is, the applications and protocols on this network supported by ISSU.
show issu sessions	Displays detailed information about a particular ISSU client--including whether the client status for the impending software upgrade is COMPATIBLE.

show issu message types

To display formats (“types”), versions, and maximum packet size of the In Service Software Upgrade (ISSU) messages supported by a particular client, use the **show issu message types**command in user EXEC or privileged EXEC mode.

show issu message types *client-id*

Syntax Description

client-id	The identification number used by ISSU for a client application.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

If you are not sure of the Client_ID number to enter into this command, use the **show issu clients** command. It displays the current list of clients, along with their names and ID numbers.

Examples

The following example displays the message type, version, and maximum message size supported by the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) client:

```
Router# show issu message types 2009
Client_ID = 2009,  Entity_ID = 1 :
   Message_Type = 1,  Version_Range = 1 ~ 1
         Message_Ver = 1,    Message_Mtu = 32
```

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

Table 86: show issu message types Field Descriptions

Field	Description
Client_ID	The identification number used by ISSU for this client.
Entity_ID	The identification number used by ISSU for this entity.
Message_Type	An identification number that uniquely identifies the format used in the ISSU messages conveyed between the two endpoints.
Version_Range	The lowest and highest message-version numbers contained in the client application.
Message_Ver	Message version. Because each client application contains one or more versions of its messages, ISSU needs to discover these versions and negotiate between the new and old system software which version to use in its preparatory communications.

Field	Description
Message_Mtu	Maximum size (in bytes) of the transmitted message. A value of 0 means there is no restriction on size; fragmentation and reassembly are therefore being handled in a manner transparent to the ISSU infrastructure.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients--that is, the applications on this network supported by ISSU.
show issu negotiated	Displays results of a negotiation that occurred concerning message versions or client capabilities.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status is compatible for the impending software upgrade.

show issu negotiated

To display details of the session's negotiation about message version or client capabilities, use the **show issu negotiated**command in user EXEC or privileged EXEC mode.

show issu negotiated {**version** | **capability**} *session-id*

Syntax Description

version	Displays results of a negotiation about versions of the messages exchanged during the specified session, between the active and standby endpoints.
capability	Displays results of a negotiation about the client application's capabilities for the specified session.
session-id	The number used by In Service Software Upgrade (ISSU) to identify a particular communication session between the active and the standby devices.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

If you are not sure of the session_ID number to enter into this command, enter the **show issu sessions** command. It will display the session_ID.

Examples

The following example displays the results of a negotiation about message versions:

```
router# show issu negotiated version 39
Session_ID = 39 :
    Message_Type = 1,  Negotiated_Version = 1,  Message_MTU = 32
```

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

Table 87: show issu negotiated version Field Descriptions

Field	Description
Session_ID	The identification number of the session being reported on.
Message_Type	An identification number that uniquely identifies the format that was used by the ISSU messages conveyed between the two endpoints.
Negotiated_Version	The message version that was decided upon, for use during the software upgrade process.
Message_Mtu	Maximum size (in bytes) of the transmitted message. A value of 0 means there is no restriction on size. In that case, fragmentation and reassembly are handled in a manner transparent to the ISSU infrastructure.

The following example displays the results of a negotiation about the client application's capabilities:

```
router# show issu negotiated capability 39
Session_ID = 39 :
     Negotiated_Cap_Entry = 1
```

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

Table 88: show issu negotiated capability Field Descriptions

Field	Description
Session_ID	The identification number of the session being reported on.
Negotiated_Cap_Entry	A numeral that stands for a list of the negotiated capabilities in the specified client session.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients--that is, the applications on this network supported by ISSU.
show issu message types	Displays the formats, versions, and maximum packet size of ISSU messages supported by a particular client.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status is compatible for the impending software upgrade.

show issu sessions

To display detailed information about a particular In Service Software Upgrade (ISSU) client--including whether the client status for the impending software upgrade is compatible--use the **show issu sessions**command in user EXEC or privileged EXEC mode.

show issu sessions *client-id*

Syntax Description

client-id	The identification number used by ISSU for the client.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

If you are not sure of the Client_ID number to enter into this command, use the **show issu clients** command to display the current list of clients with their names and ID numbers.

Examples

The following example shows detailed information about the LDP Client:

```
Router# show issu sessions 2011
 Client_ID = 2011,  Entity_ID = 1 :
 *** Session_ID = 46,  Session_Name = LDP Session :
    Peer    Peer  Negotiate  Negotiated   Cap      Msg     Session
  UniqueID  Sid     Role       Result   GroupID  GroupID  Signature
     4       34   PRIMARY   COMPATIBLE    1        1         0
                           (no policy)
    Negotiation Session Info for This Message Session:
         Nego_Session_ID = 46
         Nego_Session_Name = LDP Session
         Transport_Mtu = 3948
```

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

Table 89: show issu sessions Field Descriptions

Field	Description
Client_ID	The identification number used by ISSU for that client.
Entity_ID	The identification number used by ISSU for each entity within this client.
Session_ID	The identification number used by ISSU for this session.
Session_Name	A character string describing the session.

Field	Description
Peer UniqueID	An identification number used by ISSU for a particular endpoint, such as a Route Processor or line card (could be a value based on slot number, for example). The peer that has the smaller unique_ID becomes the Primary (initiating) side in the capability and message version negotiations.
Peer Sid	Peer session ID.
Negotiate Role	Negotiation role of the endpoint: either PRIMARY (in which case the device initiates the negotiation) or PASSIVE (in which case the device responds to a negotiation initiated by the other device).
Negotiated Result	The features ("capabilities") of this client's new software were found to be either COMPATIBLE or INCOMPATIBLE with the intended upgrade process. ("Policy" means that an override of the negotiation result has been allowed by the software. Likewise, "no policy" means that no such override is present to be invoked).
Cap GroupID	Capability group ID: the identification number used for a list of distinct functionalities that the client application contains.
Msg GroupID	Message group ID: the identification number used for a list of formats employed when conveying information between the active device and the standby device.
Session Signature	Session signature: a unique ID to identify a current session in a shared negotiation scenario.
Nego_Session_ID	Negotiation session ID: the identification number used by ISSU for this negotiation session.
Nego_Session_Name	Negotiation session name: a character string describing this negotiation session.
Transport_Mtu	Maximum packet size (in bytes) of the ISSU messages conveyed between the two endpoints. A value of 0 means there is no restriction on size; in this case, fragmentation and reassembly then are handled in a manner transparent to the ISSU infrastructure.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients--that is, the applications on this network supported by ISSU.
show issu message types	Displays the formats, versions, and maximum packet size of ISSU messages supported by a particular client.
show issu negotiated	Displays results of a negotiation that occurred concerning message versions or client capabilities.

show l2vpn atom binding

To display Layer 2 VPN (L2VPN) Any Transport over MPLS (AToM) label binding information, use the **show l2vpn atom binding** command in privileged EXEC mode.

show l2vpn atom binding [{*vc-idip-address* | **local-label** *number* | **pseudowire** *int-number* | **remote-label** *number*}]

Syntax Description

vc-id	(Optional) Displays L2VPN AToM label binding information for the specified virtual circuit (VC).
ip-address	(Optional) Displays L2VPN AToM label binding information for the specified VC destination.
local-label *number*	(Optional) Displays L2VPN AToM label binding information for the specified local assigned label.
pseudowire *int-number*	(Optional) Displays pseudowire interface number.
remote-label *number*	(Optional) Displays L2VPN AToM label binding information for the specified remote assigned label.

Command Modes

Privileged EXEC (#)

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 **show mpls l2transport binding** 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 the L2VPN AToM label binding information:

```
Device# show l2vpn atom binding

Destination Address: 10.5.5.51,  VC ID: 108
    Local Label:  1001
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1]
              CV Type: None
    Remote Label: 16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: "This is Left PE"
        VCCV: CC Type: CW [1], RA [2], TTL [3]
              CV Type: LSPV [2], BFD [3]
```

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

Table 90: show l2vpn atom binding Field Descriptions

Field	Description
Destination Address	IP address of the interface on the remote device to which the VC has been established.
VC ID	The VC identifier assigned to one of the interfaces on the device.
Local Label	The VC label that a device signals to its peer device, which is used by the peer device during imposition.
Remote Label	The disposition VC label of the remote peer device.
Cbit	The control word bit. If it is set, the value is 1.
VC Type	The type of VC, such as ATM, Ethernet, and Frame Relay.
GroupID	The group ID assigned to the local or remote VCs.
MTU	The maximum transmission unit assigned.
Interface Desc	Interface parameters, if applicable.
VCCV Capabilities	Any Transport over Multi Protocol Label Switching (AToM) Virtual Circuit Connectivity Verification (VCCV) information. This field displays how an AToM VCCV packet is identified. • Type 1—The Protocol ID field of the AToM Control Word (CW) is identified in the AToM VCCV packet. • Type 2—An MPLS Router Alert (RA) Level above the VC label identified in the AToM VCCV packet. Type 2 is used for VC types that do not support or do not interpret the AToM Control Word.
VCCV: CC Type	Type of Control Channel (CC) processing that are supported. The number indicates the position of the bit that was set in the received octet. The following values can be displayed: • CW [1]—Control Word • RA [2]—Router Alert • TTL [3]—Time to Live • Unkn [x]—Unknown

Field	Description
CV Type	Type of Connectivity Verification (CV) packets that can be processed in the control channel of the MPLS pseudowire. The following are the CV packets that can be processed. The number following the CV type indicates the position of the bit that was set in the received octet. • ICMP [1]—Internet Control Management Protocol (ICMP) is used to verify connectivity. • LSPV [2]—Link-state packet (LSP) ping is used to verify connectivity. • BFD [3]—Bidirectional Forwarding Detection (BFD) is used to verify connectivity for more than one pseudowire. • Unkn [x]—A CV type was received that could not be interpreted.

The following sample output shows information about L2VPN multisegment pseudowires:

```
Device# show l2vpn atom binding

Destination Address: 10.1.1.1,  VC ID: 102
    Local Label:  17
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2], TTL [3]
              CV Type: LSPV [2]
    Remote Label: 16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2], TTL [3]
              CV Type: LSPV [2]
        PW Switching Point:
Vcid   local IP addr      remote IP addr      Description
101        10.11.11.11    10.20.20.20         PW Switching Point PE3
100        10.20.20.20    10.11.11.11         PW Switching Point PE2
```

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

Table 91: show l2vpn atom binding Field Descriptions for Multisegment Pseudowires

Field	Description
TTL	Time to live (TTL) setting of the label.
Vcid	VC identifier.
local IP addr	Local IP address assigned to the switching point.
remote IP addr	Remote IP address assigned to the switching point.
Description	Description assigned to the switching point.

Related Commands

Command	Description
cell-packing	Enables ATM over MPLS or L2TPv3 to pack multiple ATM cells into each MPLS or L2TPv3 packet.
show l2vpn atom hw-capability	Displays the transport types and their supported capabilities.
show l2vpn atom vc	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a device.
show mpls l2transport binding	Displays VC label binding information.

show l2vpn atom checkpoint

To display checkpointing information about Layer 2 VPN (L2VPN) Any Transport over Multiprotocol Label Switching (AToM) virtual circuits (VCs), use the **show l2vpn atom checkpoint** command in privileged EXEC mode.

show l2vpn atom checkpoint

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

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 **show mpls l2transport checkpoint** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

The output of the commands varies, depending on whether the output reflects the active or standby Route Processor (RP). In general, the output on the active RP shows that checkpointing information is sent to the backup RP. The output on the backup RP shows that checkpointing information is received from the active RP.

Examples

On the active RP, the command displays the following output:

```
Device# show l2vpn atom checkpoint

AToM Checkpoint info for active RP
Checkpointing is allowed
Bulk-sync checkpointed state for 1 VC
```

On the standby RP, the command displays the following output:

```
Device# show l2vpn atom checkpoint

AToM HA Checkpoint info for standby RP
1 checkpoint information block in use
```

The output fields are self-explanatory.

Related Commands

Command	Description
show l2vpn atom vc	Displays information about the checkpointed data when checkpointing is enabled.
show mpls l2transport checkpoint	Displays information of MPLS Layer 2 transport checkpointed data when checkpointing is enabled.

show l2vpn atom hw-capability

To display the transport types supported on an interface, use the **show l2vpn atom hw-capability** command in privileged EXEC mode.

show l2vpn atom hw-capability interface *type number*

Syntax Description

interface	Displays information for the specified interface.
type number	Type and number of the interface.

Command Modes

Privileged EXEC (#)

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 **show mpls l2transport hw-capability** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the **show l2vpn atom hw-capability** command to determine the interface to use for the various transport types. Use this command to check if core-facing and edge-facing interfaces can accommodate different transport types.

Examples

The following is sample output from the **show l2vpn atom hw-capability** command:

```
Device# show l2vpn atom hw-capability interface serial5/1

Interface Serial5/1
Transport type FR DLCI
  Core functionality:
    MPLS label disposition supported
    Control word processing supported
    Sequence number processing not supported
  Edge functionality:
    MPLS label imposition supported
    Control word processing supported
    Sequence number processing not supported
    !
    !
    !
```

Note These examples show only a portion of the output. The command displays the capabilities of every transport type.

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

Table 92: show l2vpn atom hw-capability Field Descriptions

Field	Description
Transport type	Indicates the transport type.
Core functionality	Displays the functionalities that the core-facing interfaces support, such as label disposition, control word, and sequence number processing.
Edge functionality	Displays the functionalities that the edge-facing interfaces support, such as label disposition, control word, and sequence number processing.

Related Commands

Command	Description
show l2vpn atom binding	Displays VC label binding information.
show l2vpn atom checkpoint	Displays the checkpoint information about AToM VCs.
show l2vpn atom summary	Displays summary information about VCs.
show l2vpn atom vc	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a device.
show mpls l2transport hw-capability	Displays the transport types supported on an interface.

show l2vpn atom memory

To display the Layer 2 VPN (L2VPN) Any Transport over MPLS (AToM) memory usage information, use the **show l2vpn atom memory** command in privileged EXEC mode.

show l2vpn atom memory [{**detail**}]

Syntax Description

detail	(Optional) Displays detailed information for L2VPN AToM memory usage.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **show mpls l2transport memory** command in future releases.

Examples

The following is sample output from the **show l2vpn atom memory detail** command:

```
Device# show l2vpn atom memory detail

AToM memory                  In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  AToM LDP Adj Chunk      :        --       320/592          --    32   10/10
  AToM LDP Chunk          :        --       400/664          --    40   10/10
  AToM LDP DB             :        --     32760/36272        --    40  512/819
  AToM LDP pw tlv chunk   :        --      2816/3272         --   256   10/11
  AToM LDP sw point subtl :        --      1456/1776         --   104   10/14
  AToM Mgr VC Table       :        --     32760/36272        --    40  512/819
  AToM Seg Context        :        76       76/128           1    76   --/--
  AToM Test LDP           :        --     32760/36272        --    40  512/819
  Total                   :        76    103348/115248       1    --   --/--

 AToM structs                 In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  atom_mgr_vc_t           :        --        --/--            --   584   --/--
  atom_mgr_sig_t          :        --        --/--            --    44   --/--
  atom_vc_msg_t           :        --        --/--            --   392   --/--
```

Related Commands

Command	Description
show l2vpn atom summary	Displays summary information about VCs that have been enabled to route AToM Layer 2 packets on a device.
show mpls l2transport memory	Displays the L2VPN AToM memory usage information.

show l2vpn atom pwid

To display Layer 2 VPN (L2VPN) Any Transport over MPLS (AToM) dataplane pseudowire identifier usage information, use the **show l2vpn atom pwid** command in privileged EXEC mode.

show l2vpn atom pwid

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command wasS introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support.. This command will replace the **show mpls l2transport pwid** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Examples

The following is sample output from the **show l2vpn atom pwid** command. The output fields are self-explanatory.

```
Device# show l2vpn atom pwid

AToM Pseudowire IDs: In use: 1, In holddown: 0

Label  Peer-Address    VCID       PWID       In-Use FirstUse ResuedAt FreedAt
------ --------------- ---------- ---------- ------ -------- -------- --------
0      10.1.1.1        4500       1          Yes    00:22:44 Never    Never
```

Related Commands

Command	Description
show l2vpn atom binding	Displays VC label binding information.
show l2vpn atom checkpoint	Displays the checkpoint information about AToM VCs.
show l2vpn atom summary	Displays summary information about VCs.
show l2vpn atom vc	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a device.
show mpls l2transport pwid	Displays Layer 2 transport dataplane pseudowire identifier usage information.

show l2vpn atom static-oam

To display the status of Layer 2 VPN (L2VPN) Any Transport over MPLS (AToM) static pseudowires, use the **show l2vpn atom static-oam** command in privileged EXEC mode.

show l2vpn atom static-oam [**fault** [{**inbound** | **outbound**}]] [**event-trace**] [*ip-address vc-id*]

Syntax Description

fault	(Optional) Displays faults related to static pseudowires.
inbound	(Optional) Displays faults related to inbound static pseudowires.
outbound	(Optional) Displays faults related to outbound static pseudowires.
event-trace	(Optional) Displays event trace information related to static pseudowires.
ip-address	(Optional) Displays information related to the static pseudowire with the specified peer IP address.
vc-id	(Optional) Displays information related to the static pseudowire with the specified virtual circuit (VC) ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **show mpls l2transport static-oam** 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 enable the display of status messages for the static pseudowire with peer IP address of 10.10.10.10 and VC ID of 4:

```
Device# show l2vpn atom static-oam 10.10.10.10 4

Peer IP address: 10.10.10.10, VC ID: 4, Protocol: MPLS, PW ID: 1
  Configured Parameters:
    Refresh send rate: 30 sec
    Refresh recv rate: 600 sec
    Ack disabled
  Negotiated Parameters:
    Peer refresh rate: 0 sec
    Requested refresh rate: 0 sec
  Remote Fault:
    FSM state: No Remote Fault, status code: fwding
  Local Fault:
    FSM state: No Local Fault, status code: fwding
```

Related Commands

Command	Description
debug l2vpn atom static-oam	Enables the display of messages related to static pseudowire OAM.
show mpls l2transport static-oam	Displays the status of MPLS TP static pseudowires.

show l2vpn atom summary

To display summary information about virtual circuits (VCs) that have been enabled to route Any Transport over MPLS (AToM) Layer 2 packets on a device, use the **show l2vpn atom summary** command in privileged EXEC mode.

show l2vpn atom summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

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 **show mpls l2transport summary** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

This command will replace the **show mpls l2transport summary** command in future releases.

Examples

The following is sample output from the command that shows summary information about the VCs that have been enabled to transport Layer 2 packets:

```
Device# show l2vpn atom summary

Destination address: 10.16.24.12 Total number of VCs: 60
0 unknown, 58 up, 0 down, 2 admin down
5 active vc on MPLS interface PO4/0
```

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

Table 93: show l2vpn atom summary Field Descriptions

Field	Description
Destination address	IP address of the remote device to which the VC has been established.
Total number of VCs	Number of VCs that are established.
unknown	Number of VCs that are in an unknown state.
up	Number of VCs that are operational.
down	Number of VCs that are not operational.
admin down	Number of VCs that have been disabled.

Related Commands

Command	Description
show l2vpn atom binding	Displays VC label binding information.
show l2vpn atom checkpoint	Displays the checkpoint information about AToM VCs.
show l2vpn atom hw-capability	Displays the transport types and their supported capabilities.
show l2vpn atom vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a device.
show mpls l2transport summary	Displays summary information about VCs that have been enabled to route AToM Layer 2 packets on a device.

show l2vpn atom vc

To display information about Any Transport over MPLS (AToM) virtual circuits (VCs) and static pseudowires that have been enabled to route Layer 2 packets on a device, use the **show l2vpn atom vc** command in user EXEC or privileged EXEC mode.

show l2vpn atom vc [[**vcid**] *vc-id-min*] [*vc-id-max*] [**interface** *type number* [*local-circuit-id*]] [**destination** {*ip-addresshostname*}] [**detail**] [**pwid** *pw-identifier*] [**vpls-id** *vpls-identifier*] [**stitch** *endpoint endpoint*]

Syntax Description

vcid	(Optional) Displays the VC ID.
vc-id-min	(Optional) Minimum VC ID value. The range is from 1 to 4294967295.
vc-id-max	(Optional) Maximum VC ID value. The range is from 1 to 4294967295.
interface	(Optional) Displays the interface or subinterface of the device that has been enabled to transport Layer 2 packets. Use this keyword to display information about the VCs that have been assigned VC IDs on that interface or subinterface.
type	(Optional) Interface type. For more information about the interface type, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
local-circuit-id	(Optional) The number assigned to the local circuit. This argument value is supported only with the following transport types: • For Frame Relay, enter the data-link connection identifier (DLCI) of the permanent virtual circuit (PVC). • For ATM adaptation layer 5 (AAL5) and cell relay, enter the virtual path identifier (VPI) or virtual channel identifier (VCI) of the PVC. • For Ethernet VLANs, enter the VLAN number.
destination	(Optional) Displays the remote device.
ip-address	(Optional) IP address of the remote device.
hostname	(Optional) The name assigned to the remote device.
detail	(Optional) Displays detailed information about VCs.

pwid *pw-identifier*	(Optional) Displays the number of a pseudowire for a single VC. The range is from 1 to 4294967295.
vpls-id *vpls-identifier*	(Optional) Virtual Private LAN Switching (VPLS) ID extended community value.
stitch *endpoint endpoint*	(Optional) Displays information about dynamically stitched pseudowires between specified endpoints. The endpoints are the Source Attachment Individual Identifier (SAII) and the Target Attachment Individual Identifier (TAII). When the **stitch** keyword is used with the **vpls-id** keyword, a single pair of stitched VCs is displayed.

Command Default

The command displays a summary of all the VCs.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **show mpls l2transport vc** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

The output of the commands varies based on the type of Layer 2 packets being transported over AToM VCs.

Examples

The following is sample output from the **show l2vpn atom vc** command, which displays information about interfaces and VCs that are configured to transport various Layer 2 packets on the device:

```
Device# show l2vpn atom vc

Local intf     Local circuit      Dest address    VC ID      Status
-------------  ------------------ --------------- ---------- ----------
Se5/0          FR DLCI 55         10.0.0.1        55         UP
AT4/0          ATM AAL5 0/100     10.0.0.1        100        UP
AT4/0          ATM AAL5 0/200     10.0.0.1        200        UP
AT4/0.300      ATM AAL5 0/300     10.0.0.1        300        UP
```

The table below describes the fields shown in the display.

Table 94: show l2vpn atom vc Field Descriptions

Field	Description
Local intf	Interface on the local device that is enabled to transport Layer 2 packets.

Field	Description
Local circuit	Type and number (if applicable) of the local circuit. The output shown in this column varies, depending on the transport type: • For Frame Relay, the output shows the DLCI of the PVC. • For ATM cell relay and AAL5, the output shows the VPI or VCI of the PVC. • For Ethernet VLANs, the output shows the VLAN number. • For PPP and High-Level Data Link Control (HDLC), the output shows the interface number.
Dest address	IP address of the remote device's interface that is the other end of the VC.
VC ID	VC identifier assigned to one of the interfaces on the device.

Status	Status of the VC, which can be one of the following:
	• Admin down—The VC is disabled by a user.
	• Down—The VC is not ready to carry traffic between the two VC endpoints. Use the **detail** keyword to determine the reason that the VC is down.
	• Hotstandby—The active pseudowire on a standby Route Processor (RP).
	• Recovering—The VC is recovering from a stateful switchover.
	• Standby—The VC is designated as the backup circuit in a stateful switchover configuration.
	• Up—The VC can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are programmed.
	  • The disposition interface is programmed if the VC is configured and the client interface is up.
	  • The imposition interface is programmed if the disposition interface is also programmed, and a remote VC label and an Interior Gateway Protocol (IGP) label are configured. The IGP label can be implicit null in a back-to-back configuration. The IGP label implies that there is a label switched path (LSP) to the peer.

The following is sample output from the **show l2vpn atom vc detail** command and shows information about the nonstop forwarding (NSF), stateful switchover (SSO), and graceful restart capabilities on the AToM VC. The SSO portion indicates whether checkpoint data is sent (on active) or received (on standby). When SSO data is successfully sent or is released, the SSO information is not displayed.

```
Device# show l2vpn atom vc detail

Local interface: Fa5/1/1.2 down, line protocol down, Eth VLAN 2 up
  Destination address: 10.55.55.2, VC ID: 1002, VC status: down
    Output interface: Se4/0/3, imposed label stack {16}
    Preferred path: not configured
 Default path: active
    Tunnel label: imp-null, next hop point2point
  Create time: 02:03:29, last status change time: 02:03:26
  Signaling protocol: LDP, peer 10.55.55.2:0 down
```

```
   MPLS VC labels: local 16, remote unassigned
   Group ID: local 0, remote unknown
   MTU: local 1500, remote unknown
   Remote interface description:
  Sequencing: receive disabled, send disabled
  SSO Descriptor: 10.55.55.2/1002, local label: 16
    SSM segment/switch IDs: 12290/8193, PWID: 8193
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

The following is sample output from the **show l2vpn atom vc detail** command and shows the information that is displayed when an AToM static pseudowire is provisioned and the command is used to check the configuration. The Signaling protocol field specifies “Manual” because a directed control protocol such as Label Distribution Protocol (LDP) cannot be used to exchange parameters on static pseudowires. The remote interface description field seen for nonstatic pseudowire configurations is not displayed because remote information is exchanged using signaling between the provider edge (PE) devices and not on static pseudowires.

```
Device# show l2vpn atom vc detail

Local interface: Et1/0 up, line protocol up, Ethernet up
   Destination address: 10.1.1.2, VC ID: 100, VC status: up
     Output interface: Et2/0, imposed label stack {10003 150}
     Preferred path: not configured
     Default path: active
     Next hop: 10.0.0.2
   Create time: 00:18:57, last status change time: 00:16:10
   Signaling protocol: Manual
     MPLS VC labels: local 100, remote 150
     Group ID: local 0, remote 0
     MTU: local 1500, remote 1500
     Remote interface description:
   Sequencing: receive disabled, send disabled
   VC statistics:
     packet totals: receive 219, send 220
     byte totals:   receive 20896, send 26694
     packet drops:  receive 0, send 0
```

The following is sample output from the **show l2vpn atom vc detail** command and shows VC statistics, including the number of packets and bytes being sent from the device. The VC statistics fields include the word “transit” to indicate that the packet totals no longer include packets being sent to the device.

```
Device# show l2vpn atom vc detail

Local interface: Et1/0 up, line protocol up, Ethernet up
.
.
.
VC statistics:
     transit packet totals: receive 219, send 220
     transit byte totals:   receive 20896, send 26694
     transit packet drops:  receive 0, send 0
```

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

Table 95: show l2vpn atom vc detail Field Descriptions

Field	Description
Local interface	Interface on the local device that has been enabled to send and receive Layer 2 packets. The interface varies, depending on the transport type. The output also shows the status of the interface.
line protocol	Status of the line protocol on the edge-facing interface.
Destination address	IP address of the remote device specified for the VC. Specify the destination IP address as part of the **mpls l2transport route** command.
VC ID	VC identifier assigned to the interface on the device.

VC status	Status of the VC, which can be one of the following:
	• Admin down—The VC was disabled by a user.
	• Down—The VC is not ready to carry traffic between the two VC endpoints.
	• up—The VC is in a state where it can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are enabled.
	  • The disposition interface is enabled if the VC is configured and the client interface is up.
	  • The imposition interface is enabled if the disposition interface is enabled and a remote VC label and an IGP label exist. The IGP label can be an implicit null in a back-to-back configuration. (An IGP label implies that there is an LSP to the peer.)

Output interface	Interface on the remote device that has been enabled to transmit and receive Layer 2 packets.
imposed label stack	Summary of the Multiprotocol Label Switching (MPLS) label stack used to direct the VC to the PE device.
Preferred path	Path that was assigned to the VC and the status of that path. The path can be an MPLS traffic engineering tunnel or an IP address or hostname of a peer PE device.
Default path	Status of the default path, which can be disabled or active. By default, if the preferred path fails, the device uses the default path. However, you can disable the device from using the default path when the preferred path fails by specifying the **disable-fallback** keyword with the **preferred-path** command.

Field	Description
Tunnel label	IGP label used to route the packet over the MPLS backbone to the destination device. The first part of the output displays the type of label. The second part of the output displays the route information. The tunnel label information can display any of the following states: • imp-null—Implicit null means that the provider device is absent and the tunnel label will not be used. Alternatively, imp-null can signify traffic engineering tunnels between the PE devices. • no adjacency—The adjacency for the next hop is missing. • no route—The label is not in the routing table. • not ready, Cisco Express Forwarding disabled—Cisco Express Forwarding is disabled. • not ready, LFIB disabled—The MPLS switching subsystem is disabled. • not ready, LFIB entry present—The tunnel label exists in the Label Forwarding Information Base (LFIB), but the VC is down. • not ready, no route—An IP route for the peer does not exist in the routing table. • not ready, not a host table—The route in the routing table for the remote peer device is not a host route. • unassigned—The label has not been assigned.
Create time	Time (in hours, minutes, and seconds) when the VC is provisioned.
last status change time	Last time (in hours, minutes, and seconds) when the VC state change occurred.
Signaling protocol	Type of protocol used to send the MPLS labels on dynamically configured connections. The output also shows the status of the peer device. For AToM statically configured pseudowires, the field indicates Manual because there is no exchange of labels using a directed control protocol, such as LDP.
MPLS VC labels	Local VC label is a disposition label, which identifies the egress interface of an arriving packet from the MPLS backbone. The remote VC label is a disposition VC label of the remote peer device.
Group ID	Local group ID used to group VCs locally. The remote group ID is used by the peer to group several VCs.
MTU	Maximum transmission unit (MTU) specified for local and remote interfaces.
Remote interface description	Interface on the remote device that is enabled to transmit and receive Layer 2 packets.
Sequencing	Indicates whether sequencing of out-of-order packets is enabled or disabled.
SSO Descriptor	Identifies the VC for which the information is checkpointed.

Field	Description
local label	Value of the local label that is checkpointed (that is, sent on the active RP and received on the standby RP).
SSM segment/switch IDs	IDs used for the control plane and data plane for this VC. This data is not for customer use but for Cisco personnel for troubleshooting purposes. When the Source Specific Multicast (SSM) IDs are followed by the word "used," the checkpointed data has been successfully sent.
PWID	Pseudowire ID used in the data plane to correlate the switching context for the segment associated with the MPLS switching context. This data is not for customer use but for Cisco personnel for troubleshooting purposes.
packet totals	Number of packets sent and received. Received packets are those AToM packets received from the MPLS core. Sent packets are those AToM packets sent to the MPLS core. This number excludes dropped packets. **Note** If the VC statistics fields include the word "transit," the output shows the number of packets and bytes being sent from the device.
byte totals	Number of bytes sent and received from the core-facing interface, including the payload, control word if present, and AToM VC label. **Note** If the VC statistics fields include the word "transit," the output shows the number of packets and bytes being sent from the device.
packet drops	Number of dropped packets. **Note** If the VC statistics fields include the word "transit," the output shows the number of packets and bytes being sent from the device.

The following is sample output from the **show l2vpn atom vc detail** command when the VPLS Autodiscovery feature has been configured on VPLS pseudowires.

```
Device# show l2vpn atom vc detail

Local interface: VFI my_test VFI up
  MPLS VC type is VFI, interworking type is Ethernet
  Destination address: 10.3.3.1, VC ID: 123456, VC status: up
    Next hop PE address: 10.55.55.2
    Output interface: Et3/0, imposed label stack {17 19}
    Preferred path: not configured
    Default path:
    Next hop: 10.1.0.2
  Create time: 2d05h, last status change time: 2d05h
Signaling protocol: LDP, peer 10.55.55.2:0 up
    MPLS VC labels: local 21, remote 19
    AGI: type 1, len 8,  0000 3333 4F4E 44C4
   Local AII:  type 1, len 4, 0909 0909 (10.9.9.9)
    Remote AII: type 1, len 4, 0303 0301 (10.3.3.3)
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
```

```
    packet totals: receive 22611, send 22611
    byte totals:   receive 2346570, send 2853581
    packet drops:  receive 0, send 0
```

The table below describes the fields shown in the display.

Table 96: show l2vpn atom vc detail Field Descriptions

Field	Description
Next hop PE address	IP address of the next hop device.
AGI	Attachment group identifier (AGI).
Local AII	Attachment individual identifier (AII)—the local IP address used for signaling.
Remote AII	Remote IP address used for signaling. This address is the provisioned IP address, which might be different from the LDP peer IP address.

The following is sample output from the **show l2vpn atom vc** command when the circuit emulation (CEM) interface is specified:

```
Device# show l2vpn atom vc interface CEM 3/1/1

Local intf  Local circuit  Dest address  VC ID  Status
----------  -------------  ------------  -----  ------
CE3/1/1     CESOPSN Basic 10.30.30.3    300    DOWN
```

The following sample output displays the number of MAC address withdrawal messages sent and received as part of the H-VPLS N-PE Redundancy for queue-in-queue (QinQ) and MPLS Access feature:

```
Device# show l2vpn atom vc detail

Local interface: VFI TEST VFI up
  MPLS VC type is VFI, interworking type is Ethernet
  Destination address: 10.1.1.1, VC ID: 1000, VC status: up
    Output interface: Se2/0, imposed label stack {17}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:04:34, last status change time: 00:04:15
  Signaling protocol: LDP, peer 10.1.1.1:0 up
    Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.1
    MPLS VC labels: local 16, remote 17
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
    MAC Withdraw: sent 5, received 3
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

The following sample output displays the status messages for the MPLS Pseudowire Status Signaling feature when it is enabled on both PE devices:

```
Device# show l2vpn atom vc detail
```

```
Local interface: Et1/0 up, line protocol up, Ethernet up
  Destination address: 10.1.1.1, VC ID: 456, VC status: up
    Output interface: Et2/0, imposed label stack {10005 10240}
    Preferred path: not configured
    Default path: active
    Next hop: 10.0.0.1
  Create time: 00:39:30, last status change time: 00:26:48
  Signaling protocol: LDP, peer 10.1.1.1:0 up
    Targeted Hello: 10.1.1.2(LDP Id) -> 10.1.1.1
  Status TLV support (local/remote)   : enabled/supported
    Label/status state machine        : established, LruRru
    Last local dataplane   status rcvd: no fault
    Last local SSS circuit status rcvd: no fault
    Last local SSS circuit status sent: no fault
    Last local  LDP TLV    status sent: no fault
    Last remote LDP TLV    status rcvd: PW DOWN(rx,tx faults)
  MPLS VC labels: local 2000, remote 10240
  Group ID: local 6, remote 0
  MTU: local 1500, remote 1500
  Remote interface description:
    Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 243651, send 243705
    byte totals:   receive 27768366, send 34109320
    packet drops:  receive 0, send 0
```

The table below describes the fields shown in the display.

Table 97: show l2vpn atom vc detail Field Descriptions

Field	Description
Status TLV support (local/remote)	For the local device, the output indicates whether the MPLS Pseudowire Signaling Status feature is enabled or disabled. For the remote device, the output indicates whether the MPLS Pseudowire Signaling Status feature is supported.
Label/status state machine	The first value in the output indicates whether label advertisement has been established or not. The second value (LruRru) indicates the status of the local and remote devices. The following list translates the status codes: • D—Dataplane • L—local device • r or n—ready (r) or not ready (n) • R—remote device • S—Local shutdown • u or d—up (u) or down (d) status
Last local dataplane status rcvd	Last status message received about the dataplane on the local device.
Last local SSS circuit status rcvd	Last status message received about the subscriber service switch (SSS) on the local device.

Field	Description
Last local SSS circuit status sent	Last status message sent about the subscriber service switch on the local device.
Last local LDP TLV status sent	Last status message sent about the type, length, values (TLV) on the local device.
Last remote LDP TLV status rcvd	Last status message received about the TLV on the local device.

The following sample output from the **show l2vpn atom vc detail** command displays the status of multisegment pseudowires:

```
Device# show l2vpn atom vc detail

Local interface: Se3/0 up, line protocol up, HDLC up
  Destination address: 10.12.1.1, VC ID: 100, VC status: down
    Output interface: Se2/0, imposed label stack {23}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:03:02, last status change time: 00:01:41
  Signaling protocol: LDP, peer 10.12.1.1:0 up
    Targeted Hello: 10.11.1.1(LDP Id) -> 10.12.1.1, LDP is UP
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRrd
      Last local dataplane   status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: DOWN(PW-tx-fault)
      Last local  LDP TLV    status sent: No fault
      Last remote LDP TLV    status rcvd: DOWN(PW-tx-fault)
       PW Switching Point:
       Fault type  Vcid   local IP addr   remote IP addr   Description
       PW-tx-fault  101        10.13.1.1         10.12.1.1   S-PE2
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 19, remote 23
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 16, send 27
    byte totals:   receive 2506, send 3098
    packet drops:  receive 0, seq error 0, send 0
```

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

Table 98: show l2vpn atom vc detail Field Descriptions

Field	Description
Fault type	Type of fault encountered on the switching point.
Vcid	ID of the VC on which the fault occurred.
local IP addr	Local IP address of the pseudowire.
remote IP addr	Remote IP address of the pseudowire.

Field	Description
Description	Descriptions assigned to the segment of the pseudowire.

The following sample output from the **show l2vpn atom vc detail** command displays the status of the control word when it is not configured (that is, it defaults to autosense):

```
Device# show l2vpn atom vc 123400 detail

Local interface: Et0/0 up, line protocol up, Ethernet up
  Destination address: 10.1.1.2, VC ID: 123400, VC status: down
    Output interface: if-?(0), imposed label stack {}
    Preferred path: not configured
    Default path: no route
    No adjacency
  Create time: 01:03:48, last status change time: 01:03:48
  Signaling protocol: LDP, peer 10.1.1.3:0 up
    Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.2
    Status TLV support (local/remote)   : enabled/unknown (no remote binding)
      Label/status state machine        : local ready, LruRnd
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: not sent
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: unknown (no remote binding)
    MPLS VC labels: local 1002, remote unassigned
    Group ID: local 0, remote unknown
    MTU: local 1500, remote unknown
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: on (configured: autosense)
```

If the control word is negotiated by the peer and is different from the configured value, the configured value is shown in parentheses.

- If the control word is configured to be disabled, the displayed value is as follows:

  ```
  Control Word: off (configured: disabled)
  ```

- If the control word is configured to be enabled but negotiated by the peer to be off, the displayed value is as follows:

  ```
  Control Word: off (configured: enabled)
  ```

- If the control word is not configured, the displayed value is as follows:

  ```
  Control Word: on (configured: autosense)
  ```

The following sample output from the **show l2vpn atom vc detail** command displays load balancing information and shows whether flow labels are added to the MPLS label as part of the L2VPN Advanced VPLS feature:

```
Device# show l2vpn atom vc detail

Local interface: VFI dci_vlan_100 VFI up
  MPLS VC type is VFI, interworking type is Ethernet
```

```
  Destination address: 10.2.2.2, VC ID: 100, VC status: up
    Output interface: Tu0, imposed label stack {16}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
    Load Balance: Flow
    Flow Label: enabled
```

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

Table 99: show l2vpn atom vc detail Field Descriptions

Field	Description
Load Balance	Displays the type of load-balancing configured. The load-balancing configuration can be either flow-based or port channel-based.
Flow Label	Indicates whether the imposition and disposition of flow labels for the pseudowire is enabled.

The following sample output from the **show l2vpn atom vc detail** command displays Bidirectional Forwarding Detection (BFD) information:

```
Device# show l2vpn atom vc detail

Local interface: AT1/1/0 up, line protocol up, ATM AAL5 10/101 up
 Destination address: 10.1.1.151, VC ID: 1234001, VC status: up
  Output interface: Gi1/0/0, imposed label stack {2000}
  Preferred path: not configured
  Default path: active
  Next hop: 10.151.152.1
 Create time: 6d03h, last status change time: 6d03h
 Signaling protocol: LDP, peer 10.1.1.151:0 up
  Targeted Hello: 10.1.1.152(LDP Id) -> 10.1.1.151, LDP is UP
  Status TLV support (local/remote)   : enabled/supported
   LDP route watch                    : enabled
   Label/status state machine         : established, LruRru
   Last local dataplane   status rcvd: No fault
   Last local SSS circuit status rcvd: No fault
   Last local SSS circuit status sent: No fault
   Last local  LDP TLV    status sent: No fault
   Last remote LDP TLV    status rcvd: No fault
   Last remote LDP ADJ    status rcvd: No fault
  MPLS VC labels: local 2000, remote 2000
  PWID: 20490
  Group ID: local 0, remote 0
  MTU: local 4470, remote 4470
  Remote interface description:
 Sequencing: receive disabled, send disabled
 Control Word: On (configured: autosense)
 VCCV BFD protection active
  BFD Template - sampleBFDTemplate
  CC Type -  1
  CV Type - fault detection only with IP/UDP headers
 VC statistics:
  transit packet totals: receive 0, send 0
  transit byte totals:   receive 0, send 0
  transit packet drops:  receive 0, seq error 0, send 0
```

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

Table 100: show l2vpn atom vc detail Field Descriptions for the BFD CC over VCCV—Support for ATM Pseudowire Feature

Field	Description
VCCV BFD protection active	Displays the virtual circuit connectivity verification (VCCV) BFD protection status.
BFD Template	Displays the BFD template name.
CC Type	Displays the continuity check (CC) type. • Type 1: control word. • Type 2: MPLS device alert label. • Type 3: MPLS pseudowire label with time to live (TTL).
CV Type	Displays the Control Verification type.

The following is sample output from the **show l2vpn atom vc** command when the L2VPN VPLS Inter-AS Option B feature has been configured. The fields in the display are self-explanatory or described in other tables in this document:

```
Device# show l2vpn atom vc

Load for five secs: 4%/1%; one minute: 4%; five minutes: 2%
Time source is hardware calendar, *17:26:56.066 GMT Mon Oct 18 2010
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
VFI auto       VFI                        10.1.1.1        100         UP
```

The following is sample output from the **show l2vpn atom vc detail** command when the L2VPN VPLS Inter-AS Option B feature has been configured:

```
Device# show l2vpn atom vc detail

Load for five secs: 4%/1%; one minute: 4%; five minutes: 2%
Time source is hardware calendar, *17:27:28.076 GMT Mon Oct 18 2010
Local interface: VFI auto VFI up
  Interworking type is Ethernet
  Destination address: 192.0.2.1, VC ID: 100, VC status: up
  Next hop PE address: 198.51.100.1
    Output interface: Et1/0, imposed label stack {2012}
    Preferred path: not configured
    Default path: active
    Next hop: 10.0.0.3
  Create time: 00:00:48, last status change time: 00:00:48
  Signaling protocol: LDP, peer 192.0.2.3:0 up
    Targeted Hello: 192.0.2.6(from BGP) -> 192.0.2.8, LDP is UP
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: No fault
      Last local  LDP TLV    status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 1011, remote 2012
```

```
    PWID: 4096
    AGI: type 1, len 8, 000A 0001 0000 0001
    Local AII: type 1, len 4, 0101 0001 (203.0.113.1)
    Remote AII: type 1, len 4, 0201 0101 (203.0.113.5)
    VPLS-ID: 1:1
    Group ID: local n/a, remote n/a
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  SSO Descriptor: 203.0.113.5/100, local label: 1011
    SSM segment/switch IDs: 16387/8193 (used), PWID: 4096
  VC statistics:
    transit packet totals: receive 0, send 0
    transit byte totals:   receive 0, send 0
    transit packet drops:  receive 0, seq error 0, send 0
```

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

Table 101: show l2vpn atom vc detail Field Descriptions for the L2VPN VPLS Inter-AS Option B

Field	Description
PWID	Pseudowire identifier.
VPLS-ID	The VPLS identifier associated with the pseudowire.

The following is sample output from the **show l2vpn atom vc detail** command when there is a remote AC failure and when VCCV BFD status signaling is enabled, that is, **vccv bfd status signaling** is configured:

```
Device# show l2vpn atom vc detail

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *03:31:33.136 PST Thu Mar 24 2011
Local interface: Et1/0.1 up, line protocol up, Eth VLAN 1001 up
Destination address: 192.0.2.1, VC ID: 1234000, VC status: down
    Output interface: Et0/0, imposed label stack {150}
    Preferred path: not configured
    Default path: active
    Next hop: 198.58.100.2
  Create time: 00:03:45, last status change time: 00:00:02
  Signaling protocol: Manual
    Status TLV support (local/remote)   : enabled/N/A
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRrd
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: DOWN AC(rx/tx faults)
      Last local  LDP TLV    status sent: None
      Last remote LDP TLV    status rcvd: DOWN AC(rx/tx faults), (UP)
      Last remote LDP ADJ    status rcvd: No fault
 MPLS VC labels: local 100, remote 150
    PWID: 4096
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  VCCV BFD protection active
     BFD Template - t1
```

```
    CC Type -  1
    CV Type - fault detection and status signaling without IP/UDP headers
VC statistics:
  transit packet totals: receive 0, send 5
  transit byte totals:   receive 0, send 580
  transit packet drops:  receive 0, seq error 0, send 0
```

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

Table 102: show l2vpn atom detail Field Descriptions for Remote AC Failure

Field	Description
Last BFD dataplane status rcvd	Last status message received about the BFD dataplane on the local device.
Last local dataplane status rcvd	Last status message received about the dataplane on the local device.
Last local SSS circuit status rcvd	Last status message received about the subscriber service switch (SSS) on the local device.
Last local SSS circuit status sent	Last status message sent about the subscriber service switch on the local device.
Last remote LDP ADJ	Last status message received about the ADJ on the local device.
VCCV BFD protection active	Displays the VCCV BFD protection status.
BFD Template	Displays the BFD template name.
CC Type	Displays the CC type. • Type 1: control word. • Type 2: MPLS device alert label. • Type 3: MPLS pseudowire label with TTL.
CV Type	Displays the Control Verification (CV) type.

Related Commands

Command	Description
show l2vpn atom summary	Displays summary information about VCs that have been enabled to route AToM Layer 2 packets on a device.
show l2vpn atom vc	Displays information about AToM VCs and static pseudowires.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.
show mpls forwarding-table	Displays the contents of the MPLS LFIB.

show l2vpn pwmib

To display information about the Layer 2 VPN (L2VPN) pseudowire MIB, use the **show l2vpn pwmib** command in privileged EXEC mode.

show l2vpn pwmib [{**peer** *ip-address* *vcid-value*}]

Syntax Description

peer	(Optional) Displays information about L2VPN cross connect attachment circuits and pseudowires associated with the specified peer.
ip-address	(Optional) IP address of the peer.
vcid-value	(Optional) Virtual circuit (VC) ID value.

Command Default

Information about the L2VPN pseudowire MIB for all peers is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **pwmib** keyword in the **show xconnect** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the **show l2vpn pwmib** command to display information about the L2VPN pseudowire MIB. You can specify the peer IP address and the virtual circuit (VC) ID value to display information associated with the specified peer IP address and the specified VC ID.

Examples

The following is sample output from the **show l2vpn pwmib** command for a peer with IP address is 10.3.2.1 and a VC ID value of 4000:

```
Device# show l2vpn pwmib peer 10.3.2.1 4000
VCINDEX     VC ID       Peer Address     Encap    Status  Interface
1           4           10.10.10.10      MPLS     up      Et1/0
2           5           11.11.11.11      MPLS     down    Et1/0
```

Related Commands

Command	Description
show l2vpn rib	Displays information about the L2VPN cross connect RIB.
show l2vpn vfi	Displays L2VPN VFI information.
show l2vpn service	Displays L2VPN service information.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

show l2vpn rib

To display information about the Layer 2 VPN (L2VPN) pseudowire Routing Information Base (RIB), use the **show l2vpn rib** command in privileged EXEC mode.

show l2vpn rib [{[[{**next-hop** | **target-id**}] *ip-address*] [{**detail**}] | **vpls-id** {*asn*:*nn* | *ip-address*:*nn*}}]

Syntax Description

next-hop	(Optional) Displays the L2VPN RIB information for the specified next hop.
target-id	(Optional) Displays the L2VPN RIB information for the specified target.
ip-address	IP address of the next-hop or target address.
detail	(Optional) Displays detailed information about the L2VPN RIB.
vpls-id	(Optional) Displays the L2VPN RIB information about the specified Virtual Private LAN Service (VPLS) extended community.
asn:*nn* *ip-address*:*nn*	(Optional) IP address and network number or autonomous system number (ASN) and network number of the VPLS.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **rib** keyword in the **show xconnect** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Examples

The following is sample output from the **show l2vpn rib** command:

```
Device# show l2vpn 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 fields shown in the command display.

Table 103: show l2vpn 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	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 device.
next-hop	IP address of the next-hop device.
Route-Target	Route target (RT). VPLS autodiscovery generates a route target using the lower 6 bytes of the route distinguisher (RD) and VPN ID.

The following is sample output for the **show l2vpn rib detail** command.

```
Device#  show l2vpn 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 fields shown in the command display.

Table 104: show l2vpn rib 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.

The following is sample output from the **show l2vpn rib** command when used in a L2VPN VPLS Inter-AS Option B configuration:

```
Device# show l2vpn 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
```

Related Commands

Command	Description
show l2vpn vfi	Displays L2VPN VFI information.
show l2vpn service	Displays L2VPN service information.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

show l2vpn service

To display Layer 2 VPN (L2VPN) service information, use the **show l2vpn service** command in privileged EXEC mode.

show l2vpn service[{**vfi** | **xconnect**}] {**all** [{**detail**}] | **interface** *int-type number* | **name** *service-name* | **peer** *peer-address* {**all** | **vcid** *vcid-value* [{**detail**}]}}

Syntax Description

vfi	(Optional) Displays all Virtual Private LAN Services (VPLS).
xconnect	(Optional) Displays all Virtual Private Wire Services (VPWS).
all	Displays all service entries.
detail	(Optional) Displays detailed service information.
interface *int-type number*	Displays information about all services by the specified interface type and number.
name *service-name*	Displays information for the specified service.
peer *peer-address*	Displays all services by the IP address of the remote peer.
vcid *vcid-value*	Displays all services by the virtual circuit (VC) ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support.
15.3(1)S	This command was integrated 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 is sample output from **show l2vpn service all** command when Label Distribution Protocol (LDP) signaling is used:

```
Device# show l2vpn service all

Legend: St=State    Prio=Priority
        UP=Up       DN=Down            AD=Admin Down      IA=Inactive
        SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

  Interface          Group       Encapsulation           Prio  St  XC St
  ---------          -----       -------------           ----  --  -----
XC name: serviceWire1, State: UP
```

```
  Eth1/1:10          access      EVC 45                0     UP  UP
  Pw1                core        MPLS 5.5.5.5:100      0     UP  UP

  Pw2                core        MPLS 6.6.6.6:200      1     SB  IA
XC name: serviceConn2, State:UP
  Eth2/1:20          access_conn EVC 55                0     UP  UP
  Eth3/1:20          core_conn   EVC 55                0     DN  IA

  Eth4/1:20          core_conn   EVC 55                1     UP  UP

XC name: serviceStit3, State: UP
  Pw3                left        MPLS 7.7.7.7:300      0     UP  UP

  Pw4                right       MPLS 8.8.8.8:300      0     UP  UP
```

The following is sample output from **show l2vpn service all detail** command when LDP signaling is used:

```
Device# show l2vpn service all detail

Legend: St=State    Prio=Priority
        UP=Up       DN=Down            AD=Admin Down      IA=Inactive
        SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

XC name: serviceWire1, State: UP, Signaling Protocol: LDP
  Group: access
    Interface              Encapsulation                Prio  St  XC St
    ---------              -------------                ----  --  -----
    Ethernet1/1            EVC 45, dot1q 10             0     UP  UP
  Group: core
    Interface              Encapsulation                Prio  St  XC St
    ---------              -------------                ----  --  -----
    Pseudowire1            MPLS 5.5.5.5:100             0     UP  UP
                           Local VC label 2004
                           Remote VC label 3004

                           Interworking: none, VC type: 4
                           template: mpls_1
    Pseudowire2            MPLS 6.6.6.6:200             1     SB  IA
                           Local VC label 2008
                           Remote VC label 4008

                           Interworking: none, VC type: 4
                           template: mpls_1
```

show l2vpn signaling rib

To display information about the Layer 2 VPN (L2VPN) signaling pseudowire Routing Information Base (RIB), use the **show l2vpn signaling rib** command in privileged EXEC mode.

show l2vpn signaling rib [{**next-hop** *ip-address* | **detail** | **rd** {*ASN*:*nn* | *ip-address*:*nn* [{**detail**}]}}]

Syntax Description

next-hop	(Optional) Displays the L2VPN RIB information for the specified next hop.
ip-address	(Optional) IP address of the next hop or target address.
detail	(Optional) Displays detailed information about the L2VPN RIB.
rd	(Optional) Displays the route distinguisher.
asn:*nn*	(Optional) IP address and network number.
ip-address:*nn*	(Optional) Autonomous system number (ASN) and network number of the Virtual Private LAN Services (VPLS).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Example

The following is sample output from the **show l2vpn signaling rib** command:

```
Device# show l2vpn signaling rib
0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *20:55:09.776 GMT Wed Aug 29 2012
+- Origin of entry (i=iBGP/e=eBGP)
| +- Provisioned (Yes/No)?
| | +- Stale entry (Yes/No)?
| | |
v v v
O P S RD VE-ID VBO VBS LB Next-Hop
-+-+-+----------------+-------+-------+-------+---------+-----------------+
i Y N 1:1 11 10 10 2002 1.1.1.2
i Y N 1:1 12 10 10 2002 1.1.1.3
i Y N 1:2 21 12 12 2012 1.1.1.2
i Y N 1:2 22 12 12 2012 1.1.1.3
PE1-standby#show l2vpn signaling rib
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *20:56:11.985 GMT Wed Aug 29 2012
+- Origin of entry (i=iBGP/e=eBGP)
| +- Provisioned (Yes/No)?
| | +- Stale entry (Yes/No)?
| | |
v v v
O P S RD VE-ID VBO VBS LB Next-Hop
-+-+-+----------------+-------+-------+-------+---------+-----------------+
```

```
i Y N 1:1 11 10 10 2002 1.1.1.2
i Y N 1:1 12 10 10 2002 1.1.1.3
i Y N 1:2 21 12 12 2012 1.1.1.2
i Y N 1:2 22 12 12 2012 1.1.1.3
```

Table 105: show l2vpn signaling rib Field Descriptions

Field	Description
Origin of entry	Origin of the entry. The origin can be “i” for internal Border Gateway Protocol (BGP) or “e” for external BGP.
Provisioned	Specifies whether the pseudowire has been provisioned using a learned route.
Next-Hop	IP address of the next-hop device.

The following is sample output from the **show l2vpn signaling rib detail** command:

```
Device# show l2vpn signaling rib rd 1:1 detail
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *20:57:12.265 GMT Wed Aug 29 2012
Route 1:1:11 (epoch:1) from iBGP peer 1.1.1.2
Provisioned (Y) Stale (N)
Route-Target: 1:1
NLRI [6E000001]
VE-ID:11 VBO:10 VBS:10 LB:2002
MTU: 1500 Control Word: off
RIB Filter [44000001]
RD: 1:1
VE-ID: 10, VBO: 10, VBS: 10 LB: 1002
Forwarder [F0000001] VFI VFI1
Route 1:1:12 (epoch:1) from iBGP peer 1.1.1.3
Provisioned (Y) Stale (N)
Route-Target: 1:1
NLRI [35000003]
VE-ID:12 VBO:10 VBS:10 LB:2002
MTU: 1500 Control Word: off
RIB Filter [44000001]
RD: 1:1
VE-ID: 10, VBO: 10, VBS: 10 LB: 1002
Forwarder [F0000001] VFI VFI1
```

Related Commands

Command	Description
show l2vpn rib	Displays information about the L2VPN cross-connect RIB.
show l2vpn rib vfi	Displays L2VPN VFI information.
show l2vpn service	Displays L2VPN service information.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

show l2vpn vfi

To display Layer 2 VPN (L2VPN) virtual forwarding instance (VFI) information use the **show l2vpn vfi** command in privileged EXEC mode.

show l2vpn vfi [{**name** *vfi-name* | **neighbor** *peer-address* **vcid** *vcid-value*}] [{**mac static address**}]

Syntax Description

name *vfi-name*	(Optional) Displays L2VPN VFI information for a specific VFI.
neighbor	(Optional) Displays VFI per neighbor information.
peer-address	(Optional) IP address of the remote peer.
mac static address	(Optional) Displays static MAC information.
vcid *vcid-value*	(Optional) Displays VFI information for the specific virtual circuit (VC) ID value of a remote peer.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **show vfi** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Examples

The following is sample output from the **show l2vpn vfi** command when Label Distribution Protocol (LDP) signaling is used. The output fields are self-explanatory.

```
Device# show l2vpn vfi

Legend: RT= Route-target

VFI name: serviceCore1, State: UP, Signaling Protocol: LDP
  VPN ID: 100, VPLS-ID: 9:10, Bridge-domain vlan: 100
  RD: 9:10, RT: 10.10.10.10:150
  Pseudo-port Interface: Virtual-Ethernet1000

  Neighbors connected via pseudowires:
  Interface    Peer Address    VC ID      Discovered Router ID   Next Hop
  Pw2000       10.0.0.1        10         10.0.0.1               10.0.0.1
  Pw2001       10.0.0.2        10         10.1.1.2               10.0.0.2
  Pw2002       10.0.0.3        10         10.1.1.3               10.0.0.3
  Pw5          10.0.0.4        10         -                      10.0.0.4
```

The following is sample output from the **show l2vpn vfi** command when Border Gateway Protocol (BGP) signaling is used. The output fields are self-explanatory.

```
Device# show l2vpn vfi
```

```
VFI name: serviceCore1, State: UP, Signaling Protocol: BGP
  Bridge Domain: <bd>
  VPN ID: <vpn>
  RD: <rd>, RT: <rt>
  Pseudo-port Interface: Virtual-Ethernet1000

  Local Edge ID: <ve_id>, Label Blocks (<num> Blocks)
  Label Base Offset      Size     Timestamp  St
  ---------- ------      ----     ---------  --
  5000       1           100      <time>     UP

  List of discovered peers (<num>):
    Remote Edge Device 1:
      Remote Edge ID: <remote_ve_id>, NLRIs (<num> NLRIs)
      Interface  Label Base  Offset     Size     Peer ID     Timestamp   St
      ---------  ----------- ------     ----     -------     ---------   --
      Pw1        6000        1          10       10.1.1.1    <time>      UP

    Remote Edge Device 2:
      Remote Edge ID: <remote_ve_id>, NLRIs (<num> NLRIs)
      Interface  Label Base  Offset     Size       Peer ID     Timestamp   St
      ---------  ----------- ------     ----       -------     ---------   --
      Pw2        7000        100        10         20.1.1.1    <time>      UP
```

Related Commands

Command	Description
show l2vpn atom binding	Displays VC label binding information.
show l2vpn atom checkpoint	Displays the checkpoint information about AToM VCs.
show l2vpn atom hw-capability	Displays the transport types and their supported capabilities.
show l2vpn atom vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a device.
show l2vpn rib	Displays information about the L2VPN crossconnect RIB.
show l2vpn service	Displays L2VPN service information.
show xconnect vfi	Displays xconnect VFI information.

show mpls atm-ldp bindings

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

To display specified entries from the ATM label binding database, use the **show mpls atm-ldp bindings** command in privileged EXEC mode.

show mpls atm-ldp bindings [*network* {*masklength*}] [**local-label** *vpi vci*] [**remote-label** *vpi vci*] [**neighbor** *interface*]

Syntax Description

network	(Optional) Defines the destination network number.
mask	(Optional) Defines the network mask in the form A.B.C.D (destination prefix).
length	(Optional) Defines the mask length (1 to 32).
local-label *vpi vci*	(Optional) Selects the label values assigned by this router. The virtual path identifier (VPI) range is 0 to 4095. The virtual channel identifier (VCI) range is 0 to 65535.
remote-label *vpi vci*	(Optional) Selects the label values assigned by the other router. VPI range is 0 to 4095. VCI range is 0 to 65535.
neighbor *interface*	(Optional) Selects the label values assigned by the neighbor on a specified interface.

Command Default

The entire ATM label binding database is displayed if no optional arguments or keywords are specified.

Note To display information about entries in the label binding database for interfaces other than ATM interfaces, use the **show mpls ip binding** command.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to use Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.

Release	Modification
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	The VPI range of values for this command was extended to 4095.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.4(20)T	This command was removed.

Usage Guidelines

The ATM label binding database contains entries for label virtual circuits (VCs) on label-controlled (LC)-ATM interfaces. Command output can show a summary of entries from the entire database, or the output can be limited to a subset of entries based on the following:

- Specific prefix
- Specific VC label value
- Specific assigning interface

Note This command displays ATM label bindings learned by the Label Distribution Protocol (LDP) or Tag Distribution Protocol (TDP). TDP is not supported for LDP features in Cisco IOS 12.0(30)S and later releases, 12.2(27)SBC and later 12.2S releases, and 12.3(14)T and later releases.

Note The show mpls ip binding command includes the output generated by the show mpls atm-ldp bindings command and information about label bindings for packet interfaces.

Examples

The following is sample output from the **show mpls atm-ldp bindings** command:

```
Router# show mpls atm-ldp bindings
 Destination: 10.24.0.0/24
    Tailend Router ATM1/0.1 1/39 Active, VCD=3
 Destination: 10.15.0.15/32
    Tailend Router ATM1/0.1 1/33 Active, VCD=4
 Destination: 10.0.7.7/32
    Headend Router ATM1/0.1 (2 hops) 1/34  Active, VCD=810
```

The following is sample output from the **show mpls atm-ldp bindings** command on an ATM switch:

```
Router# show mpls atm-ldp bindings
Destination: 172.16.0.0/16
    Tailend Switch ATM0/0/3 1/35 Active -> Terminating Active
Destination: 10.4.4.4/32
    Transit ATM0/0/3 1/33 Active -> ATM0/1/1 1/33 Active
```

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

Table 106: show mpls atm-ldp bindings Field Descriptions

Field	Description
Destination	Destination (network/mask).
Headend Router Tailend Router Tailend Switch Transit	Indicates types of VCs. Options are the following: • Tailend--VC that terminates at this platform • Headend--VC that originates at this router • Transit--VC that passes through a switch
ATM1/0.1	ATM interface.
1/35	VPI/VCI.
Active	Indicates VC state. Options include the following: • Active--Set up and working • Bindwait--Waiting for a response • Remote Resource Wait--Waiting for resources (VPI/VCI space) to be available on the downstream device • Parent Wait--Transit VC input side waiting for output side to become active
VCD=3	Virtual circuit descriptor number.

Related Commands

Command	Description
show mpls ip binding	Displays specified information about label bindings learned by the MPLS LDP.

show mpls atm-ldp bindwait

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

To display the number of bindings waiting for label assignments from a remote Multiprotocol Label Switching (MPLS) ATM switch, use the **show mpls atm-ldp bindwait** command in privileged EXEC mode.

show mpls atm-ldp bindwait

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was modified to use MPLS Internet Engineering Task Force (IETF) command syntax and terminology.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(20)T	This command was removed.

Usage Guidelines

Use this command to display information about virtual circuits (VCs) in the bindwait state.

Examples

The following is sample output from the **show mpls atm-ldp bindwait** command:

```
Router# show mpls atm-ldp bindwait
Waiting for bind on ATM1/0.2
  10.3.3.1/32          10.3.3.1/32          10.3.3.2/32
  10.3.3.2/32          10.3.3.3/32          10.3.3.3/32
  10.3.3.4/32          10.3.3.4/32          10.3.3.5/32
  10.3.3.5/32          10.3.3.6/32          10.3.3.6/32
  10.3.3.7/32          10.3.3.7/32          10.3.3.8/32
  10.3.3.8/32          10.3.3.9/32          10.3.3.9/32
.
```

```
.
.
end
```

If there are no bindings waiting for label assignments from the remote MPLS ATM switch, this command does not display any output.

Related Commands

Command	Description
show mpls atm-ldp bindings	Displays specified entries from the ATM label binding database.

show mpls atm-ldp capability

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

To display the Multiprotocol Label Switching (MPLS) ATM capabilities negotiated with Label Distribution Protocol (LDP) neighbors for label-controlled (LC)-ATM interfaces, use the **show mpls atm-ldp capability** command in privileged EXEC mode.

show mpls atm-ldp capability

Syntax Description

This command has no arguments or keywords.

Command Default

This command always displays all the MPLS ATM capabilities negotiated with all the LDP neighbors.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to use MPLS Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.

Release	Modification
12.4(20)T	This command was removed.

Usage Guidelines

When two label switch routers (LSRs) establish an LDP session, they negotiate parameters for the session, such as the range of virtual path identifiers (VPIs) and virtual channel identifiers (VCIs) that will be used as labels.

This command displays the MPLS ATM capabilities negotiated by LDP or the Tag Distribution Protocol (TDP).

Note TDP is not supported for LDP features in Cisco IOS 12.0(30)S and later releases, 12.2(27)SBC and later 12.2S releases, and 12.3(14)T and later releases.

Examples

The following is sample output from the **show mpls atm-ldp capability** command:

```
Router# show mpls atm-ldp capability
                VPI           VCI           Alloc   Odd/Even  VC Merge
ATM0/1/0        Range         Range         Scheme  Scheme    IN   OUT
  Negotiated    [100 - 101]   [33 - 1023]   UNIDIR            -    -
  Local         [100 - 101]   [33 - 16383]  UNIDIR            EN   EN
  Peer          [100 - 101]   [33 - 1023]   UNIDIR            -    -

                VPI           VCI           Alloc   Odd/Even  VC Merge
ATM0/1/1        Range         Range         Scheme  Scheme    IN   OUT
  Negotiated    [201 - 202]   [33 - 1023]   BIDIR             -    -
  Local         [201 - 202]   [33 - 16383]  UNIDIR  ODD       NO   NO
  Peer          [201 - 202]   [33 - 1023]   BIDIR   EVEN      -    -
```

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

Table 107: show mpls atm-ldp capability Field Descriptions

Field	Description
VPI Range	Minimum and maximum numbers of VPIs supported on this interface.
VCI Range	Minimum and maximum numbers of VCIs supported on this interface.

Field	Description
Alloc Scheme	Indicates the applicable allocation scheme, as follows: • UNIDIR--Unidirectional capability indicates that the peer can, within a single VPI, support binding of the same VCI to different prefixes on different directions of the link. • BIDIR--Bidirectional capability indicates that within a single VPI, a single VCI can appear in one binding only. In this case, one peer allocates bindings in the even VCI space, and the other in the odd VCI space. The system with the lower LDP identifier assigns even-numbered VCIs. The negotiated allocation scheme is UNIDIR, only if both peers have UNIDIR capability. Otherwise, the allocation scheme is BIDIR. **Note** These definitions for unidirectional and bidirectional are consistent with normal ATM usage of the terms; however, they are exactly opposite from the definitions for them in the IETF LDP specification.
Odd/Even Scheme	Indicates whether the local device or the peer is assigning an odd- or even-numbered VCI when the negotiated scheme is BIDIR. It does not display any information when the negotiated scheme is UNIDIR.

VC Merge	Indicates the type of virtual circuit (VC) merge support available on this interface. There are two possibilities, as follows:
	• IN--Indicates the input interface merge capability. IN accepts the following values:
	  • EN--The hardware interface supports VC merge, and VC merge is enabled on the device.
	  • DIS--The hardware interface supports VC merge and VC merge is disabled on the device.
	  • NO--The hardware interface does not support VC merge.
	• OUT--Indicates the output interface merge capability. OUT accepts the same values as the input merge side.
	The VC merge capability is meaningful only on ATM switches. This capability is not negotiated.

Negotiated	Indicates the set of options that both LDP peers have agreed to share on this interface. For example, the VPI or VCI allocation on either peer remains within the negotiated range.
Local	Indicates the options supported locally on this interface.
Peer	Indicates the options supported by the remote LDP peer on this interface.

Related Commands

Command	Description
mpls ldp atm vc-merge	Controls whether the vc-merge (multipoint-to-point) is supported for unicast label VCs.

show mpls atm-ldp summary

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

To display summary information about all the entries in the ATM label binding database, use the **show mpls atm-ldp summary** command in privileged EXEC mode.

show mpls atm-ldp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to use Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(20)T	This command was removed.

Usage Guidelines

Use this command to display dynamic ATM accounting information.

Examples

The following is sample output from the **show mpls atm-ldp summary** command:

```
Router# show mpls atm-ldp summary
Total number of destinations: 406

ATM label bindings summary
interface      total   active  local   remote  Bwait   Rwait   IFwait
ATM0/0/0       406     406     404     2       0       0       0
ATM0/0/1       406     406     3       403     0       0       0
```

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

Table 108: show mpls atm-ldp summary Field Descriptions

Field	Description
Total number of destinations:	Number of known destination address prefixes.
interface	Name of an interface with associated ATM label bindings.
total	Total number of ATM labels on this interface.
active	Number of ATM labels in an “active” state that are ready to use for data transfer.
local	Number of ATM labels assigned by this label switch router (LSR) on this interface.
remote	Number of ATM labels assigned by the neighbor LSR on this interface.
Bwait	Number of bindings that are waiting for a label assignment from the neighbor LSR.
Rwait	Number of bindings that are waiting for resources (virtual path identifier [VPI] /virtual channel identifier [VCI] space) to be available on the downstream device.
IFwait	Number of bindings that are waiting for learned labels to be installed for switching use.

Related Commands

Command	Description
show isis database verbose	Displays the requested entries from the ATM LDP label binding database.

show mls cef mpls exact-route

To display the Multiprotocol Label Switching (MPLS) hardware load-sharing results from the Multilayer Switching (MLS) hardware Layer 3 switching table, use the **show mls cef mpls exact-route** command in user EXEC or privileged EXEC mode.

show mls cef mpls exact-route {*dst-address src-address* **label-stack-depth** *value* **label** *outer-most-value* | **label** *outer-most-value*} [**label** *inner-most-value*]

Syntax Description

dst-address	Destination IP address.
src-address	Source IP address.
label-stack-depth *value*	Specifies the depth of the label stack. The range is from 1 to 1048575. The default value is zero.
label *outer-most-value*	Specifies the top-most label in the incoming packet. The range is from 16 to 1048575. The default value is zero.
label *inner-most-value*	(Optional) Specifies the bottom-most label in the incoming packet. The range is from 16 to 1048575. The default value is zero.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced on Cisco 7600 series routers.

Usage Guidelines

You can use the **show mls cef mpls exact-route** command to find the actual path used by the label traffic in an Equal Cost Multipath (ECMP). This command helps in debugging Layer 2 VPN (L2VPN)) and Layer 3 VPN (L3VPN) load balancing.

Note The **show mls cef mpls exact-route** command is supported only for L2VPN and L3VPN.

You must configure the appropriate parameters based on the control word in the incoming packets as follows:

- If the incoming packet contains the control word, you need not provide the source and destination address along with the label stack depth value.

Note You must configure the inner label value if you do not specify the source and destination IP address.

- If the incoming packet does not have the control word, you must provide all the attributes applicable for the packet; that is, source address, destination address, and label stack depth value.

Note The **show mls cef mpls exact-route** command may not display valid results when you use the command on provider edge (PE) routers for L2 and L3 VPNs. Hence, Cisco does not recommend using the command on PE routers for L2 and L3 VPNs.

Examples

The following is sample output from the **show mls cef mpls exact-route** command. Fields in the display are self-explanatory.

```
Router# show mls cef mpls exact-route 192.0.2.1 192.0.2.2 label-stack-depth 2 label 19
For EOS [0] choice Adjacency details are:
       Interface: Gi3/3/0, Next Hop: 192.168.3.1, Vlan: 1019, DestinationMac: 0006.5248.a400

 For EOS [1] choice Adjacency details are:
       Interface: Gi3/3/0, Next Hop: 192.168.3.1, Vlan: 1019, DestinationMac: 0006.5248.a400
```

The following is sample output from the **show mls cef mpls exact-route** command when the source and destination IP address are not specified. Fields in the display are self-explanatory.

```
Router# show mls cef mpls exact-route label 18 label 20
 For EOS [0] choice Adjacency details are:
        Interface: Te1/0/0, Next Hop: 10.0.0.1, Vlan: 1023, DestinationMac: 000b.fc1c.ee40
 For EOS [1] choice Adjacency details are:
        Interface: Te1/0/0, Next Hop: 10.0.0.1, Vlan: 1023, DestinationMac: 000b.fc1c.ee40
```

Related Commands

Command	Description
show mpls forwarding-table	Displays the contents of the MPLS LIB.

show mpls cos-map

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

To display the quality of service (QoS) map used to assign a quantity of label virtual circuits and the associated class of service (CoS) for those virtual circuits, use the **show mpls cos-map** in privileged EXEC mode.

show mpls cos-map [*cos-map*]

Syntax Description

cos-map	(Optional) Number specifying the QoS 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 match Multiprotocol Label Switching (MPLS) syntax and terminology.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(25)S	The heading in the output was changed from tag-vc to label-vc.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(20)T	This command was removed.

Usage Guidelines

Not entering a specific QoS number causes all QoS maps to be displayed.

Note Cisco 10000 series routers do not use the **show mpls cos-map** command.

Examples

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

```
Router# show mpls cos-map 2
cos-map 2    class  Label-VC
             3      control
             2      control
             1      available
             0      available
```

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

Table 109: show mpls cos-map Field Descriptions

Field	Description
cos-map	Configures a class map, which specifies how classes map to MPLS virtual circuits when they are combined with a prefix map.
class	The IP precedence.
Label-VC	An ATM virtual circuit that is set up through ATM label switch router (LSR) label distribution procedures.

Related Commands

Command	Description
mpls cos-map	Creates a class map specifying how classes map to label virtual circuits when they are combined with a prefix map.

show mpls flow mappings

To display all entries in the Multiprotocol Label Switching (MPLS) Prefix/Application/Label (PAL) table, use the **show mpls flow mappings** command in user EXEC mode or privileged EXEC mode.

show mpls flow mappings

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you are interested in only a certain type of MPLS label and do not want to display the entire MPLS PAL table, you can use the **show mpls flow mappings** | **include** *label-type* command.

Examples

The following sample output from the **show mpls flow mappings** command displays all entries in the MPLS PAL table:

```
Router# show mpls flow mappings
Label    Owner    Route-Distinguisher Prefix          Allocated
18       LDP                          10.0.0.5        00:52:10
21       BGP                          0.0.0.0         00:52:18
22       BGP                          0.0.0.0         00:52:18
25       BGP                          0.0.0.0         00:51:44
26       LDP                          10.32.0.0       00:52:10
27       TE-MIDPT                     10.30.0.2       00:52:06
28       LDP                          10.33.0.0       00:52:10
29       LDP                          10.0.0.1        00:52:10
30       LDP                          10.0.0.3        00:52:10
```

In this example, the **mpls export vpnv4 prefixes** command was not configured. Therefore, the MPLS PAL table did not export a route distinguisher for the Border Gateway Protocol (BGP) application, and the associated prefix is exported as 0.0.0.0.

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

Table 110: show mpls flow mappings Field Descriptions

Field	Description
Label	Value given to the MPLS label by the router.

Field	Description
Owner	MPLS application that allocated the label. • LDP = Label Distribution Protocol • BGP = Border Gateway Protocol • TE-MIDT = Traffic engineering tunnel midpoint
Route-Distinguisher	Value (8-byte) that is concatenated with an IPv4 prefix to create a unique VPN IPv4 prefix.
Prefix	Prefix used by the router to route data to the destination address.
Allocated	System uptime at which the MPLS PAL mapping record was created.

The following is sample output from the **show mpls flow mappings** command if you previously entered the **mpls export vpnv4 prefixes** command:

```
Router# show mpls flow mappings
Label    Owner    Route-Distinguisher Prefix           Allocated
16       LDP                          10.0.0.3        00:58:03
17       LDP                          10.33.0.0       00:58:03
19       TE-MIDPT                     10.30.0.2       00:58:06
20       LDP                          10.0.0.5        00:58:03
23       LDP                          10.0.0.1        00:58:03
24       LDP                          10.32.0.0       00:58:03
27       BGP      100:1               10.34.0.0       00:57:48
31       BGP      100:1               10.0.0.9        00:58:21
32       BGP      100:1               10.3.3.0        00:58:21
```

The following sample output from the **show mpls flow mappings** | **include LDP** command displays only MPLS PAL entries that were allocated by LDP:

```
Router# show mpls flow mappings | include LDP
Label    Owner    Route-Distinguisher Prefix           Allocated
16       LDP                          10.0.0.3        00:58:03
17       LDP                          10.33.0.0       00:58:03
20       LDP                          10.0.0.5        00:58:03
23       LDP                          10.0.0.1        00:58:03
24       LDP                          10.32.0.0       00:58:03
```

Related Commands

Command	Description
show ip cache verbose flow	Displays a detailed summary of NetFlow statistics.
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

show mpls forwarding vrf

To display label forwarding information for advertised Virtual Private Network (VPN) routing and forwarding (VRF) instance routes, use the **show mpls forwarding vrf** command in privileged EXEC mode. To disable the display of label forwarding information, use the **no** form of this command.

show mpls forwarding vrf *vrf-name*[{*ip-prefix/length*[{*mask*}]}][{**detail**}][{*output-modifiers*}]
no show mpls forwarding vrf *vrf-name*[{*ip-prefix/length*[{*mask*}]}][{**detail**}][{*output-modifiers*}]

Syntax Description

vrf-name	Displays network layer reachability information (NLRI) associated with the named VRF.
ip-prefix/length	(Optional) IP prefix address (in dotted decimal format) and length of mask (0 to 32).
mask	(Optional) Destination network mask, in dotted decimal format.
detail	(Optional) Displays detailed information on the VRF routes.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was modified to reflect new Multiprotocol Label Switching (MPLS) Internet Engineering Taskforce (IETF) terminology and CLI command syntax and 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.
12.0(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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(22)S	The command output was modified so that directly connected VRF networks no longer display as aggregate; no label appears instead.
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

Use this command to display label forwarding entries associated with a particular VRF or IP prefix.

Examples

The following example shows label forwarding entries that correspond to the VRF called vpn1:

```
        Router# show mpls forwarding vrf vpn1 detail
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
35     24 10.0.0.0/8[V]     0          Et0/0/4 10.0.0.1
        MAC/Encaps=14/22, MRU=1496, Tag Stack{24 19}
        00D006FEDBE100D0974988048847 0001800000013000
        VPN route: vpn1
        No output feature configured
    Per-packet load-sharing
```

Related Commands

Command	Description
show ip cef vrf	Displays VRFs and associated interfaces.
show mpls forwarding-table	Displays the contents of the LFIB.

show mpls forwarding-table

To display the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB), use the **show mpls forwarding-table** command in user EXEC or privileged EXEC mode.

Note When a local label is present, the forwarding entry for IP imposition will not be showed; if you want to see the IP imposition information, use **show ip cef**.

show mpls forwarding-table [{*network* {*masklength*} | **interface** *interface* | **labels** *label* [**dash** *label*] | **lcatm atm** *atm-interface-number* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**vrf** *vrf-name*] [**detail slot** *slot-number*]

Syntax Description

network	(Optional) Destination network number.
mask	IP address of the destination mask whose entry is to be shown.
length	Number of bits in the mask of the destination.
interface *interface*	(Optional) Displays entries with the outgoing interface specified.
labels *label-label*	(Optional) Displays entries with the local labels specified.
lcatm atm *atm-interface-number*	Displays ATM entries with the specified Label Controlled Asynchronous Transfer Mode (LCATM).
next-hop *address*	(Optional) Displays only entries with the specified neighbor as the next hop.
lsp-tunnel	(Optional) Displays only entries with the specified label switched path (LSP) tunnel, or with all LSP tunnel entries.
tunnel-id	(Optional) Specifies the LSP tunnel for which to display entries.
vrf *vrf-name*	(Optional) Displays entries with the specified VPN routing and forwarding (VRF) instance.
detail	(Optional) Displays information in long form (includes length of encapsulation, length of MAC string, maximum transmission unit [MTU], and all labels).
slot *slot-number*	(Optional) Specifies the slot number, which is always 0.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.

Release	Modification
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T. The command was updated with MPLS terminology and command syntax.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. The command was modified to accommodate use of the MPLS experimental (EXP) level as a selection criterion for packet forwarding. The output display was modified to include a bundle adjacency field and exp (vcd) values when the optional **detail** keyword is specified.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. The IPv6 MPLS aggregate label and prefix information was added to the display.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S. The command output was modified to include explicit-null label information.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The output was changed in the following ways: • The term “tag” was replaced with the term “label.” • The term “untagged” was replaced with the term “no label.”
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. This command was modified to remove the **lsp-tunnel** keyword.
12.2(33)SXH	This command was modified. The command output shows the status of local labels in holddown for the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature. The status indicator showing that traffic is forwarded through an LSP tunnel is moved to the local label and the **lsp-tunnel** keyword was removed.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S. The output was modified to display the pseudowire identifier when the **interface** keyword is used.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS XE Release 3.12S	The output was modified to display the configured label blocks.

Examples

The following is sample output from the **show mpls forwarding-table** command:

```
Device# show mpls forwarding-table
Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
```

```
Label Label or VC   or Tunnel Id      switched  interface
26    No Label      10.253.0.0/16     0         Et4/0/0       10.27.32.4
28    1/33          10.15.0.0/16      0         AT0/0.1       point2point
29    Pop Label     10.91.0.0/16      0         Hs5/0         point2point
      1/36          10.91.0.0/16      0         AT0/0.1       point2point
30    32            10.250.0.97/32    0         Et4/0/2       10.92.0.7
      32            10.250.0.97/32    0         Hs5/0         point2point
34    26            10.77.0.0/24      0         Et4/0/2       10.92.0.7
      26            10.77.0.0/24      0         Hs5/0         point2point
35    No Label[T]   10.100.100.101/32 0         Tu301         point2point
36    Pop Label     10.1.0.0/16      0         Hs5/0         point2point
      1/37          10.1.0.0/16      0         AT0/0.1       point2point
[T]     Forwarding through a TSP tunnel.
        View additional labeling info with the 'detail' option
```

The following is sample output from the **show mpls forwarding-table** command when the IPv6 Provider Edge Router over MPLS feature is configured to allow IPv6 traffic to be transported across an IPv4 MPLS backbone. The labels are aggregated because there are several prefixes for one local label, and the prefix column contains “IPv6” instead of a target prefix.

```
Device# show mpls forwarding-table
Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
Label Label or VC   or Tunnel Id      switched  interface
16    Aggregate     IPv6              0
17    Aggregate     IPv6              0
18    Aggregate     IPv6              0
19    Pop Label     192.168.99.64/30  0         Se0/0         point2point
20    Pop Label     192.168.99.70/32  0         Se0/0         point2point
21    Pop Label     192.168.99.200/32 0         Se0/0         point2point
22    Aggregate     IPv6              5424
23    Aggregate     IPv6              3576
24    Aggregate     IPv6              2600
```

The following is sample output from the **show mpls forwarding-table detail** command. If the MPLS EXP level is used as a selection criterion for packet forwarding, a bundle adjacency exp (vcd) field is included in the display. This field includes the EXP value and the corresponding virtual circuit descriptor (VCD) in parentheses. The line in the output that reads “No output feature configured” indicates that the MPLS egress NetFlow accounting feature is not enabled on the outgoing interface for this prefix.

```
Device# show mpls forwarding-table detail
Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
label   label or VC     or Tunnel Id      switched  interface
16    Pop label       10.0.0.6/32        0         AT1/0.1       point2point
  Bundle adjacency exp(vcd)
  0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
  MAC/Encaps=12/12, MTU=4474, label Stack{}
      00010000AAAA030000008847
  No output feature configured
17    18            10.0.0.9/32        0         AT1/0.1       point2point
  Bundle adjacency exp(vcd)
  0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
  MAC/Encaps=12/16, MTU=4470, label Stack{18}
      00010000AAAA030000008847 00012000
  No output feature configured
18    19            10.0.0.10/32        0        AT1/0.1       point2point
  Bundle adjacency exp(vcd)
  0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
  MAC/Encaps=12/16, MTU=4470, label Stack{19}
      00010000AAAA030000008847 00013000
  No output feature configured
```

```
19    17            10.0.0.0/8         0        AT1/0.1       point2point
  Bundle adjacency exp(vcd)
  0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
  MAC/Encaps=12/16, MTU=4470, label Stack{17}
      00010000AAAA030000008847 00011000
  No output feature configured
20    20            10.0.0.0/8         0        AT1/0.1       point2point
  Bundle adjacency exp(vcd)
  0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
  MAC/Encaps=12/16, MTU=4470, label Stack{20}
      00010000AAAA030000008847 00014000
  No output feature configured
21    Pop label       10.0.0.0/24        0        AT1/0.1       point2point
  Bundle adjacency exp(vcd)
  0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
  MAC/Encaps=12/12, MTU=4474, label Stack{}
      00010000AAAA030000008847
  No output feature configured
22    Pop label       10.0.0.4/32         0        Et2/3         10.0.0.4
  MAC/Encaps=14/14, MTU=1504, label Stack{}
      000427AD10430005DDFE043B8847
  No output feature configured
```

The following is sample output from the **show mpls forwarding-table detail** command. In this example, the MPLS egress NetFlow accounting feature is enabled on the first three prefixes, as indicated by the line in the output that reads “Feature Quick flag set.”

```
Device# show mpls forwarding-table detail
Local  Outgoing    Prefix            Bytes label  Outgoing   Next Hop
label    label or VC   or Tunnel Id      switched   interface
16     Aggregate   10.0.0.0/8[V]     0
        MAC/Encaps=0/0, MTU=0, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
17     No label    10.0.0.0/8[V]      0          Et0/0/2    10.0.0.1
        MAC/Encaps=0/0, MTU=1500, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
18     No label    10.42.42.42/32[V] 4185       Et0/0/2    10.0.0.1
        MAC/Encaps=0/0, MTU=1500, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
19     2/33        10.41.41.41/32    0          AT1/0/0.1  point2point
        MAC/Encaps=4/8, MTU=4470, label Stack{2/33(vcd=2)}
        00028847 00002000
        No output feature configured
```

Cisco 10000 Series Examples

The following is sample output from the **show mpls forwarding-table** command for Cisco 10000 series routers:

```
Device# show mpls forwarding-table

Local   Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label   Label or VC   or Tunnel Id      Switched      interface
16      Pop Label     10.0.0.0/8        0             Fa1/0/0    10.0.0.2
```

```
        Pop Label     10.0.0.0/8        0             Fa1/1/0    10.0.0.2
17      Aggregate     10.0.0.0/8[V]     570           vpn2
21      Pop Label     10.11.11.11/32    0             Fa1/0/0    10.0.0.2
22      Pop Label     10.12.12.12/32    0             Fa1/1/0    10.0.0.2
23      No Label      10.3.0.0/16[V]     0             Fa4/1/0   10.0.0.2
```

The following is sample output from the **show mpls forwarding-table detail** command for Cisco 10000 series routers:

```
Device# show mpls forwarding-table detail

Local   Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label   Label or VC   or Tunnel Id      Switched      interface
16      Pop Label     10.0.0.0/8        0             Fa1/0/0    10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
        000B45C93889000B45C930218847
        No output feature configured
        Pop Label     10.0.0.0/8        0             Fa1/1/0     10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
        000B45C92881000B45C930288847
        No output feature configured
17      Aggregate    10.0.0.0/8[V]      570           vpn2
        MAC/Encaps=0/0, MRU=0, Label Stack{}
        VPN route: vpn2
        No output feature configured
21      Pop Label     10.11.11.11/32     0             Fa1/0/0     10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
       000B45C93889000B45C930218847
       No output feature configured
```

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

Table 111: show mpls forwarding-table Field Descriptions

Field	Description
Local label	Label assigned by this device.
Outgoing Label or VC **Note** This field is not supported on the Cisco 10000 series routers.	Label assigned by the next hop or the virtual path identifier (VPI)/virtual channel identifier (VCI) used to get to next hop. The entries in this column are the following: • [T]--Forwarding is through an LSP tunnel. • No Label--There is no label for the destination from the next hop or label switching is not enabled on the outgoing interface. • Pop Label--The next hop advertised an implicit NULL label for the destination and the device removed the top label. • Aggregate--There are several prefixes for one local label. This entry is used when IPv6 is configured on edge devices to transport IPv6 traffic over an IPv4 MPLS network.

Field	Description
Prefix or Tunnel Id	Address or tunnel to which packets with this label are sent. **Note** If IPv6 is configured on edge devices to transport IPv6 traffic over an IPv4 MPLS network, "IPv6" is displayed here. • [V]--The corresponding prefix is in a VRF.
Bytes label switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.
Bundle adjacency exp(vcd)	Bundle adjacency information. Includes the MPLS EXP value and the corresponding VCD.
MAC/Encaps	Length in bytes of the Layer 2 header and length in bytes of the packet encapsulation, including the Layer 2 header and label header.
MTU	MTU of the labeled packet.
label Stack	All the outgoing labels. If the outgoing interface is transmission convergence (TC)-ATM, the VCD is also shown. **Note** TC-ATM is not supported on Cisco 10000 series routers.
00010000AAAA030000008847 00013000	The actual encapsulation in hexadecimal form. A space is shown between Layer 2 and the label header.

Explicit-Null Label Example

The following is sample output, including the explicit-null label = 0 (commented in bold), for the **show mpls forwarding-table** command on a CSC-PE device:

```
Device# show mpls forwarding-table
Local  Outgoing      Prefix            Bytes label  Outgoing   Next Hop
label  label or VC   or Tunnel Id      switched     interface
17     Pop label     10.10.0.0/32      0            Et2/0      10.10.0.1
18     Pop label     10.10.10.0/24     0            Et2/0      10.10.0.1
19     Aggregate     10.10.20.0/24[V]  0
20     Pop label     10.10.200.1/32[V] 0            Et2/1      10.10.10.1
21     Aggregate     10.10.1.1/32[V]   0
22     0             192.168.101.101/32[V]   \
                                       0            Et2/1      192.168.101.101
23     0             192.168.101.100/32[V]   \
                                       0            Et2/1      192.168.101.100
25     0             192.168.102.125/32[V] 0        Et2/1      192.168.102.125 !outlabel
value 0
```

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

Table 112: show mpls forwarding-table Field Descriptions

Field	Description
Local label	Label assigned by this device.
Outgoing label or VC	Label assigned by the next hop or VPI/VCI used to get to the next hop. The entries in this column are the following: • [T]--Forwarding is through an LSP tunnel. • No label--There is no label for the destination from the next hop or that label switching is not enabled on the outgoing interface. • Pop label--The next hop advertised an implicit NULL label for the destination and that this device popped the top label. • Aggregate--There are several prefixes for one local label. This entry is used when IPv6 is configured on edge devices to transport IPv6 traffic over an IPv4 MPLS network. • 0--The explicit null label value = 0.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are sent. **Note** If IPv6 is configured on edge devices to transport IPv6 traffic over an IPv4 MPLS network, IPv6 is displayed here. • [V]--Means that the corresponding prefix is in a VRF.
Bytes label switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.

Cisco IOS Software Modularity: MPLS Layer 3 VPNs Example

The following is sample output from the **show mpls forwarding-table** command:

```
Device# show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  IPv4 VRF[V]      62951000      aggregate/v1
17    [H]  No Label   10.1.1.0/24      0             AT1/0/0.1 point2point
           No Label   10.1.1.0/24      0             PO3/1/0 point2point
      [T]  No Label   10.1.1.0/24      0             Tu1 point2point
18    [HT] Pop Label  10.0.0.3/32      0             Tu1 point2point
19    [H]  No Label   10.0.0.0/8       0             AT1/0/0.1 point2point
           No Label   10.0.0.0/8       0             PO3/1/0 point2point
20    [H]  No Label   10.0.0.0/8       0             AT1/0/0.1 point2point
           No Label   10.0.0.0/8       0             PO3/1/0 point2point
21    [H]  No Label   10.0.0.1/32      812           AT1/0/0.1 point2point
           No Label   10.0.0.1/32      0             PO3/1/0 point2point
```

```
22    [H]  No Label   10.1.14.0/24     0             AT1/0/0.1 point2point
           No Label   10.1.14.0/24     0             PO3/1/0 point2point
23    [HT] 16         172.1.1.0/24[V]  0             Tu1 point2point
24    [HT] 24         10.0.0.1/32[V]   0             Tu1 point2point
25    [H]  No Label   10.0.0.0/8[V]    0             AT1/1/0.1 point2point
26    [HT] 16         10.0.0.3/32[V]   0             Tu1 point2point
27         No Label   10.0.0.1/32[V]   0             AT1/1/0.1 point2point
[T]     Forwarding through a TSP tunnel.
        View additional labelling info with the 'detail' option
[H]     Local label is being held down temporarily.
```

The table below describes the Local Label fields relating to the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature.

Table 113: show mpls forwarding-table Field Descriptions

Field	Description
Local Label	Label assigned by this device. • [H]--Local labels are in holddown, which means that the application that requested the labels no longer needs them and stops advertising them to its labeling peers. The label's forwarding-table entry is deleted after a short, application-specific time. If any application starts advertising a held-down label to its labeling peers, the label could come out of holddown. **Note** [H] is not shown if labels are held down globally. A label enters global holddown after a stateful switchover or a restart of certain processes in a Cisco IOS modularity environment. • [T]--The label is forwarded through an LSP tunnel. **Note** Although [T] is still a property of the outgoing interface, it is shown in the Local Label column. • [HT]--Both conditions apply.

L2VPN Inter-AS Option B: Example

The following is sample output from the **show mpls forwarding-table interface** command. In this example, the pseudowire identifier (that is, 4096) is displayed in the Prefix or Tunnel Id column. The **show mpls l2transport vc detail** command can be used to obtain more information about the specific pseudowire displayed.

```
Device# show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label    Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched       interface
1011       No Label   l2ckt(4096)          0          none       point2point
```

The table below describes the fields shown in the display.

Table 114: show mpls forwarding-table interface Field Descriptions

Field	Description
Local Label	Label assigned by this device.
Outgoing Label	Label assigned by the next hop or virtual path identifier (VPI)/virtual channel identifier (VCI) used to get to the next hop.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are going.
Bytes Label Switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.

Related Commands

Command	Description
neighbor send-label	Enables a BGP device to send MPLS labels with BGP routes to a neighboring BGP device.
neighbor send-label explicit-null	Enables a BGP device to send MPLS labels with explicit-null information for a CSC-CE device and BGP routes to a neighboring CSC-PE device.
show mpls l2transport vc detail	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a device.

show mpls forwarding-table exact-route

To display the exact path for the source and destination address pair, use the **show mpls forwarding-table exact-route** command in user EXEC or privileged EXEC mode.

show mpls forwarding-table exact-route label *label-number* {**bottom-label** *value* | **ipv4** *source destination* | **ipv6** *source destination* | **ethernet** *source destination*} [**detail**]

Syntax Description

label *label-number*	Displays the exact path for a source and destination address pair.
bottom-label *value*	Bottom label value. Range is from 0 to 1048575.
ipv4 *source destination*	Exact path for IPv4 traffic. The IPv4 source and destination addresses are in x.x.x.x format.
ipv6 *source destination*	Exact path for IPv6 traffic. The IPv6 source and destination addresses are in x:x::x format.
ethernet *source destination*	(Optional) Exact path for Ethernet traffic. The Ethernet source and destination addresses are in aaaa.bbbb.cccc format.
[**detail**]	(Optional) Displays detailed information about the exact path for the source and destination address pair.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.4(1)T	This command was introduced.
15.4(1)S	This command was integrated into Cisco IOS Release 15.4(1)S.

Usage Guidelines

The **ethernet** option is available only when the *label-number* specified in the **label** option is an L2VPN flow aware local label.

Examples

The following is detailed sample output from the **show mpls forwarding-table exact-route detail** command:

```
Device# show mpls forwarding-table exact-route label 16 ethernet source aaaa.aaaa.aaaa
destination bbbb.bbbb.bbbb detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         No Label   l2ckt(1)         0             Fa0/0/2    point2point
        MAC/Encaps=0/0, MRU=0, Label Stack{}
        No output feature configured
        Flow label: 4112
```

The following is sample output from the **show mpls forwarding-table exact-route** command:

```
Device# show mpls forwarding-table exact-route label 19 bottom-label 4112

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
19         20         4.4.4.4/32       687           Fa0/0/0    10.10.10.2
```

The following is sample output from the **show mpls forwarding-table exact-route** command, showing the exact path for IPv4 traffic:

```
Device# show mpls forwarding-table exact-route label 19 ipv4 source 1.1.1.1 destination
3.3.3.3

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
19         17         3.3.3.3/32       0             Fa1/1      12.12.12.2
```

Related Commands

Command	Description
show mpls forwarding-table	Displays the contents of the MPLS LFIB.

show mpls infra lfd block-database

To display Multiprotocol Label Switching (MPLS) block application key databases, use the **show mpls infra lfd block-database** command in privileged EXEC mode.

show mpls infra lfd block-database [{**detail** | **internal** | **slot** *number*}] | [{**label** *number* | **id** *id-value* [{**detail** | **internal** | **slot** *number*}]}]

Syntax Description

detail	(Optional) Displays detailed information.
internal	(Optional) Displays the internal event counter.
slot *number*	(Optional) Specifies slot and the slot number (0 to15) of the Label Forwarding Database (LFD).
label *number*	(Optional) Displays the MPLS label block and the label number (16 to1048575).
id *id-value*	(Optional) Displays the block ID (1 to 4294967295).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

To enable the **show mpls infra lfd block-database key** command, the user must firstly enter global configuration mode, and then enter the **service internal** command, followed by the **end** command.

Example

The following shows how to enable the **show mpls infra lfd block-database** command:

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# service internal
Device(config)# end
01:23:40: %SYS-5-CONFIG_I: Configured from console by console
Device# show mpls infra lfd block-database
```

Example

The following is sample output from the **show mpls infra lfd block-database id 3** command. In this example, the pseudowire identifier (that is, l2ckt[46]) corresponding to a label block is displayed.

```
Device#show mpls infra lfd block-database id 3
 Block-DB entry for block-id : 0x3
 Block-size : 10, App-Key type : AToM PWID
 App-Key entries:
 l2ckt(46) 16
 l2ckt(47) 17
 l2ckt(48) 18
```

```
l2ckt(49) 19
l2ckt(50) 20
l2ckt(51) 21
l2ckt(52) 22
l2ckt(53) 23
l2ckt(54) 24
l2ckt(55) 25
```

Related Commands

Command	Description
service internal	Enables **infra** commands to be configured.
show mpls forwarding-table	Displays the contents of the MPLS LFIB.
show mpls l2vc detail	Displays detailed information related to the VC.

show mpls interfaces

To display information about one or more or all interfaces that are configured for label switching, use the **show mpls interfaces** command in user EXEC or privileged EXEC mode.

show mpls interfaces [{*interface* | **vrf** *vpn-name*}] [**all**] [**detail**] [**internal**]

Syntax Description

interface	(Optional) Defines the interface about which to display label switching information.
vrf *vpn-name*	(Optional) Displays information about the interfaces that have been configured for label switching for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vpn-name*).
all	(Optional) When the **all** keyword is specified alone in this command, information about the interfaces configured for label switching is displayed for all VPNs, including the VPNs in the default routing domain.
detail	(Optional) Displays detailed label switching information.
internal	(Optional) Indicates whether Multiprotocol Label Switching (MPLS) egress NetFlow accounting is enabled.

Command Default

If no optional keyword or argument is specified in this command, summary information is displayed for each interface that has been configured for label switching in the default routing domain.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was updated with MPLS command syntax and terminology.
12.0(10)ST	The **internal** keyword was added.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(25)S	This command was modified to show Border Gateway Protocol (BGP) and static routing information.
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.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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

This command shows MPLS information about the specified interface, or about all the interfaces for which MPLS has been configured.

If no optional keyword or argument is specified in this command, summary information is displayed for each interface configured for label switching.

Examples

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

```
Router# show mpls interfaces
Interface              IP         Tunnel   Operational
Ethernet1/1/1          Yes (tdp)  No       No
Ethernet1/1/2          Yes (tdp)  Yes      No
Ethernet1/1/3          Yes (tdp)  Yes      Yes
POS2/0/0               Yes (tdp)  No       No
ATM0/0.1               Yes (tdp)  No       No          (ATM labels)
ATM3/0.1               Yes (ldp)  No       Yes         (ATM labels)
ATM0/0.2               Yes (tdp)  No       Yes
```

Cisco 10000 Series Example

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

```
Router# show mpls interfaces
Interface                    IP           Tunnel   BGP Static Operational
GigabitEthernet1/0/0         Yes          No       No  No     No
GigabitEthernet2/0/0         No           No       No  Yes    No
GigabitEthernet3/0/0         No           Yes      No  No     No
```

Note If an interface uses LC-ATM procedures, the associated line in the display is flagged with the notation (ATM labels).

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

Table 115: show mpls interfaces Field Descriptions

Field	Description
Interface	Interface name.
IP	If IP label switching (sometimes called hop-by-hop label switching) is enabled on this interface, the column entry is “Yes.” Otherwise, the entry is “No.”

Field	Description
Tunnel	If label switched path (LSP) tunnel labeling is on this interface, the column entry is “Yes.” Otherwise, the entry is “No.”
BGP	If BGP has been enabled, the column entry is “Yes.” Otherwise, the entry is “No.”
Static	If static routes have been enabled, the column entry is “Yes.” Otherwise, the entry is “No.”
Operational	If packets are being labeled, the column entry is “Yes.” Otherwise, the entry is “No.”

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

```
Router# show mpls interfaces detail
Interface Ethernet1/1/1:
        IP labeling enabled (tdp)
        LSP Tunnel labeling not enabled
        MPLS operational
        MPLS turbo vector
        MTU = 1500
Interface POS2/0/0:
        IP labeling enabled (ldp)
        LSP Tunnel labeling not enabled
        MPLS not operational
        MPLS turbo vector
        MTU = 4470
Interface ATM3/0.1:
        IP labeling enabled (ldp)
        LSP Tunnel labeling not enabled
        MPLS operational
        MPLS turbo vector
        MTU = 4470
        ATM labels: Label VPI = 1
                Label VCI range = 33 - 65535
                Control VC = 0/32
```

Cisco 10000 Series Example

The following example is sample output of the **show mpls interfaces detail** command:

```
Router# show mpls interfaces detail
Interface GigabitEthernet1/0/0:
         IP labeling enabled (ldp)
         LSP Tunnel labeling not enabled
         MPLS operational
         MTU = 1500
Interface POS2/0/0:
         IP labeling enabled (ldp)
         LSP Tunnel labeling not enabled
         MPLS not operational
         MTU = 4470
```

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

Table 116: show mpls interfaces detail Field Descriptions

Field	Description
Interface	Interface name.
IP labeling	If IP label switching is enabled on this interface, the entry is "enabled." Otherwise, the entry is "not enabled." The output also shows whether LDP or TDP is being used.
LSP Tunnel labeling	If the LSP tunnel labeling is enabled on this interface, the entry is "enabled." Otherwise, the entry is "not enabled."
MPLS	If packets are labeled, the entry is "operational." Otherwise, the entry is "not operational."
BGP	If BGP has been enabled, the entry is "enabled." Otherwise, the entry is "not enabled."
MTU	The setting of the maximum transmission unit, in bytes.
ATM labels: Label VPI	The virtual path identifier (VPI). **Note** This field does not apply to the Cisco 10000 series routers.
Label VCI range	The range of values used in the VPI field for label VCs. **Note** This field does not apply to the Cisco 10000 series routers.
Control VC	The values assigned to the control VC. **Note** This field does not apply to the 10000 series routers.

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

```
Router# show mpls interfaces all
Interface              IP           Tunnel   Operational
ATM1/1/0.1             Yes (tdp)    No       Yes
VRF vpn1:
ATM3/0/0.1             Yes (ldp)    No       Yes
VRF vpn2:
ATM3/0/0.2             Yes (ldp)    No       Yes
VRF vpn3:
ATM3/0/0.3             Yes (ldp)    No       Yes
VRF vpn4:
ATM3/0/0.4             Yes (ldp)    No       Yes
VRF vpn5:
ATM3/0/0.5             Yes (ldp)    No       Yes
VRF vpn6:
Interface              IP           Tunnel   Operational
ATM3/0/0.6             Yes (ldp)    No       Yes
VRF vpn7:
ATM3/0/0.7             Yes (ldp)    No       Yes
VRF vpn8:
ATM3/0/0.8             Yes (ldp)    No       Yes
VRF vpn9:
ATM3/0/0.9             Yes (ldp)    No       Yes
```

```
VRF vpn10:
ATM3/0/0.10            Yes (ldp)     No       Yes
VRF vpn11:
ATM3/0/0.11            Yes (ldp)     No       Yes
VRF vpn12:
ATM3/0/0.12            Yes (ldp)     No       Yes
.
.
.
```

The following is sample output from the **show mpls interfaces internal** command. The output shows whether MPLS egress NetFlow accounting is enabled on the interface. If MPLS egress NetFlow accounting is disabled, the Output_feature_state field displays 0x0. If MPLS egress Netflow accounting is enabled, the Output_feature_state field is any number, except 0x0.

```
Router# show mpls interfaces internal
Interface Ethernet0/0/1:
        IP labeling enabled (tdp)
        LSP Tunnel labeling not enabled
        MPLS operational
        IP to Tag Fast Feature Switching Vector
        MPLS turbo vector
        MTU = 1500, status=0x100043, appcount=1
        Output_feature_state=0x0
Interface Ethernet0/0/2:
        IP labeling enabled (tdp)
        LSP Tunnel labeling not enabled
        MPLS operational
        IP to Tag Fast Feature Switching Vector
        MPLS turbo vector
        MTU = 1500, status=0x100043, appcount=1
        Output_feature_state=0x1
```

Related Commands

Command	Description
mpls ip (global configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform.
mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.
mpls label protocol (global configuration)	Specifies the default label distribution protocol for a platform.
mpls label protocol (interface configuration)	Specifies the label distribution protocol to be used on a given interface.
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 ip binding

To display specified information about label bindings learned by the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), use the show **show mpls ip binding** command in user EXEC or privileged EXEC mode.

show mpls ip binding [{**vrf** *vrf-name* | **all**}] [*network* {*masklength*} [**longer-prefixes**]] [{**neighbor** *address* | **local**}] [**local-label** {**atm** *vpi vci* | *label* [**-** *label*]}] [**remote-label** {**atm** *vpi vc* **I** | *label* [**-** *label*]}] [**interface** *interface*] [{**generic** | **atm**}]
show mpls ip binding [{**vrf** *vrf-name* | **all**}] [{**detail** | **summary**}]

Cisco 10000 Series Routers
show mpls ip binding [*network* {*masklength*} [**longer-prefixes**]] [{**neighbor** *address* | **local**}] [**local-label** *label* [**-** *label*]] [**remote-label** *label* [**-** *label*]] [**generic**]
show mpls ip binding [{**detail** | **summary**}]

Syntax Description

vrf *vrf-name*	(Optional) Displays the LDP neighbors for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vrf-name*). **Note** This keyword and argument pair does not apply to the Cisco 10000 series routers.
all	(Optional) Displays binding information for all VRFs. **Note** This keyword does not apply to the Cisco 10000 series routers.
network	(Optional) Defines the destination network number.
mask	Defines the network mask, written as A.B.C.D.
length	Defines the mask length (1 to 32 characters).
longer-prefixes	(Optional) Selects any prefix that matches the *mask* with a *length* from 1 to 32 characters.
neighbor *address*	(Optional) Displays label bindings assigned by the selected neighbor.
local	(Optional) Displays the local label bindings.
local-label atm *vpi vci*	(Optional) Displays the entry with the locally assigned ATM label that matches the specified ATM label value. The virtual path identifier (VPI) range is 0 to 4095. The virtual channel identifier (VCI) range is 0 to 65535. **Note** These keywords and arguments do not apply to the Cisco 10000 series routers.
local-label *label-label*	(Optional) Displays entries with locally assigned labels that match the specified label values. Use the arguments and keyword to indicate the label range. The hyphen (-) keyword is required for a label range.

remote-label atm atm *vpi vci*	(Optional) Displays entries with remotely assigned ATM label values learned from neighbor routers that match the specified ATM label value. The VPI range is 0 to 4095. The VCI range is 0 to 65535. **Note** These keywords and arguments do not apply to the Cisco 10000 series routers.
remote-label *label-label*	(Optional) Displays entries with remotely assigned labels learned from neighbor routers that match the specified label values. Use the arguments to indicate the label range. The hyphen (-) keyword is required for a label range.
interface *interface*	(Optional) Displays label bindings associated with the specified interface (for label-controlled (LC)-ATM only). **Note** This keyword and argument pair does not apply to the Cisco 10000 series routers.
generic	(Optional) Displays only generic (non-LC-ATM) label bindings.
atm	(Optional) Displays only LC-ATM label bindings. **Note** This keyword does not apply to the Cisco 10000 series routers.
detail	(Optional) Displays detailed information about label bindings learned by LDP.
summary	(Optional) Displays summary information about label bindings learned by LDP.

Command Default

All label bindings are displayed when no optional arguments or keywords are specified.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	The VPI range of values was extended to 4095.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.

Release	Modification
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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **detail** keyword was added to display checkpoint status for local label bindings.
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

The **show mpls ip binding** command displays label bindings learned by LDP or the Tag Distribution Protocol (TDP).

Note TDP is not supported for LDP features in Cisco IOS 12.0(30)S and later releases, 12.2(27)SBC and later 12.2S releases, and 12.3(14)T and later releases.

To summarize information about label bindings learned by LDP, use the **show mpls ip binding summary** command in user EXEC or privileged EXEC mode.

A request can specify that the entire database be displayed, that a summary of entries from the database be displayed, or that the display be limited to a subset of entries. The subset can be limited according to any of the following:

- Prefix
- Input or output label values or ranges
- Neighbor advertising the label
- Interface for label bindings of interest (LC-ATM only)

Note LC-ATM label binding interface does not apply to the Cisco 10000 series routers.

- Generic (non-LC-ATM) label bindings
- LC-ATM label bindings

Note LC-ATM label binding interface does not apply to the Cisco 10000 series routers.

Examples

The following is sample output from the **show mpls ip binding** command. The output shows all the label bindings in the database.

```
Router# show mpls ip binding

  10.0.0.0/8
        in label:     20
        out label:    26        lsr: 10.0.0.55:0
        out vc label: 1/80      lsr: 10.0.7.7:2      ATM1/0.8
                      Active    ingress 3 hops (vcd 49)
  172.16.0.0/8
        in label:     25
        in vc label:  1/36      lsr: 10.0.7.7:2      ATM1/0.8
                      Active    egress (vcd 55)
        out label:    imp-null  lsr: 10.0.0.55:0     inuse
  192.168.0.66/32
        in label:     26
        in vc label:  1/39      lsr: 10.0.7.7:2      ATM1/0.8
                      Active    egress (vcd 58)
        out label:    16        lsr: 10.0.0.55:0     inuse
.
.
.
```

In the following example, a request is made for the display of the label binding information for prefix 192.168.44.0/24:

```
Router# show mpls ip binding 192.168.44.0 24
  192.168.44.0/24
        in label:     24
        in vc label:  1/37      lsr: 10.0.7.7:2      ATM1/0.8
                      Active    egress (vcd 56)
        out label:    imp-null  lsr: 10.0.0.55:0     inuse
```

In the following example, the local-label keyword is used to request that label binding information be displayed for the prefix with local label 58:

```
Router# show mpls ip binding local-label 58
  192.168.0.0/16
        in label:     58
        out label:    imp-null  lsr: 10.0.0.55:0     inuse
```

The following sample output shows the label bindings for the VPN routing and forwarding instance named vpn1:

```
Router# show mpls ip binding vrf vpn1
  10.3.0.0/16
        in label:    117
        out label:   imp-null  lsr:10.14.14.14:0
  10.13.13.13/32
        in label:    1372
        out label:   268       lsr:10.14.14.14:0
  10.14.14.14/32
        in label:    118
        out label:   imp-null  lsr:10.14.14.14:0
  10.15.15.15/32
        in label:    1370
        out label:   266       lsr:10.14.14.14:0
  10.16.16.16/32
        in label:    8370
```

```
        out label:   319       lsr:10.14.14.14:0
  10.18.18.18/32
        in label:    21817
        out label:   571       lsr:10.14.14.14:0
  30.2.0.0/16
        in label:    6943
        out label:   267       lsr:10.14.14.14:0
  10.30.3.0/16
        in label:    2383
        out label:   imp-null  lsr:10.14.14.14:0
  10.30.4.0/16
        in label:    77
        out label:   imp-null  lsr:10.14.14.14:0
  10.30.5.0/16
        in label:    20715
        out label:   504       lsr:10.14.14.14:0
  10.30.7.0/16
        in label:    17
        out label:   imp-null  lsr:10.14.14.14:0
  10.30.10.0/16
        in label:    5016
        out label:   269       lsr:10.14.14.14:0
  10.30.13.0/16
        in label:    76
        out label:   imp-null  lsr:10.14.14.14:0
```

The following sample output shows label binding information for all VRFs:

```
Router# show mpls ip binding all

  10.0.0.0/24
        in label:     imp-null
        out label:    imp-null  lsr: 10.131.0.1:0
  10.11.0.0/24
        in label:     imp-null
        out label:    imp-null  lsr: 10.131.0.1:0
  10.101.0.1/32
        out label:    imp-null  lsr: 10.131.0.1:0
  10.131.0.1/32
        in label:     20
        out label:    imp-null  lsr: 10.131.0.1:0      inuse
  10.134.0.1/32
        in label:     imp-null
        out label:    16        lsr: 10.131.0.1:0
VRF vrf1:
  10.0.0.0/24
        out label:    imp-null  lsr: 10.132.0.1:0
  10.11.0.0/24
        out label:    imp-null  lsr: 10.132.0.1:0
  10.12.0.0/24
        in label:     17
        out label:    imp-null  lsr: 10.132.0.1:0
  10.132.0.1/32
        out label:    imp-null  lsr: 10.132.0.1:0
  10.134.0.2/32
        in label:     18
        out label:    16        lsr: 10.132.0.1:0
  10.134.0.4/32
        in label:     19
        out label:    17        lsr: 10.132.0.1:0
  10.138.0.1/32
        out label:    imp-null  lsr: 10.132.0.1:0
```

Cisco 10000 Series Examples

The following sample shows binding information for a Cisco 10000 series router:

```
Router# show mpls ip binding

  0.0.0.0/0
        in label:     imp-null
  10.29.0.0/16
        in label:     imp-null
        out label:    imp-null  lsr: 10.66.66.66:0
        out label:    imp-null  lsr: 10.44.44.44:0
  10.20.0.0/24
        in label:     imp-null
        out label:    26        lsr: 10.66.66.66:0
        out label:    imp-null  lsr: 10.44.44.44:0
  10.30.0.0/24
        in label:     imp-null
        out label:    imp-null  lsr: 10.66.66.66:0
        out label:    18        lsr: 10.44.44.44:0
  10.44.44.44/32
        in label:     21
        out label:    19        lsr: 10.66.66.66:0
        in label:     imp-null
        out label:    26        lsr: 10.66.66.66:0
        out label:    imp-null  lsr: 10.44.44.44:0
  10.30.0.0/24
        in label:     imp-null
        out label:    imp-null  lsr: 10.66.66.66:0
        out label:    18        lsr: 10.44.44.44:0
  10.44.44.44/32
        in label:     21
        out label:    19        lsr: 10.66.66.66:0
        out label:    imp-null  lsr: 10.44.44.44:0    inuse
  10.55.55.55/32
        in label:     imp-null
        out label:    25        lsr: 10.66.66.66:0
        out label:    55        lsr: 10.44.44.44:0
  10.66.66.66/32
        in label:     18
        out label:    imp-null  lsr: 10.66.66.66:0    inuse
        out label:    16        lsr: 10.44.44.44:0
  10.255.254.244/32
        in label:     24
        out label:    16        lsr: 10.66.66.66:0
        out label:    59        lsr: 10.44.44.44:0
```

In the following example on a Cisco 10000 series router, a request is made for the display of the label binding information for prefix 172.16.44.44/32:

```
Router# show mpls ip binding 172.16.44.44 32
  172.16.44.44/32
        in label:     21
        out label:    19        lsr: 10.66.66.66:0
        out label:    imp-null  lsr: 10.44.44.44:0    inuse
```

In the following example on a Cisco 10000 series router, the local-label keyword is used to request that label binding information be displayed for the prefix with local label 21:

```
Router# show mpls ip binding local-label 21
```

```
10.44.44.44/32
      in label:     21
```

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

Table 117: show mpls ip binding Field Descriptions

Field	Description
172.16.44.44/32	Destination prefix. Indicates that the following lines are for a particular destination (network/mask).
in label	Incoming label. This is the local label assigned by the label switch router (LSR) and advertised to other LSRs. The label value imp-null indicates the well-known Implicit NULL label.
out label	Outgoing label. This is a remote label learned from an LDP neighbor. The neighbor is identified by its LDP ID in the lsr field.
inuse	Indicates that the outgoing label is in use for Multiprotocol Label Switching (MPLS) forwarding, that is, it is installed in the MPLS forwarding table (the Label Forwarding Information Base [LFIB]).
in vc label	Incoming MPLS ATM label. This is the local VPI/VCI assigned by the LSR as the incoming label for the destination and advertised to the upstream LSRs. **Note** This field applies to the Cisco 7500 series routers only.
out vc label	Outgoing MPLS ATM label. This is the VPI/VCI learned from the destination next hop as its label for the destination and advertised to this LSR. **Note** This field applies to the Cisco 7500 series routers only.
ATM1/0.8	The ATM interface with which the MPLS ATM label is associated. **Note** This field applies to the Cisco 7500 series routers only.

Field	Description
Active	State of the label VC (LVC) associated with the destination prefix. **Note** This field applies to the Cisco 7500 series routers only. States are the following: • Active. Established and operational. • Bindwait. Waiting for a response from the destination next hop. • Remote Resource Wait. Waiting for resources (VPI/VCI) to become available on the destination next hop. • Parent Wait. Transit LVC upstream side waiting for downstream side to become active. • AbortAckWait. Waiting for response to a Label Abort message sent to the destination next hop. • ReleaseWait. Waiting for response to a Label Withdraw message sent to an upstream neighbor.
vcd 49	Virtual circuit descriptor number for the LVC. **Note** This field applies to the Cisco 7500 series routers only.
ingress 3 hops	Indicates whether the LSR is an ingress, transit, or egress node for the destination. **Note** This field applies to the Cisco 7500 series routers only. Options include the following: • Ingress 3 hops. The LSR is an ingress edge router for the MPLS ATM cloud for the destination. • Egress. The LSR is an egress edge router for the MPLS ATM cloud for the destination. • Transit. The LSR is a transit LSR within the MPLS ATM cloud for the destination.

The following sample output displays detailed information about the label bindings:

```
Router# show mpls ip binding detail
  10.0.0.0/8, rev 2, chkpt: add-skipped
        in label:     imp-null   (owner LDP)
          Advertised to:
          10.60.60.60:0          10.30.30.30:0
        out label:    imp-null  lsr: 10.60.60.60:0
        out label:    imp-null  lsr: 10.30.30.30:0
  10.10.10.10/32, rev 18, chkpt: added
        in label:     17         (owner LDP)
          Advertised to:
          10.60.60.60:0          10.30.30.30:0
        out label:    142       lsr: 10.60.60.60:0
        out label:    19        lsr: 10.30.30.30:0    inuse
  10.0.0.1/32, rev 10, chkpt: add-skipped
        in label:     imp-null   (owner LDP)
```

```
          Advertised to:
          10.60.60.60:0          10.30.30.30:0
        out label:    21        lsr: 10.60.60.60:0
        out label:    17        lsr: 10.30.30.30:0
  10.30.30.30/32, rev 20, chkpt: added
        in label:     18         (owner LDP)
          Advertised to:
          10.60.60.60:0          10.30.30.30:0
        out label:    22        lsr: 10.60.60.60:0
```

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

Table 118: show mpls ip binding detail Field Descriptions

Field	Description
chkpt	The status of the checkpointed entry. • add-skipped--Means that the local label is a null label and does not need to be checkpointed. • added-- Means that the checkpoints entry was copied to the backup Route Processor (RP)
owner	The application that created the binding. • owner LDP--Means that LDP created the binding. • owner other--Means that another application created the binding, possibly Border Gateway protocol (BGP).
Advertised to	The LSRs that received the local label binding.
inuse or stale	The status of the label. • inuse--Indicates that the outgoing label is in use for MPLS forwarding, that is, it is installed in the MPLS forwarding table (LFIB). • stale--Indicates a label that is no longer in use. This happens when an LDP session is lost and the routers begin a graceful restart. Then the remote label bindings are marked stale.

Cisco 7500 Series Example

The following sample output shows summary information about the label bindings learned by LDP:

```
Router# show mpls ip binding summary

Total number of prefixes: 53

Generic label bindings
                     assigned        learned
       prefixes      in labels     out labels
             53             53             51

ATM label bindings summary
      interface   total  active   local  remote   Bwait   Rwait  IFwait
```

```
       ATM1/0.8       47       47       40       7        0        0        0
Router#
```

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

Table 119: show mpls ip binding summary Field Descriptions (Cisco 7500 Series Example)

Field	Description
Total number of prefixes	Number of destinations for which the LSR has label bindings.
Generic label bindings	Indicates the start of summary information for “generic” label bindings. Generic labels are used for MPLS forwarding on all interface types except MPLS ATM interfaces.
prefixes	Number of destinations for which the LSR has a generic label binding.
assigned in labels	Number of prefixes for which the LSR has assigned an incoming (local) label.
learned out labels	Number of prefixes for which the LSR has learned an outgoing (remote) label from an LDP neighbor.
ATM label bindings summary	Indicates the start of summary information for MPLS ATM label bindings. An ATM label is a VPI/VCI.
interface	Indicates a row in the ATM label bindings summary table. The summary information in the row is for ATM labels associated with this interface.
total	Total number of ATM labels associated with the interface.
active	Number of ATM labels (LVCs) in the active (operational) state.
local	Number of ATM labels assigned by this LSR for the interfaces. These are incoming labels.
remote	Number of ATM labels learned from the neighbor LSR for this interface. These are outgoing labels.
Bwait	Number of bindings (LVCs) waiting for a label assignment from the neighbor LSR for the interface.
Rwait	Number of bindings (LVCs) waiting for resources (VPI/VCIs) to become available on the neighbor LSR for the interface.
IFwait	Number of bindings (LVCs) waiting for labels to be installed for switching use.

Cisco 10000 Series Example

The following sample output displays summary information about the label bindings learned by LDP:

```
Router# show mpls ip binding summary
```

```
Total number of prefixes: 53

Generic label bindings
                     assigned        learned
       prefixes      in labels     out labels
             53             53             51
```

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

Table 120: show mpls ip binding summary Field Descriptions (Cisco 10000 Series Example)

Field	Description
Total number of prefixes	Number of destinations for which the LSR has label bindings.
Generic label bindings	Indicates the start of summary information for “generic” label bindings. Generic labels are used for MPLS forwarding on all interface types except MPLS ATM interfaces.
prefixes	Number of destinations for which the LSR has a generic label binding.
assigned in labels	Number of prefixes for which the LSR has assigned an incoming (local) label.
learned out labels	Number of prefixes for which the LSR has learned an outgoing (remote) label from an LDP neighbor.

Related Commands

Command	Description
show mpls atm-ldp bindings	Displays specified entries from the ATM label binding database.
show mpls ldp bindings	Displays the contents of the LIB.

show mpls ip iprm counters

To display the number of occurrences of various Multiprotocol Label Switching (MPLS) IP Rewrite Manager (IPRM) events, use the show mpls ip iprm counters command in privileged EXEC mode.

show mpls ip iprm counters

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command reports the occurrences of IPRM events.

Examples

The command in the following example displays the events that the IPRM logs:

```
Router# show mpls ip iprm counters
  CEF Tree Changes Processed/Ignored:           91/12
  CEF Deletes Processed/Ignored:                12/2
  Label Discoveries:                            74
  Rewrite Create Successes/Failures:            60/0
  Rewrite Gets/Deletes:                         82/0
  Label Announcements: Info/Local/Path:         6/119/80
  Walks: Recursion Tree/CEF Full/CEF interface: 78/2/0
```

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

Table 121: show mpls ip iprm counters Command Field Descriptions

Field	Description
CEF Tree Changes Processed/Ignored	Processed--The number of Cisco Express Forwarding tree change announcements that IPRM processed. Ignored--The number of Cisco Express Forwarding tree change announcements that IPRM ignored. Typically, IPRM processes tree change announcements only for prefixes in a routing table.
CEF Deletes Processed/Ignored	Processed--The number of Cisco Express Forwarding delete entry announcements that IPRM processed. Ignored--The number of Cisco Express Forwarding delete entry announcements that IPRM ignored. Typically, IPRM processes delete entry announcements only for prefixes in a routing table.
Label Discoveries	The number of label discoveries performed by IPRM. Label discovery is the process by which IPRM obtains prefix labels from the IP Label Distribution Modules (LDMs).
Rewrite Create Successes/Failures	Successes--The number of times IPRM successfully updated the MPLS forwarding information. Failures--The number of times IPRM attempted to update the MPLS forwarding information and failed.
Rewrite Gets/Deletes	Gets--The number of times IPRM retrieved forwarding information from the MPLS forwarding infrastructure. Deletes--The number of times IPRM removed prefix forwarding information from the MPLS forwarding infrastructure.
Label Announcements: Info/Local/Path	Info--The number of times an IP label distribution module informed IPRM that label information for a prefix changed. Local--The number of times an IP label distribution module specified local labels for a prefix. Path--The number of times an IP LDM specified outgoing labels for a prefix route.
Walks: Recursion Tree/CEF Full/CEF interface	Recursion Tree--The number of times IPRM requested Cisco Express Forwarding to walk the recursion (path) tree for a prefix. CEF Full--The number of times IPRM requested Cisco Express Forwarding to walk a Cisco Express Forwarding table and notify IPRM about each prefix. CEF interface--The number of times IPRM requested Cisco Express Forwarding to walk a Cisco Express Forwarding table and notify IPRM about each prefix with a path that uses a specific interface.

Related Commands

Command	Description
clear mpls ip iprm counters	Clears the IPRM counters.
show mpls ip iprm ldm	Displays information about the IP LDMs that have registered with the IPRM.

show mpls ip iprm ldm

To display information about the IP Label Distribution Modules (LDMs) that have registered with the IP Rewrite Manager (IPRM), use the show mpls ip iprm ldm command in privileged EXEC mode.

show mpls ip iprm ldm [{**table** {**all** | **table-id**} | **vrf vrf-name**}] [{**ipv4** | **ipv6**}]

Cisco 10000 Series Routers
show mpls ip iprm ldm [{**table** {**all** | **table-id**} | **vrf vrf-name**}] [**ipv4**]

Syntax Description

table	(Optional) Displays the LDMs for one or more routing tables.
all	Displays the LDMs for all routing tables.
table-id	Displays the LDMs for the routing table you specify. Table 0 is the default or global routing table.
vrf	(Optional) Displays the LDMs for the VPN routing and forwarding (VRF) instance you specify.
vrf-name	(Optional) The name of the VRF instance. You can find VRF names with the show ip vrf command.
ipv4	(Optional) Displays IPv4 LDMs.
ipv6	(Optional) Displays IPv6 LDMs. **Note** Applies to Cisco 7500 series routers only.

Command Default

If you do not specify any keywords or parameters, the command displays the LDMs for the global routing table (the default).

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)SSH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command displays the IP LDMs registered with IPRM.

Examples

The command in the following example displays the LDMs for the global routing tables. It shows that two LDMs (lcatm and ldp) are registered for the ipv4 global routing table, and that one LDM (bgp ipv6) is registered for the ipv6 global routing table.

```
Router# show mpls ip iprm ldm
  table (glbl;ipv4); ldms: 2
    lcatm, ldp
  table (glbl;ipv6); ldms: 1
    bgp ipv6
```

The command in the following example displays all of the LDMs registered with IPRM. The output shows the following:

- The LDMs called lcatm and ldp have registered with IPRM for the ipv4 global table.
- The LDM called bgp ipv6 is registered for the IPv6 global table.
- The LDM called bgp vpnv4 is registered for all IPv4 vrf routing tables.

```
Router# show mpls ip iprm ldm table all
  table (glbl;ipv4); ldms: 2
    lcatm, ldp
  table (glbl;ipv6); ldms: 1
    bgp ipv6
  table (all-tbls;ipv4); ldms: 1
    bgp vpnv4
```

The command in the following example displays the LDMs registered for the IPv6 routing tables.

```
Router# show mpls ip iprm ldm ipv6
  table (glbl;ipv6); ldms: 1
    bgp ipv6
```

Cisco 10000 Series Examples Only

The command in the following example displays the LDMs for the global routing tables. It shows that one LDM (ldp) is registered for the ipv4 global routing table.

```
Router# show mpls ip iprm ldm
  table (glbl;ipv4); ldms: 1
    ldp
```

The command in the following example displays all of the LDMs registered with IPRM. The output shows the following:

- The LDM called ldp has registered with IPRM for the ipv4 global table.
- The LDM called bgp vpnv4 is registered for all IPv4 vrf routing tables.

```
Router# show mpls ip iprm ldm table all
  table (glbl;ipv4); ldms: 1
    ldp
  table (all-tbls;ipv4); ldms: 1
    bgp vpnv4
```

Related Commands

Command	Description
show mpls ip iprm counters	Displays the number of occurrences of various IPRM events.

show mpls ip iprm statistics

To display information about the IP Rewrite Manager (IPRM) statistics, use the **show mpls ip iprm statistics** command in privileged EXEC mode.

show mpls ip iprm statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(20)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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show mpls ip iprm statistics** command:

```
Router# show mpls ip iprm statistics
Chunk cache size: IPv4 pfx/path:              ½
Chunk cache size: outinfo:                    2
```

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

Table 122: show mpls ip iprm statistics Field Descriptions

Field	Description
Chunk cache size	Displays the size of the cache.

Related Commands

Command	Description
show mpls ip iprm counters	Displays the number of occurrences of various MPLS IPRM events.

show mpls l2 vc detail

To display detailed information related to a virtual circuit (VC), use the **show mpls l2 vc detail** command in user EXEC or privileged EXEC mode.

show mpls l2 vc *vc-id* **detail**

Syntax Description

vc-id	Name of the VC.

Command Default

This command displays detailed information related to a VC.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
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)SRE	This command was modified. STANDBY and HOTSTANDBY were added as options for the Status column in output displays.
15.0(1)S	This command was integrated into Cisco IOS Release 15.(0)1S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Examples

The following is sample output from the **show mpls l2 vc 1100 detail** command:

```
Device# show mpls l2 vc 1100 detail

Local interface: VFI VPLS-1100 up
 MPLS VC type is VFI, internetworking type is Ethernet
 Destination address: 1.1.1.1,VC ID:1100, VC status: up
  Output interface: Tu0,imposed label stack {27 17}
  Preferred path: not configured
  Default path: active
  Next hop:point2point
 Create time:2d23h, last status change time: 2d23h
 Signaling protocol: LDP, peer 1.1.1.1:0 up
  MPLS VC labels: local 17, remote 17
  Group ID: local 0, remote 0
  MTU: local 1500, remote 1500
  Remote interface description:
 Sequencing: receive disabled, send disabled
 Control Word: on (configured: autosense)
 VC statistics
  packet totals: receive 1146978, send 3856011
  byte totals: receive 86579172, send 316899920
  packet drops: receive 0, send 0
```

The following examples show the status of the active and backup pseudowires before, during, and after a switchover.

The **show mpls l2 vc detail** command on the active PE device displays the status of the pseudowires.

```
Device# show mpls l2 vc detail

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0.1      ATM VPC CELL 50            10.1.1.2         100        UP
AT0/2/0.1      ATM VPC CELL 50            10.1.1.3         100        STANDBY
```

The **show mpls l2 vc detail** command on the backup PE device displays the status of the pseudowires. The active pseudowire on the backup PE device has the HOTSTANDBY status.

```
Device-standby# show mpls l2 vc detail

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0.1      ATM VPC CELL 50            10.1.1.2         100        HOTSTANDBY
AT0/2/0.1      ATM VPC CELL 50            10.1.1.3         100        DOWN
```

During a switchover, the status of the active and backup pseudowires changes:

```
Device# show mpls l2 vc detail

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0.1      ATM VPC CELL 50            10.1.1.2         100        RECOVERING
AT0/2/0.1      ATM VPC CELL 50            10.1.1.3         100        DOWN
```

After the switchover is complete, the recovering pseudowire shows a status of UP:

```
Device# show mpls l2 vc detail

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0.1      ATM VPC CELL 50            10.1.1.2         100        UP
AT0/2/0.1      ATM VPC CELL 50            10.1.1.3         100        STANDBY
```

Related Commands

Command	Description
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

show mpls l2transport binding

To display virtual circuit (VC) label binding information, use the **show mpls l2transport binding** command in privileged EXEC mode.

show mpls l2transport binding [{*vc-idip-address* | **local-label** *number* | **remote-label** *number*}]

Syntax Description

vc-id	(Optional) Displays VC label binding information for the specified VC.
ip-address	(Optional) Displays VC label binding information for the specified VC destination.
local-label *number*	(Optional) Displays VC label binding information for the specified local assigned label.
remote-label *number*	(Optional) Displays VC label binding information for the specified remote assigned label.

Command Modes

EXEC and Privileged EXEC (#)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(27)S	This command was updated to display AToM Virtual Circuit Connection Verification (VCCV) information.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(30)S	This command was updated to display Connectivity Verification (CV) type capabilities.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was updated to display Circuit Emulation (CEM) information for the Cisco 7600 series router.
Cisco IOS XE Release 2.3	The command was updated to display information about multisegment pseudowires.
12.2(1)SRE	This command was modified to display VC label binding information for the control word.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. The display was updated to show VC label binding information for the control word.

Release	Modification
Cisco IOS XE Release 3.1S	This command was modified. The display was updated to show VC label binding information for the control word.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example shows the VC label binding information for Cisco IOS Releases 12.0(27)S and 12.2(18)SXE and later releases:

```
Router# show mpls l2transport binding
Destination Address: 10.0.0.203,  VC ID: 1
    Local Label:  16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV Capabilities: Type 1, Type 2
    Remote Label: 16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV Capabilities: Type 1, Type 2
```

The following example shows the VC label binding information for Cisco IOS Release 12.2(30)S and later releases:

```
Router# show mpls l2transport binding
Destination Address: 10.5.5.51,  VC ID: 108
    Local Label:  16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
    Remote Label: 16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
```

The output of the command changed between Cisco IOS releases. The following table maps the older output to the new output:

Output in Cisco IOS Releases 12.0(27)S and 12.2(18)SXE	Output In Cisco IOS Release 12.2(30)S
`VCCV Capabilities`	`VCCV: CC Type`
`Type 1`	`CW [1]`
`Type 2`	`RA [2]`

The following sample output from the **show mpls l2transport binding** command shows the VC label binding information on a Cisco uBR10012 router:

```
Router# show mpls l2transport binding
Destination Address: 10.76.1.1,  VC ID: 2002
  Local Label:  42
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
```

```
      VCCV: CC Type: CW [1], RA [2]
            CV Type: LSPV [2]
  Remote Label: 60
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
Destination Address: 10.76.1.1,  VC ID: 2003
  Local Label:  46
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: CW [1], RA [2]
            CV Type: LSPV [2]
  Remote Label: 27
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
Destination Address: 10.76.1.1,  VC ID: 2004
  Local Label:  unassigned.
  Remote Label: 111
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
Destination Address: 10.76.1.1,  VC ID: 2017
  Local Label:  43
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: CW [1], RA [2]
            CV Type: LSPV [2]
  Remote Label: 110
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
Destination Address: 10.76.1.1,  VC ID: 2018
  Local Label:  45
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: CW [1], RA [2]
            CV Type: LSPV [2]
  Remote Label: 88
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
Destination Address: 10.76.1.1,  VC ID: 2019
  Local Label:  44
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: CW [1], RA [2]
            CV Type: LSPV [2]
  Remote Label: 16
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
```

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

Table 123: show mpls l2transport binding Field Descriptions

Field	Description
Destination Address	The IP address of the remote router's interface that is at the other end of the VC.
VC ID	The virtual circuit identifier assigned to one of the interfaces on the router.
Local Label	The VC label that a router signals to its peer router, which is used by the peer router during imposition.
Remote Label	The disposition VC label of the remote peer router.
Cbit	The control word bit. If it is set, the value is 1.
VC Type	The type of VC, such as Frame Relay, Ethernet, and ATM.
GroupID	The group ID assigned to the local or remote VCs.
MTU	The maximum transmission unit assigned.
Interface Desc	Interface parameters, if applicable.
VCCV Capabilities	(Cisco IOS Releases 12.0(27)S and 12.2(18)SXE and later releases) AToM VCCV information. This field displays how an AToM VCCV packet is identified. • Type 1--The Protocol ID field of the AToM Control Word (CW) is identified in the AToM VCCV packet. • Type 2--An MPLS Router Alert (RA) Level above the VC label in identified in the AToM VCCV packet. Type 2 is used for VC types that do not support or do not interpret the AToM Control Word.
VCCV: CC Type	(Cisco IOS Releases 12.2(30)S and later releases) The types of Control Channel (CC) processing that are supported. The number indicates the position of the bit that was set in the received octet. The following values can be displayed: • CW [1]--Control Word • RA [2]--Router Alert • TTL [3]--Time to Live • Unkn [x]--Unknown

Field	Description
CV Type	(Cisco IOS Releases 12.2(30)S and later releases) The type of Connectivity Verification (CV) packets that can be processed in the control channel of the MPLS pseudowire. The number indicates the position of the bit that was set in the received octet. • ICMP [1]--Internet Control Management Protocol (ICMP) is used to verify connectivity. • LSPV [2]--LSP Ping is used to verify connectivity. • BFD [3]--Bidirectional Forwarding Detection is used to verify connectivity for more than one pseudowire. • Unkn [x]--A CV type was received that could not be interpreted.

The following sample output shows information about L2VPN multisegment pseudowires (in bold):

```
Router# show mpls l2transport binding
  Destination Address: 10.1.1.1,  VC ID: 102
    Local Label:  17
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2], TTL [3]
              CV Type: LSPV [2]
    Remote Label: 16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2], TTL [3]
              CV Type: LSPV [2]
        PW Switching Point:
             Vcid   local IP addr      remote IP addr      Description
101         10.11.11.11    10.20.20.20         PW Switching Point PE3
              100         10.20.20.20    10.11.11.11         PW Switching Point PE2
```

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

Table 124: show mpls l2transport binding Field Descriptions for Multisegment Pseudowires

Field	Description
TTL	The Time to Live (TTL) setting of the label.
Vcid	The virtual circuit identifier.
local IP addr	The local IP address assigned to the switching point.
remote IP addr	The remote IP address assigned to the switching point.
Description	The description assigned to the switching point.

CEM circuits are supported on the Cisco 7600 series router transport time-division multiplexing (TDM) traffic. The following sample output displays AToM VCs and the applicable local and remote CEM settings as exchanged over LDP label mapping messages.

Router# **show mpls l2transport binding**

```
  Destination Address: 10.7.1.1,  VC ID: 100
    Local Label:  18
        Cbit: 1,    VC Type: CESoPSN BRI,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
        CEM/TDM Options
              Payload Bytes: 80,    Payload Type: 0
              SP bits: 11 - Data/Signaling,    CAS Type: CAS T1 SF
              RTP header in use: Yes,    Bitrate (Kbit/s): 64
              Differential Timestamp Mode: disabled
              Clock Frequency (kHz): 64
              Synchronization Source id: 0
    Remote Label: 19
        Cbit: 1,    VC Type: CESoPSN BRI,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
        CEM/TDM Options
              Payload Bytes: 80,    Payload Type: 0
              SP bits: 11 - Data/Signaling,    CAS Type: CAS T1 SF
              RTP header in use: Yes,    Bitrate (Kbit/s): 64
              Differential Timestamp Mode: disabled
              Clock Frequency (kHz): 64
              Synchronization Source id: 0
```

The following sample output shows the VC label binding information for the control word, which in this case is set to 0, meaning that it is disabled:

```
Router# show mpls l2transport binding 102
Destination Address: 10.1.1.3,  VC ID: 102
    Local Label:  1004
        Cbit: 0,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
    Remote Label: 1005
        Cbit: 0,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
```

The following sample output shows the maximum number of cells that can be packed (in bold) for both provider edge routers, as specified by the **cell-packing** command:

```
Router# show mpls l2transport binding 1010
  Destination Address: 10.6.1.2,  VC ID: 1010
    Local Label:  20008
        Cbit: 1,    VC Type: ATM VCC CELL,    GroupID: 0
        MTU: n/a,   Interface Desc: n/a
        Max Concatenated ATM Cells: 10
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2], BFD [3]
    Remote Label: 47
        Cbit: 1,    VC Type: ATM VCC CELL,    GroupID: 0
        MTU: n/a,   Interface Desc: n/a
        Max Concatenated ATM Cells: 10
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
```

Related Commands

Command	Description
cell-packing	Enables ATM over MPLS or L2TPv3 to pack multiple ATM cells into each MPLS or L2TPv3 packet.
show mpls l2transport hw-capability	Displays the transport types and their supported capabilities.
show mpls l2transport vc	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a router.

show mpls l2transport checkpoint

To display checkpointing information about Any Transport over MPLS (AToM) virtual circuits (VCs), use the **show mpls l2transport checkpoint** command in privileged EXEC mode.

show mpls l2transport checkpoint

Syntax Description

This command has no arguments or keywords.

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.
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 integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Examples

The output of the commands varies, depending on whether the output reflects the active or standby Route Processor (RP).

On the active RP, the command displays the following output:

```
Router# show mpls l2transport checkpoint
AToM Checkpoint info for active RP
Checkpointing is allowed
Bulk-sync checkpointed state for 1 VC
```

On the standby RP, the command displays the following output:

```
Router# show mpls l2transport checkpoint
AToM HA Checkpoint info for standby RP
1 checkpoint information block in use
```

In general, the output on the active RP shows that checkpointing information was sent to the backup RP. The output on the backup RP shows that checkpointing information was received from the active RP.

Related Commands

Command	Description
show mpls l2transport vc	Displays information about the checkpointed data when checkpointing is enabled.

show mpls l2transport hw-capability

To display the transport types supported on an interface, use the **show mpls l2transport hw-capability** command in privileged EXEC mode.

show mpls l2transport hw-capability interface *type number*

Syntax Description

interface	Displays information for the specified interface.
type number	Type and number of the interface. For example, serial6/0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(27)S	This command was updated to display AToM Virtual Circuit Connection Verification (VCCV) information.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(30)S	This command was updated to display VCCV type capabilities.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Usage Guidelines

This command can help you determine the interface to use for the various transport types. Use this command to check if core-facing and edge-facing interfaces can accommodate different transport types.

Examples

The following is partial sample output of the **show mpls l2transport hw-capability** command for Cisco IOS Releases 12.0(23)S, 12.2(14)S, and 12.2(15)T and later. For more information on the fields, see the table below.

```
Router# show mpls l2transport hw-capability interface serial5/1

Interface Serial5/1
Transport type FR DLCI
  Core functionality:
    MPLS label disposition supported
    Control word processing supported
    Sequence number processing not supported
  Edge functionality:
    MPLS label imposition supported
    Control word processing supported
```

```
    Sequence number processing not supported
.
.
.
```

Note These examples show only a portion of the output. The command displays the capabilities of every transport type.

The following is partial sample output of the **show mpls l2transport hw-capability** command for Cisco IOS Releases 12.0(27)S and 12.2(18)SXE and later releases. This output shows VCCV data under the Core Functionality section. Type 1 means that the AToM Control Word identified the AToM VCCV packet. For more information on the fields, see the table below.

```
Transport type FR DLCI
  Core functionality:
    MPLS label disposition supported
    Control word processing supported
    Sequence number processing not supported
    VCCV CC Type 1 processing supported
  Edge functionality:
    MPLS label imposition supported
    Control word processing supported
    Sequence number processing not supported
.
```

The following is partial sample output of the **show mpls l2transport hw-capability** command for Cisco IOS Releases 12.2(30)S and later releases. The VCCV output shows that AToM Control Word (CW) identified the AToM VCCV packet. For more information on the fields, see the table below.

```
Transport type FR DLCI
  Core functionality:
    MPLS label disposition supported
    Control word processing supported
    Sequence number processing not supported
    VCCV CC Type CW [1] processing supported
  Edge functionality:
    MPLS label imposition supported
    Control word processing supported
    Sequence number processing not supported
.
```

The following is a sample output of the **show mpls l2transport hw-capability** command that displays the transport types supported on the Gigabit Ethernet interface 3/0/0 on a Cisco uBR10012 router:

```
Router# show mpls l2transport hw-capability interface gigabitethernet 3/0/0
Interface GigabitEthernet3/0/0
Transport type DOCSIS
  Core functionality:
    MPLS label disposition supported
    Control word processing supported
    Sequence number processing not supported
    VCCV CC Type CW [1] processing not supported
  Edge functionality:
    Not supported
Transport type DOCSIS VLAN
  Core functionality:
```

```
    MPLS label disposition supported
    Control word processing supported
    Sequence number processing not supported
    VCCV CC Type CW [1] processing not supported
  Edge functionality:
    Not supported
```

The output of the command changed between Cisco IOS releases. The following table maps the older output to the newer output:

Output in Cisco IOS Releases 12.0(27)S and 12.2(18)SXE and later	Output In Cisco IOS Release 12.2(30)S
`VCCV CC processing supported`	`VCCV CC processing supported`
`Type 1`	`Type CW [1]`

The table below describes the fields shown in the **show mpls l2transport hw-capability** command display.

Table 125: show mpls l2transport hw-capability Field Descriptions

Field	Description
Transport type	Indicates the transport type.
Core functionality	Displays the functionalities that the core-facing interfaces support, such as label disposition, and control word and sequence number processing.
VCCV CC Type processing supported	Displays whether the core-facing interfaces support Control Word processing, or Router Alert Processing. (Cisco IOS Releases 12.0(27)S and 12.2(18)SXE and later) • Type 1--The Protocol ID field of in the AToM Control Word (CW) identified the AToM VCCV packet. (Cisco IOS Releases 12.2(30)S and later) • CW [1]--Control Word • Unkn [x]--Unknown. The number indicates the position of the bit that was set in the received octet.
Edge functionality	Displays the functionalities that the edge-facing interfaces support, such as label disposition, and control word and sequence number processing.

Related Commands

Command	Description
show mpls l2transport binding	Displays virtual circuit (VC) label binding information.
show mpls l2transport checkpoint	Displays the checkpoint information about Any Transport over MPLS (AToM) virtual circuits.
show mpls l2transport summary	Displays summary information about virtual circuits.

Command	Description
show mpls l2transport vc	Displays information about AToM virtual circuits and static pseudowires that have been enabled to route Layer 2 packets on a router.

show mpls l2transport static-oam

To display the status of Multiprotocol Label Switching (MPLS) Transport Profile (TP) static pseudowires, use the **show mpls l2transport static-oam** command in privileged EXEC mode.

show mpls l2transport static-oam [**fault** [{**inbound** | **outbound**}]] [*ip-address vc-id*]

Syntax Description

fault	Displays faults related to static pseudowires.
inbound	Displays faults related to inbound static pseudowires.
outbound	Displays faults related to outbound static pseudowires.
ip-address	Displays information related to the static pseudowire with the specified peeer IP address.
vc-id	Displays information related to the static pseudowire with the specified virtual circuit (VC) ID.

Command Default

Status messages are not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Usage Guidelines

This command is for MPLS-TP static pseudowires.

Examples

The following example enables the display of status messages for the static pseudowire with the peer IP address of 10.10.10.10 and the VC ID of 4:

```
Router# show mpls l2transport static-oam 10.10.10.10 4
```

Related Commands

Command	Description
debug mpls l2transport static-oam	Enables the display of messages related to static pseudowire operations administrative and management (OAM).

show mpls l2transport summary

To display summary information about virtual circuits (VCs) that have been enabled to route Any Transport over MPLS (AToM) Layer 2 packets on a router, use the **show mpls l2transport summary** command in privileged EXEC mode.

show mpls l2transport summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
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)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Examples

The following is a sample output of the **show mpls l2transport summary** command that shows summary information about the VCs that have been enabled to transport Layer 2 packets:

```
Router# show mpls l2transport summary
Destination address: 10.16.24.12 Total number of VCs: 60
0 unknown, 58 up, 0 down, 2 admin down
5 active vc on MPLS interface PO4/0
```

The following is a sample output of the **show mpls l2transport summary** command that shows summary information about the VCs that have been enabled to transport Layer 2 packets on a Cisco uBR10012 router:

```
Router# show mpls l2transport summary
Destination address: 10.76.1.1, total number of vc: 6
  0 unknown, 5 up, 1 down, 0 admin down, 0 recovering, 0 standby
  5 active vc on MPLS interface Gi3/0/0
```

The table below describes the fields shown in the **show mpls l2transport summary** command display.

Table 126: show mpls l2transport summary Field Descriptions

Field	Description
Destination address	IP address of the remote router to which the VC has been established.
Total number of VCs	Number of VCs that have been established.
unknown	Number of VCs that are in an unknown state.
up	Number of VCs that are operational.
down	Number of VCs that are not operational.
admin down	Number of VCs that have been disabled.

Related Commands

Command	Description
show mpls l2transport binding	Displays virtual circuit (VC) label binding information.
show mpls l2transport checkpoint	Displays the checkpoint information about Any Transport over MPLS (AToM) virtual circuits.
show mpls l2transport hw-capability	Displays the transport types and their supported capabilities.
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

show mpls l2transport vc

To display information about Any Transport over MPLS (AToM) virtual circuits (VCs) and static pseudowires that have been enabled to route Layer 2 packets on a router, use the **show mpls l2transport vc** command in user EXEC or privileged EXEC mode.

show mpls l2transport vc [[**vcid**] *vc-id-min*] [*vc-id-max*] [**interface** *type number* [*local-circuit-id*]] [**destination** {*ip-addresshostname*}] [**detail**] [**pwid** *pw-identifier*] [**vpls-id** *vpls-identifier*] [**stitch** *endpoint endpoint*]

Syntax Description

vcid	(Optional) Specifies the VC ID.
vc-id-min	(Optional) Minimum VC ID value. The range is 1 to 4294967295.
vc-id-max	(Optional) Maximum VC ID value. The range is 1 to 4294967295.
interface	(Optional) Specifies the interface or subinterface of the router that has been enabled to transport Layer 2 packets. Use this keyword to display information about the VCs that have been assigned VC IDs on that interface or subinterface.
type	(Optional) Interface type. For more information about the interface type, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
local-circuit-id	(Optional) The number assigned to the local circuit. This argument value is supported only with the following transport types: • For Frame Relay, enter the data-link connection identifier (DLCI) of the permanent virtual circuit (PVC). • For ATM adaptation layer 5 (AAL5) and cell relay, enter the virtual path identifier (VPI) or virtual channel identifier (VCI) of the PVC. • For Ethernet VLANs, enter the VLAN number.
destination	(Optional) Specifies the remote router.
ip-address	(Optional) The IP address of the remote router.
hostname	(Optional) The name assigned to the remote router.
detail	(Optional) Specifies detailed information about VCs.
pwid *pw-identifier*	(Optional) Specifies the number of a pseudowire for a single VC. Valid entries are from 1 to 4294967295.
vpls-id *vpls-identifier*	(Optional) Virtual Private LAN Switching (VPLS) ID extended community value.

stitch *endpoint endpoint*	(Optional) Specifies dynamically stitched pseudowires between specified endpoints. The endpoints are the Source Attachment Individual Identifier (SAII) and the Target Attachment Individual Identifier (TAII). When the **stitch** keyword is used with the **vpls-id** keyword, a single pair of stitched VCs is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(8a)E	This command was introduced.
12.0(21)ST	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 and implemented on the Cisco 10720 router.
12.0(23)S	This command was modified. The **interface** and **destination** keywords were added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and was implemented on the Supervisor Engine 720.
12.2(14)SZ	This command was integrated into Cisco IOS Release 12.2(14)SZ.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and was implemented on the Cisco 10000 series routers. The example output was changed for the Cisco 10000 series router, and two fields (SSO Descriptor and SSM segment/switch IDs) were removed from the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. This command was updated to include forwarding equivalence class (FEC) 129 signaling information for pseudowires configured through VPLS Autodiscovery, and to support provisioning Any Transport over MPLS (AToM) static pseudowires.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was modified. This command was updated to display the number of MAC address withdrawal messages sent and received as part of the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature. This command was updated to display pseudowire status between peer routers that have been configured for the MPLS Pseudowire Status Signaling feature.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Release	Modification
Cisco IOS XE Release 2.3	This command was modified. This command output was updated to display the following information: • The status of pseudowires before, during, and after a switchover. • The status of a pseudowire switching point for multisegment pseudowires. • The number of packets and bytes being sent from the router. The VC statistics fields include the word "transit" to show that the packet totals no longer include packets being sent to the router.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.
12.2(33)SXI4	This command was modified. The command output was updated to display information about load balancing and the imposition and disposition of flow labels for the L2VPN Advanced VPLS feature.
15.0(1)S	This command was modified. The command output was updated to display information about Bidirectional Forwarding Detection (BFD).
15.1(1)S	• This command was modified. Support for the L2VPN VPLS Inter-AS Option B feature was provided, and the **pwid**, **stitch**, and **vpls-id** keywords were added. • The command output was updated to display information about remote AC failures and when Virtual Circuit Connectivity Verification (VCCV) BFD status signaling is enabled.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

If you do not specify any keywords or arguments, the command displays a summary of all the VCs.

Examples

The output of the commands varies, depending on the type of Layer 2 packets being transported over AToM VCs.

The following sample output shows information about interfaces and VCs that have been configured to transport various Layer 2 packets on the router:

```
Router# show mpls l2transport vc

Local intf     Local circuit      Dest address    VC ID      Status
-------------  ------------------ --------------- ---------- ----------
Se5/0          FR DLCI 55         10.0.0.1        55         UP
AT4/0          ATM AAL5 0/100     10.0.0.1        100        UP
AT4/0          ATM AAL5 0/200     10.0.0.1        200        UP
AT4/0.300      ATM AAL5 0/300     10.0.0.1        300        UP
```

The table below describes the fields shown in the display.

Table 127: show mpls l2transport vc Field Descriptions

Field	Description
Local intf	Interface on the local router that has been enabled to transport Layer 2 packets.
Local circuit	Type and number (if applicable) of the local circuit. The output shown in this column varies, depending on the transport type: • For Frame Relay, the output shows the DLCI of the PVC. • For ATM cell relay and AAL5, the output shows the VPI or VCI of the PVC. • For Ethernet VLANs, the output shows the VLAN number. • For PPP and High-Level Data Link Control (HDLC), the output shows the interface number.
Dest address	IP address of the remote router's interface that is the other end of the VC.
VC ID	Virtual circuit identifier assigned to one of the interfaces on the router.

Status	Status of the VC, which can be one of the following:
	• Admin down—The VC was disabled by a user.
	• Down--The VC is not ready to carry traffic between the two VC endpoints. Use the **detail** keyword to determine the reason that the VC is down.
	• Hotstandby—The active pseudowire on a standby Route Processor (RP).
	• Recovering—The VC is recovering from a stateful switchover.
	• Standby—The VC is designated as the backup circuit in a stateful switchover configuration.
	• Up—The VC can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are programmed.
	  • The disposition interface is programmed if the VC has been configured and the client interface is up.
	  • The imposition interface is programmed if the disposition interface is programmed and you have a remote VC label and an Interior Gateway Protocol (IGP) label. The IGP label can be implicit null in a back-to-back configuration. An IGP label means there is a label switched path (LSP) to the peer.

The following sample output shows information about the nonstop forwarding (NSF), stateful switchover (SSO), and graceful restart capabilities on the AToM VC. The SSO portion indicates whether checkpoint data has been sent (on active) or received (on standby). When SSO data has not been successfully sent or has been released, the SSO information is not displayed.

```
Router# show mpls l2transport vc detail
Local interface: Fa5/1/1.2 down, line protocol down, Eth VLAN 2 up
  Destination address: 10.55.55.2, VC ID: 1002, VC status: down
```

```
    Output interface: Se4/0/3, imposed label stack {16}
    Preferred path: not configured
Default path: active
    Tunnel label: imp-null, next hop point2point
  Create time: 02:03:29, last status change time: 02:03:26
  Signaling protocol: LDP, peer 10.55.55.2:0 down
    MPLS VC labels: local 16, remote unassigned
    Group ID: local 0, remote unknown
    MTU: local 1500, remote unknown
    Remote interface description:
  Sequencing: receive disabled, send disabled
  SSO Descriptor: 10.55.55.2/1002, local label: 16
    SSM segment/switch IDs: 12290/8193, PWID: 8193
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

The table above and the tables below describe the fields shown in the display.

The following sample output shows the information that is displayed when an AToM static pseudowire has been provisioned and the **show mpls l2transport vc detail** command is used to check the configuration. The Signaling protocol field specifies Manual because a directed control protocol such as Label Distribution Protocol (LDP) cannot be used to exchange parameters on static pseudowires. The remote interface description field seen for nonstatic pseudowire configurations is not displayed because remote information is exchanged using signaling between the Provider Edge (PE) routers and this is not done on static pseudowires.

```
Router# show mpls l2transport vc detail
Local interface: Et1/0 up, line protocol up, Ethernet up
   Destination address: 10.1.1.2, VC ID: 100, VC status: up
     Output interface: Et2/0, imposed label stack {10003 150}
     Preferred path: not configured
     Default path: active
     Next hop: 10.0.0.2
   Create time: 00:18:57, last status change time: 00:16:10
   Signaling protocol: Manual
     MPLS VC labels: local 100, remote 150
     Group ID: local 0, remote 0
     MTU: local 1500, remote 1500
     Remote interface description:
   Sequencing: receive disabled, send disabled
   VC statistics:
     packet totals: receive 219, send 220
     byte totals:   receive 20896, send 26694
     packet drops:  receive 0, send 0
```

The table above and the tables below describe the fields shown in the display.

The following sample output shows VC statistics, including the number of packets and bytes being sent from the router. The VC statistics fields include the word “transit” to indicate that the packet totals no longer include packets being sent to the router.

```
Router# show mpls l2transport vc detail
Local interface: Et1/0 up, line protocol up, Ethernet up
.
.
.
VC statistics:
     transit packet totals: receive 219, send 220
```

```
transit byte totals:   receive 20896, send 26694
transit packet drops:  receive 0, send 0
```

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

Table 128: show mpls l2transport vc detail Field Descriptions

Field	Description
Local interface	Interface on the local router that has been enabled to send and receive Layer 2 packets. The interface varies, depending on the transport type. The output also shows the status of the interface.
line protocol	Status of the line protocol on the edge-facing interface.
Destination address	IP address of the remote router specified for this VC. Specify the destination IP address as part of the **mpls l2transport route** command.
VC ID	Virtual circuit identifier assigned to the interface on the router.

VC status	Status of the VC, which can be one of the following:
	• Admin down—The VC was disabled by a user.
	• Down—The VC is not ready to carry traffic between the two VC endpoints.
	• up—The VC is in a state where it can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are enabled.
	  • The disposition interface is enabled if the VC has been configured and the client interface is up.
	  • The imposition interface is enabled if the disposition interface is enabled and a remote VC label and an IGP label exist. The IGP label can be an implicit null in a back-to-back configuration. (An IGP label means there is an LSP to the peer.)

Output interface	Interface on the remote router that has been enabled to transmit and receive Layer 2 packets.
imposed label stack	Summary of the Multiprotocol Label Switching (MPLS) label stack used to direct the VC to the PE router.
Preferred path	Path that was assigned to the VC and the status of that path. The path can be an MPLS traffic engineering tunnel or an IP address or hostname of a peer PE router.
Default path	Status of the default path, which can be disabled or active. By default, if the preferred path fails, the router uses the default path. However, you can disable the router from using the default path when the preferred path fails by specifying the **disable-fallback** keyword with the **preferred-path** command.

Field	Description
Tunnel label	IGP label used to route the packet over the MPLS backbone to the destination router. The first part of the output displays the type of label. The second part of the output displays the route information. The tunnel label information can display any of the following states: • imp-null: Implicit null means that the provider (P) router is absent and the tunnel label will not be used. Alternatively, imp-null can signify traffic engineering tunnels between the PE routers. • no adjacency: The adjacency for the next hop is missing. • no route: The label is not in the routing table. • not ready, Cisco Express Forwarding disabled: Cisco Express Forwarding is disabled. • not ready, LFIB disabled: The MPLS switching subsystem is disabled. • not ready, LFIB entry present: The tunnel label exists in the Label Forwarding Information Base (LFIB), but the VC is down. • not ready, no route: An IP route for the peer does not exist in the routing table. • not ready, not a host table: The route in the routing table for the remote peer router is not a host route. • unassigned: The label has not been assigned.
Create time	Time (in hours, minutes, and seconds) when the VC was provisioned.
last status change time	Last time (in hours, minutes, and seconds) the VC state changed.
Signaling protocol	Type of protocol used to send the MPLS labels on dynamically configured connections. The output also shows the status of the peer router. For AToM statically configured pseudowires, the field indicates Manual because there is no exchange of labels using a directed control protocol, such as LDP.
MPLS VC labels	Local VC label is a disposition label, which determines the egress interface of an arriving packet from the MPLS backbone. The remote VC label is a disposition VC label of the remote peer router.
Group ID	Local group ID used to group VCs locally. The remote group ID is used by the peer to group several VCs.
MTU	Maximum transmission unit specified for local and remote interfaces.
Remote interface description	Interface on the remote router that has been enabled to transmit and receive Layer 2 packets.
Sequencing	Indicates whether sequencing of out-of-order packets is enabled or disabled.
SSO Descriptor	Identifies the VC for which the information was checkpointed.

Field	Description
local label	Value of the local label that was checkpointed (that is, sent on the active RP and received on the standby RP).
SSM segment/switch IDs	IDs used for the control plane and data plane for this VC. This data is not for customer use but for Cisco personnel for troubleshooting purposes. When the Source Specific Multicast (SSM) IDs are followed by the word "used," the checkpointed data has been successfully sent.
PWID	Pseudowire ID used in the data plane to correlate the switching context for the segment associated with the MPLS switching context. This data is not for customer use but for Cisco personnel for troubleshooting purposes.
packet totals	Number of packets sent and received. Received packets are those AToM packets received from the MPLS core. Sent packets are those AToM packets sent to the MPLS core. This number excludes dropped packets. **Note** If the VC statistics fields include the word "transit," the output shows the number of packets and bytes being sent from the router.
byte totals	Number of bytes sent and received from the core-facing interface, including the payload, control word if present, and AToM VC label. **Note** If the VC statistics fields include the word "transit," the output shows the number of packets and bytes being sent from the router.
packet drops	Number of dropped packets. **Note** If the VC statistics fields include the word "transit," the output shows the number of packets and bytes being sent from the router.

The following is sample output from the **show mpls l2transport vc detail** command when the VPLS Autodiscovery feature has been configured on VPLS pseudowires. The output that is specific to VPLS Autodiscovery is shown in bold.

```
Router# show mpls l2transport vc detail
Local interface: VFI my_test VFI up
  MPLS VC type is VFI, interworking type is Ethernet
  Destination address: 10.3.3.1, VC ID: 123456, VC status: up
    Next hop PE address: 10.55.55.2
    Output interface: Et3/0, imposed label stack {17 19}
    Preferred path: not configured
    Default path:
    Next hop: 10.1.0.2
  Create time: 2d05h, last status change time: 2d05h
Signaling protocol: LDP, peer 10.55.55.2:0 up
    MPLS VC labels: local 21, remote 19
    AGI: type 1, len 8,  0000 3333 4F4E 44C4
    Local AII:  type 1, len 4, 0909 0909 (10.9.9.9)
    Remote AII: type 1, len 4, 0303 0301 (10.3.3.3)
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
```

```
    packet totals: receive 22611, send 22611
    byte totals:   receive 2346570, send 2853581
    packet drops:  receive 0, send 0
```

The table below describes the fields shown in the display.

Table 129: show mpls l2transport vc detail Field Descriptions for VPLS Autodiscovery

Field	Description
Next hop PE address	IP address of the next hop router.
AGI	Attachment group identifier (AGI).
Local AII	Attachment individual identifier (AII)—the local IP address used for signaling.
Remote AII	Remote IP address used for signaling. This address is the provisioned IP address, which might be different from the LDP peer IP address.

The following is sample output from the **show mpls l2transport vc** command when the circuit emulation (CEM) interface is specified:

```
Router# show mpls l2transport vc interface CEM 3/1/1


Local intf  Local circuit  Dest address  VC ID  Status
----------  -------------  ------------  -----  ------
CE3/1/1     CESOPSN Basic 10.30.30.3    300    DOWN
```

The tables above and the tables below describes the fields shown in the display.

The following sample output displays (in bold) the number of MAC address withdrawal messages sent and received as part of the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature:

```
Router# show mpls l2transport vc detail

Local interface: VFI TEST VFI up
  MPLS VC type is VFI, interworking type is Ethernet
  Destination address: 10.1.1.1, VC ID: 1000, VC status: up
    Output interface: Se2/0, imposed label stack {17}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:04:34, last status change time: 00:04:15
  Signaling protocol: LDP, peer 10.1.1.1:0 up
    Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.1
    MPLS VC labels: local 16, remote 17
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
    MAC Withdraw: sent 5, received 3
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

The tables above and the tables below describe the fields shown in the display.

The following sample output displays (in bold) the status messages for the MPLS Pseudowire Status Signaling feature when it is enabled on both PE routers:

```
Router# show mpls l2transport vc detail

Local interface: Et1/0 up, line protocol up, Ethernet up
  Destination address: 10.1.1.1, VC ID: 456, VC status: up
    Output interface: Et2/0, imposed label stack {10005 10240}
    Preferred path: not configured
    Default path: active
    Next hop: 10.0.0.1
  Create time: 00:39:30, last status change time: 00:26:48
  Signaling protocol: LDP, peer 10.1.1.1:0 up
    Targeted Hello: 10.1.1.2(LDP Id) -> 10.1.1.1
  Status TLV support (local/remote)   : enabled/supported
    Label/status state machine        : established, LruRru
    Last local dataplane   status rcvd: no fault
    Last local SSS circuit status rcvd: no fault
    Last local SSS circuit status sent: no fault
    Last local  LDP TLV    status sent: no fault
    Last remote LDP TLV    status rcvd: PW DOWN(rx,tx faults)
  MPLS VC labels: local 2000, remote 10240
  Group ID: local 6, remote 0
  MTU: local 1500, remote 1500
  Remote interface description:
    Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 243651, send 243705
    byte totals:   receive 27768366, send 34109320
    packet drops:  receive 0, send 0
```

The table below describes the fields shown in the display.

Table 130: show mpls l2transport vc detail Field Descriptions for the MPLS Pseudowire Signaling Status Feature

Field	Description
Status TLV support (local/remote)	For the local router, the output indicates whether the MPLS Pseudowire Signaling Status feature is enabled or disabled. For the remote router, the output indicates whether the MPLS Pseudowire Signaling Status feature is supported.
Label/status state machine	The first value in the output indicates whether label advertisement has been established or not. The second value (LruRru) indicates the status of the local and remote routers. The following list translates the status codes: • D—Dataplane • L—local router • r or n—ready (r) or not ready (n) • R—remote router • S—Local shutdown • u or d—up (u) or down (d) status

Field	Description
Last local dataplane status rcvd	Last status message received about the dataplane on the local router.
Last local SSS circuit status rcvd	Last status message received about the subscriber service switch (SSS) on the local router.
Last local SSS circuit status sent	Last status message sent about the subscriber service switch on the local router.
Last local LDP TLV status sent	Last status message sent about the type, length, values (TLV) on the local router.
Last remote LDP TLV status rcvd	Last status message received about the TLV on the local router.

The following sample output from the **show mpls l2transport vc detail** command displays the status of multisegment pseudowires:

```
Router# show mpls l2transport vc detail
Local interface: Se3/0 up, line protocol up, HDLC up
  Destination address: 10.12.1.1, VC ID: 100, VC status: down
    Output interface: Se2/0, imposed label stack {23}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:03:02, last status change time: 00:01:41
  Signaling protocol: LDP, peer 10.12.1.1:0 up
    Targeted Hello: 10.11.1.1(LDP Id) -> 10.12.1.1, LDP is UP
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRrd
      Last local dataplane   status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: DOWN(PW-tx-fault)
      Last local  LDP TLV    status sent: No fault
      Last remote LDP TLV    status rcvd: DOWN(PW-tx-fault)
       PW Switching Point:
       Fault type  Vcid   local IP addr   remote IP addr   Description
       PW-tx-fault  101        10.13.1.1         10.12.1.1   S-PE2
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 19, remote 23
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 16, send 27
    byte totals:   receive 2506, send 3098
    packet drops:  receive 0, seq error 0, send 0
```

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

Table 131: show mpls l2transport vc detail Field Descriptions for the MPLS Multisegment Pseudowire Feature

Field	Description
Fault type	Type of fault encountered on the switching point.
Vcid	ID of the VC on which the fault occurred.

Field	Description
local IP addr	Local IP address of the pseudowire.
remote IP addr	Remote IP address of the pseudowire.
Description	Descriptions assigned to the segment of the pseudowire.

The following sample output from the **show mpls l2transport vc detail** command displays the status of the control word when it is not configured (that is, it defaults to autosense):

```
Router# show mpls l2transport vc 123400 detail
Local interface: Et0/0 up, line protocol up, Ethernet up
  Destination address: 10.1.1.2, VC ID: 123400, VC status: down
    Output interface: if-?(0), imposed label stack {}
    Preferred path: not configured
    Default path: no route
    No adjacency
  Create time: 01:03:48, last status change time: 01:03:48
  Signaling protocol: LDP, peer 10.1.1.3:0 up
    Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.2
    Status TLV support (local/remote)   : enabled/unknown (no remote binding)
      Label/status state machine        : local ready, LruRnd
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: not sent
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: unknown (no remote binding)
    MPLS VC labels: local 1002, remote unassigned
    Group ID: local 0, remote unknown
    MTU: local 1500, remote unknown
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: on (configured: autosense)
```

If the control word is negotiated by the peer and is different from the configured value, the configured value is shown in parentheses.

- If the control word is configured to be disabled, the displayed value is as follows:

```
Control Word: off (configured: disabled)
```

- If the control word is configured to be enabled but negotiated by the peer to be off, the displayed value is as follows:

```
Control Word: off (configured: enabled)
```

- If the control word is not configured, the displayed value is as follows:

```
Control Word: on (configured: autosense)
```

The following sample output from the **show mpls l2transport vc detail** command displays load balancing information and shows whether flow labels are added to the MPLS label as part of the L2VPN Advanced VPLS feature:

```
Router# show mpls l2transport vc detail
```

```
Local interface: VFI dci_vlan_100 VFI up
  MPLS VC type is VFI, interworking type is Ethernet
  Destination address: 10.2.2.2, VC ID: 100, VC status: up
    Output interface: Tu0, imposed label stack {16}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
    Load Balance: Flow
    Flow Label: enabled
```

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

Table 132: show mpls l2transport vc detail Field Descriptions for the L2VPN Advanced VPLS Feature

Field	Description
Load Balance	Displays the type of load-balancing configured. The load-balancing configuration can be either flow-based or port channel-based.
Flow Label	Indicates whether the imposition and disposition of flow labels for the pseudowire is enabled.

The following sample output from the **show mpls l2transport vc detail** command displays BFD information:

```
Router# show mpls l2transport vc detail
Local interface: AT1/1/0 up, line protocol up, ATM AAL5 10/101 up
 Destination address: 10.1.1.151, VC ID: 1234001, VC status: up
  Output interface: Gi1/0/0, imposed label stack {2000}
  Preferred path: not configured
  Default path: active
  Next hop: 10.151.152.1
 Create time: 6d03h, last status change time: 6d03h
 Signaling protocol: LDP, peer 10.1.1.151:0 up
  Targeted Hello: 10.1.1.152(LDP Id) -> 10.1.1.151, LDP is UP
  Status TLV support (local/remote)   : enabled/supported
   LDP route watch                    : enabled
   Label/status state machine         : established, LruRru
   Last local dataplane   status rcvd: No fault
   Last local SSS circuit status rcvd: No fault
   Last local SSS circuit status sent: No fault
   Last local  LDP TLV    status sent: No fault
   Last remote LDP TLV    status rcvd: No fault
   Last remote LDP ADJ    status rcvd: No fault
  MPLS VC labels: local 2000, remote 2000
  PWID: 20490
  Group ID: local 0, remote 0
  MTU: local 4470, remote 4470
  Remote interface description:
 Sequencing: receive disabled, send disabled
 Control Word: On (configured: autosense)
 VCCV BFD protection active
  BFD Template - sampleBFDTemplate
  CC Type -  1
  CV Type - fault detection only with IP/UDP headers
 VC statistics:
  transit packet totals: receive 0, send 0
  transit byte totals:   receive 0, send 0
  transit packet drops:  receive 0, seq error 0, send 0
```

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

Table 133: show mpls l2transport vc detail Field Descriptions for the BFD CC over VCCV - Support for ATM Pseudowire Feature

Field	Description
VCCV BFD protection active	Displays the VCCV BFD protection status.
BFD Template	Displays the BFD template name.
CC Type	Displays the CC type. • Type 1: control word. • Type 2: MPLS router alert label. • Type 3: MPLS pseudowire label with TTL.
CV Type	Displays the Control Verification type.

The following is sample output from the **show mpls l2transport vc** command when the L2VPN VPLS Inter-AS Option B feature has been configured. The fields in the display are self-explanatory or described in other tables in this document.

```
Router# show mpls l2transport vc
Load for five secs: 4%/1%; one minute: 4%; five minutes: 2%
Time source is hardware calendar, *17:26:56.066 GMT Mon Oct 18 2010
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
VFI auto       VFI                        10.1.1.1        100         UP
```

The following is sample output from the **show mpls l2transport vc detail** command when the L2VPN VPLS Inter-AS Option B feature has been configured. The output that is specific to the L2VPN VPLS Inter-AS Option B feature is shown in bold.

```
Router# show mpls l2transport vc detail
Load for five secs: 4%/1%; one minute: 4%; five minutes: 2%
Time source is hardware calendar, *17:27:28.076 GMT Mon Oct 18 2010
Local interface: VFI auto VFI up
  Interworking type is Ethernet
  Destination address: 192.0.2.1, VC ID: 100, VC status: up
  Next hop PE address: 198.51.100.1
    Output interface: Et1/0, imposed label stack {2012}
    Preferred path: not configured
    Default path: active
    Next hop: 10.0.0.3
  Create time: 00:00:48, last status change time: 00:00:48
  Signaling protocol: LDP, peer 192.0.2.3:0 up
    Targeted Hello: 192.0.2.6(from BGP) -> 192.0.2.8, LDP is UP
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: No fault
      Last local  LDP TLV    status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 1011, remote 2012
    PWID: 4096
```

```
    AGI: type 1, len 8, 000A 0001 0000 0001
    Local AII: type 1, len 4, 0101 0001 (203.0.113.1)
    Remote AII: type 1, len 4, 0201 0101 (203.0.113.5)
    VPLS-ID: 1:1
    Group ID: local n/a, remote n/a
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  SSO Descriptor: 203.0.113.5/100, local label: 1011
    SSM segment/switch IDs: 16387/8193 (used), PWID: 4096
  VC statistics:
    transit packet totals: receive 0, send 0
    transit byte totals:   receive 0, send 0
    transit packet drops:  receive 0, seq error 0, send 0
```

The table below describes the feature-specific significant fields shown in the display.

Table 134: show mpls l2transport vc detail Field Descriptions for the L2VPN VPLS Inter-AS Option B

Field	Description
PWID	Pseudowire identifier.
VPLS-ID	The VPLS identifier associated with the pseudowire.

The following is sample output from the **show mpls l2transport vc detail** command when there is a remote AC failure and when VCCV BFD status signaling is enabled, that is, **vccv bfd status signaling** is configured.

```
Router# show mpls l2transport vc detail
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *03:31:33.136 PST Thu Mar 24 2011
Local interface: Et1/0.1 up, line protocol up, Eth VLAN 1001 up
Destination address: 192.0.2.1, VC ID: 1234000, VC status: down
    Output interface: Et0/0, imposed label stack {150}
    Preferred path: not configured
    Default path: active
    Next hop: 198.58.100.2
  Create time: 00:03:45, last status change time: 00:00:02
  Signaling protocol: Manual
    Status TLV support (local/remote)   : enabled/N/A
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRrd
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: DOWN AC(rx/tx faults)
      Last local  LDP TLV    status sent: None
      Last remote LDP TLV    status rcvd: DOWN AC(rx/tx faults), (UP)
      Last remote LDP ADJ    status rcvd: No fault
 MPLS VC labels: local 100, remote 150
    PWID: 4096
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  VCCV BFD protection active
     BFD Template - t1
     CC Type -  1
     CV Type - fault detection and status signaling without IP/UDP headers
```

```
VC statistics:
  transit packet totals: receive 0, send 5
  transit byte totals:   receive 0, send 580
  transit packet drops:  receive 0, seq error 0, send 0
```

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

Table 135: show mpls l2transport vc detail Field Descriptions for Remote AC Failure

Field	Description
Last BFD dataplane status rcvd	Last status message received about the BFD dataplane on the local router.
Last local dataplane status rcvd	Last status message received about the dataplane on the local router.
Last local SSS circuit status rcvd	Last status message received about the subscriber service switch (SSS) on the local router.
Last local SSS circuit status sent	Last status message sent about the subscriber service switch on the local router.
Last remote LDP ADJ	Last status message received about the ADJ on the local router.
VCCV BFD protection active	Displays the VCCV BFD protection status.
BFD Template	Displays the BFD template name.
CC Type	Displays the CC type. • Type 1: control word. • Type 2: MPLS router alert label. • Type 3: MPLS pseudowire label with TTL.
CV Type	Displays the Control Verification type.

Sample Output for show mpls l2transport vc Command on a Cisco uBR10012 Router in the Brief Display Format in Cisco IOS Release 12.2(33)SCF

The following is sample output from the **show mpls l2transport vc** command when the L2VPN Pseudowire Redundancy feature has been configured. The fields in the display are self-explantory or described in other tables in this document:

```
Router# show mpls l2transport vc
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Bu254          DOCSIS 55                  10.2.3.4        55         DOWN
Bu254          DOCSIS 1000                10.2.3.4        1000       UP
Bu254          DOCSIS 400                 10.76.2.1       400        UP
Bu254          DOCSIS 600                 10.76.2.1       600        DOWN
Bu254          DOCSIS 1800                10.76.2.1       1800       UP
Bu254          DOCSIS 45454               10.76.2.1       45454      DOWN
```

Related Commands

Command	Description
show mpls forwarding-table	Displays the contents of the MPLS LFIB.
show mpls l2transport summary	Displays summary information about VCs that have been enabled to route AToM Layer 2 packets on a router.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

show mpls label range

To display the range of local labels available for use on packet interfaces, use the show **show mpls label range** command in privileged EXEC mode.

show mpls label range

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(9)ST	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.
XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. The “Usage Guidelines” and the sample command output changed.

Usage Guidelines

You can use the **mpls label range** command to configure a range for local labels that is different from the default range. The **show mpls label range** command displays both the label range currently in use and the label range that will be in use following the next router reload.

Examples

In the following example, the use of the **show mpls label range** command is shown before and after the **mpls label range** command is used to configure a label range that does not overlap the starting label range:

```
Router# show mpls label range
Downstream label pool: Min/Max label: 16/100000
Router# configure terminal
Router(config)# mpls label range 200 120000
Router(config)# exit
Router# show mpls label range
Downstream label pool: Min/Max label: 200/120000
```

Related Commands

Command	Description
mpls label range	Configures a range of values for use as local labels.

show mpls ldp backoff

To display information about the configured session setup backoff parameters and any potential Label Distribution Protocol (LDP) peers with which session setup attempts are being throttled, use the **show mpls ldp backoff** command in user EXEC or privileged EXEC mode.

show mpls ldp backoff [{**vrf** *vrf-name* | **all**}]

Syntax Description

vrf *vrf-name*	(Optional) Displays backoff information for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vrf-name*).
all	(Optional) Displays LDP discovery information for all VPNs.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(30)S	The **vrf** *vrf-name* keyword and argument pair and the **all** keyword were added.
12.4(3)	The **vrf** *vrf-name* keyword and argument pair and the **all** keyword were added.
12.4(4)T	The **vrf** *vrf-name* keyword and argument pair and the **all** keyword were added.
12.0(32)S	The **vrf** *vrf-name* keyword and argument pair and the **all** keyword were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
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 ldp backoff** command:

```
Router# show mpls ldp backoff

LDP initial/maximum backoff: 30/240 sec
Backoff table: 2 entries
LDP Id              Backoff(sec)   Waiting(sec)
10.144.0.44:0        60             30
10.155.0.55:0        120            90
```

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

Table 136: show mpls ldp backoff Field Descriptions

Field	Description
LDP initial/maximum backoff	Indicates the configured backoff parameters (initial and maximum) in seconds.
Backoff table	Contains a list of discovered LDP neighbors for which session setup is being delayed because of previous failures to establish a session due to incompatible configuration. The backoff table incorporates the following information: • LDP Id--Identifies the LDP neighbors. • Backoff(sec)--Shows the amount of time that session setup is being delayed. • Waiting(sec)--Shows the approximate amount of time that session setup has been delayed.

The following is sample output from the **show mpls ldp backoff vrf** *vrf-name* command that shows one entry in the Backoff table for VRF vrf1:

```
Router# show mpls ldp backoff vrf vrf1

LDP initial/maximum backoff: 15/120 sec
VRF vrf1 Backoff table: 1 entries
LDP Id              Backoff(sec)   Waiting(sec)
10.12.0.2:0         120            30
```

The following is sample output from a form of the **show mpls ldp backoff all** command:

```
Router# show mpls ldp backoff all

LDP initial/maximum backoff: 15/120 sec
Backoff table: 2 entries
LDP Id              Backoff(sec)   Waiting(sec)
10.155.0.55:0       120            30
10.144.0.44:0       60             60
```

```
VRF vrf1 Backoff table: 1 entries
LDP Id              Backoff(sec)   Waiting(sec)
10.12.0.2:0         120            45
VRF vrf2 Backoff table: 1 entries
LDP Id              Backoff(sec)   Waiting(sec)
10.13.0.1:0         120            30
```

See the table below for a description of the significant fields shown in the displays.

Related Commands

Command	Description
mpls ldp backoff	Configures session setup delay parameters for the LDP backoff mechanism.

show mpls ldp bindings

To display the contents of the Label Information Base (LIB), use the **show mpls ldp bindings** command in user EXEC or privileged EXEC mode.

show mpls ldp bindings [{**vrf** *vrf-name* | **all**}] [*network* {*masklength*} [**longer-prefixes**]] [**local-label** *label* [- *label*]] [**remote-label** *label* [- *label*]] [{**neighbor** *address* | **local**}] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the label bindings for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vrf-name*).
all	(Optional) Displays LIB information for all VPNs.
network	(Optional) Destination network number.
mask	Network mask, written as A.B.C.D.
length	Mask length (1 to 32 characters).
longer-prefixes	(Optional) Selects any prefix that matches the value in the *mask* argument with a *length* from 1 to 32 characters.
local-label *label-label*	(Optional) Display entries matching local label values. Use the *label-label* arguments and keyword to indicate the label range. The hyphen (-) keyword is required for a label range.
remote-label *label-label*	(Optional) Displays entries matching the label values assigned by a neighbor router. Use the *label-label* arguments and keyword to indicate the label range. The hyphen (-) keyword is required for a label range.
neighbor *address*	(Optional) Displays the label bindings assigned by the selected neighbor.
local	(Optional) Displays the local label bindings.
detail	(Optional) Displays the checkpoint status of the local label bindings.

Command Default

If no optional keywords or arguments are entered, the command displays the LIB for the default routing domain only.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to support Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.

Release	Modification
12.0(14)ST	This command was modified to include MPLS Virtual Private Network (VPN) support for Label Distribution Protocol (LDP).
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	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.
12.0(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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **detail** keyword was added.
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.
12.2(33)SRC	The output of the command was updated to display information about LDP local label allocation filtering.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **show mpls ldp bindings** command displays label bindings learned by the LDP or Tag Distribution Protocol (TDP).

Note TDP is not supported for LDP features in Cisco IOS 12.0(30)S and later releases, 12.2(28)SB and later 12.2S releases, and 12.3(14)T and later releases.

A request can specify that the entire database be displayed, or that the display be limited to a subset of entries according to the following:

- Prefix
- Input or output label values or ranges
- Neighbor advertising the label

Note The **show mpls ip bindings** command includes the output generated by the show mpls ldp bindings command. On the Cisco 7000 series router, this command displays information about label bindings for LC-ATM interfaces.

Examples

The following is sample output from the **show mpls ldp bindings** command. This form of the command displays the contents of the LIB for the default routing domain.

```
Router# show mpls ldp bindings
  10.0.0.0/8, rev 9
        local binding:  label: imp-null
        remote binding: lsr: 10.10.0.55:0, label: 17
        remote binding: lsr: 10.66.0.66:0, label: 18
        remote binding: lsr: 10.0.0.44:0, label: imp-null
  172.16.0.0/8, rev 17
        local binding:  label: 19
        remote binding: lsr: 10.0.0.55:0, label: imp-null
        remote binding: lsr: 10.66.0.66:0, label: 16
        remote binding: lsr: 10.0.0.44:0, label: imp-null
  192.168.0.66/32, rev 19
        local binding:  label: 20
        remote binding: lsr: 10.0.0.55:0, label: 19
        remote binding: lsr: 10.66.0.66:0, label: imp-null
        remote binding: lsr: 10.0.0.44:0, label: 18
.
.
.
```

The following is sample output from the **show mpls ldp bindings** *network length* **longer-prefixes neighbor** *address* variant of the command; it displays labels learned from label switch router (LSR) 10.144.0.44 for network 10.166.0.0 and any of its subnets. The use of the **neighbor** keyword suppresses the output of local labels and labels learned from other neighbors.

```
Router# show mpls ldp bindings 10.166.0.0 8 longer-prefixes neighbor 10.144.0.44
  10.166.44.0/16, rev 31
        remote binding: lsr: 10.144.0.44:0, label: 25
  10.166.45.0/16, rev 33
        remote binding: lsr: 10.144.0.44:0, label: 26
  10.166.245.0/16, rev 71
        remote binding: lsr: 10.144.0.44:0, label: 45
  10.166.246.0/16, rev 73
        remote binding: lsr: 10.144.0.44:0, label: 46
.
.
.
```

The following is sample output from the **show mpls ldp bindings vrf vpn1** command, which displays the label bindings for the specified VPN routing and forwarding instance named vpn1:

```
Router# show mpls ldp bindings vrf vpn1
  10.3.3.0/16, rev 164
        local binding: label:117
        remote binding:lsr:10.14.14.14:0, label:imp-null
  10.13.13.13/32, rev 1650
        local binding: label:1372
        remote binding:lsr:10.14.14.14:0, label:268
  10.14.14.14/32, rev 165
```

```
        local binding: label:118
        remote binding:lsr:10.14.14.14:0, label:imp-null
  10.15.15.15/32, rev 1683
        local binding: label:1370
        remote binding:lsr:10.14.14.14:0, label:266
  10.16.16.16/32, rev 775
        local binding: label:8370
        remote binding:lsr:10.14.14.14:0, label:319
  10.18.18.18/32, rev 1655
        local binding: label:21817
        remote binding:lsr:10.14.14.14:0, label:571
  10.30.2.0/16, rev 1653
        local binding: label:6943
        remote binding:lsr:10.14.14.14:0, label:267
  10.30.3.0/16, rev 413
        local binding: label:2383
        remote binding:lsr:10.14.14.14:0, label:imp-null
  10.30.4.0/16, rev 166
        local binding: label:77
        remote binding:lsr:10.14.14.14:0, label:imp-null
  10.30.5.0/16, rev 1429
        local binding: label:20715
        remote binding:lsr:10.14.14.14:0, label:504
  10.30.7.0/16, rev 4
        local binding: label:17
        remote binding:lsr:10.14.14.14:0, label:imp-null
  10.30.10.0/16, rev 422
        local binding: label:5016
        remote binding:lsr:10.14.14.14:0, label:269
.
.
.
```

The following is sample output from the **show mpls ldp bindings all** command, which displays the label bindings for all VRFs:

```
Router# show mpls ldp bindings all

  lib entry: 10.0.0.0/24, rev 4
        local binding:  label: imp-null
        remote binding: lsr: 10.131.0.1:0, label: imp-null
  lib entry: 10.11.0.0/24, rev 15
        local binding:  label: imp-null
        remote binding: lsr: 10.131.0.1:0, label: imp-null
  lib entry: 10.101.0.1/32, rev 18
        remote binding: lsr: 10.131.0.1:0, label: imp-null
  lib entry: 10.131.0.1/32, rev 17
        local binding:  label: 20
        remote binding: lsr: 10.131.0.1:0, label: imp-null
  lib entry: 10.134.0.1/32, rev 6
        local binding:  label: imp-null
        remote binding: lsr: 10.131.0.1:0, label: 16
VRF vrf1:
  lib entry: 10.0.0.0/24, rev 6
        remote binding: lsr: 10.132.0.1:0, label: imp-null
  lib entry: 10.11.0.0/24, rev 7
        remote binding: lsr: 10.132.0.1:0, label: imp-null
  lib entry: 10.12.0.0/24, rev 8
        local binding:  label: 17
        remote binding: lsr: 10.132.0.1:0, label: imp-null
  lib entry: 10.132.0.1/32, rev 4
        remote binding: lsr: 10.132.0.1:0, label: imp-null
  lib entry: 10.134.0.2/32, rev 9
```

```
        local binding:  label: 18
        remote binding: lsr: 10.132.0.1:0, label: 16
  lib entry: 10.134.0.4/32, rev 10
        local binding:  label: 19
        remote binding: lsr: 10.132.0.1:0, label: 17
  lib entry: 10.138.0.1/32, rev 5
        remote binding: lsr: 10.132.0.1:0, label: imp-null
```

The following is sample output from the **show mpls ldp bindings detail** command:

```
Router# show mpls ldp bindings detail
lib entry: 10.3.3.0/16, rev 2,
        local binding:  label: imp-null
          Advertised to:
          10.20.20.20:0          10.25.25.25:0
        remote binding: lsr: 10.20.20.20:0, label: imp-null  stale
        remote binding: lsr: 10.25.25.25:0, label: imp-null  stale
  lib entry: 10.13.1.0/24, rev 4,
        local binding:  label: imp-null
          Advertised to:
          10.20.20.20:0          10.25.25.25:0
        remote binding: lsr: 10.20.20.20:0, label: imp-null  stale
        remote binding: lsr: 10.25.25.25:0, label: 16  stale
  lib entry: 10.13.2.0/24, rev 6,
        local binding:  label: imp-null
          Advertised to:
          10.20.20.20:0          10.25.25.25:0
        remote binding: lsr: 10.20.20.20:0, label: 16  stale
        remote binding: lsr: 10.25.25.25:0, label: imp-null  stale
  lib entry: 10.6.1.0/24, rev 22,
        local binding:  label: 21
          Advertised to:
          10.20.20.20:0          10.25.25.25:0
        remote binding: lsr: 10.20.20.20:0, label: 19  stale
        remote binding: lsr: 10.25.25.25:0, label: imp-null  stale
```

The following is sample output from the **show mpls ldp bindings detail** command when LDP local label allocation filtering is configured:

```
Router# show mpls ldp bindings detail
Advertisement spec:
        Prefix acl = bar
Local label filtering spec: host routes.
  lib entry: 10.1.1.1/32, rev 9
  lib entry: 10.10.7.0/24, rev 10
  lib entry: 10.10.8.0/24, rev 11
  lib entry: 10.10.9.0/24, rev 12
  lib entry: 10.41.41.41/32, rev 17
  lib entry: 10.50.50.50/32, rev 15
  lib entry: 10.60.60.60/32, rev 18
  lib entry: 10.70.70.70/32, rev 16
  lib entry: 10.80.80.80/32, rev 14
```

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

Table 137: show mpls ldp bindings Field Descriptions

Field	Description
10.3.3.0/16 10.1.1.1/32	IP prefix and mask for a particular destination (network/mask).

Field	Description
rev 9	Revision number that is used internally to manage label distribution for this destination.
Advertised to	The LSRs that received the label binding.
local binding	Labels assigned by the local LSR.
remote binding	List of outgoing labels for this destination learned from other LSRs. Each item in this list identifies the LSR from which the outgoing label was learned and the label itself. The LSR is identified by its LDP identifier.
stale	After an LDP session is lost and the routers begin a graceful restart, the remote label bindings are marked stale.
Local label filtering spec: host routes.	LDP allocates local labels for host routes.

Related Commands

Command	Description
show mpls ip binding	Displays specified information about label bindings learned by the MPLS LDP.
show mpls ldp neighbor	Displays the status of LDP sessions.

show mpls ldp capabilities

To display the Label Distribution Protocol (LDP) capability information, use the **show mpls ldp capabilities** command in user EXEC or privileged EXEC mode.

show mpls ldp capabilities [{**vrf** *vrf-name* | **all**}]

Syntax Description

vrf *vrf-name*	(Optional) Displays the LDP capability information for the specified VPN routing and forwarding (VRF) instance.
all	(Optional) Displays LDP capability information for all VPNs, including those in the default routing domain.

Command Default

Displays information about LDP capability for the default routing domain if you do not specify the optional **vrf** or **all** keyword.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE4	This command was introduced.

Usage Guidelines

The **show mpls ldp capabilities** command can provide information about the capabilities that will be advertised through LDP sessions associated to a particular routing domain.

Examples

The following is sample output from the **show mpls ldp capabilities** command, which shows the router's capabilities associated with the default routing domain.

```
Router# show mpls ldp capabilities
LDP Capabilities - [<description> (<type>)]
-----------------------------------------------------------
    [Dynamic Announcement (0x0506)]
    [Typed Wildcard (0x050B)]
```

The following is sample output from the **show mpls ldp capabilities all** command, which shows the router's capabilities associated with all VRF routing domains including the default routing domain.

```
Router# show mpls ldp
capabilities all

LDP Capabilities - [<description> (<type>)]
-----------------------------------------------------------
    [Dynamic Announcement (0x0506)]
    [Typed Wildcard (0x050B)]
VRF vpn1:
    [Dynamic Announcement (0x0506)]
    [Typed Wildcard (0x050B)]
VRF vpn2:
```

```
    [Dynamic Announcement (0x0506)]
    [Typed Wildcard (0x050B)]
```

The following is sample output from the **show mpls ldp capabilities vrf** command, which shows the router's capabilities associated with the VRF routing domain named vpn1:

```
Router# show mpls ldp
capabilities vrf vpn1
LDP Capabilities - [<description> (<type>)]
------------------------------------------------------------
    [Dynamic Announcement (0x0506)]
    [Typed Wildcard (0x050B)]
```

Table 138: show mpls ldp neighbor Field Descriptions

Field	Description
LDP Capabilities	LDP capability information.
VRF	LDP capability information for the specified VRF.

Related Commands

Command	Description
show mpls ldp neighbor capabilities	Displays LDP announce and receive information for an LDP neighbor.
show mpls ldp neighbor details	Displays information in long form, including password information for a neighbor.

show mpls ldp checkpoint

To display information about the Label Distribution Protocol (LDP) checkpoint system on the active route processor, use the **show mpls ldp checkpoint** command in user EXEC or privileged EXEC mode.

show mpls ldp checkpoint

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
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 shows the following LDP checkpointing information:

- The status of the checkpointing system
- The status of the resend timer
- The number of Label Information Base (LIB) entries in a checkpointed state

This command displays checkpoint status information only for the active route processor.

Examples

The following example shows the LDP checkpoint settings and configuration:

```
Router# show mpls ldp checkpoint
Checkpoint status: dynamic-sync
Checkpoint resend timer: not running
5 local bindings in add-skipped
9 local bindings in added
1 of 15+ local bindings in none
```

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

Table 139: show mpls ldp checkpoint Field Descriptions

Field	Description
Checkpoint status	The status of the checkpointing system. If the status shows dynamic-sync or another enabled state, then the checkpointing system is enabled. If the status shows disabled, then the checkpointing system is disabled.

Field	Description
Checkpoint resend timer	The status of the resend timer.
local bindings in add-skipped	The number of local bindings that were not checkpointed, because they do not need to be checkpointed. For example, local label bindings using null labels are not checkpointed.
local bindings in added	The number of local bindings that were copied to the standby route processor.
local bindings in none	The number of local bindings that reside on the active route processor and need to be copied to the backup route processor.

Related Commands

Command	Description
show mpls ldp graceful-restart	Displays a summary of the LDP Graceful Restart status.

show mpls ldp discovery

To display the status of the Label Distribution Protocol (LDP) discovery process, use the **show mpls ldp discovery** command in user EXEC or privileged EXEC mode.

show mpls ldp discovery [{**vrf** *vrf-name* | **all**}] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the neighbor discovery information for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.
all	(Optional) Displays LDP discovery information for all VPNs, including those in the default routing domain.
detail	(Optional) Displays detailed information about all LDP discovery sources on a label switch router (LSR).

Command Default

This command displays neighbor discovery information for the default routing domain if an optional **vrf** keyword is not specified.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST. The command was modified to comply with Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was modified for MPLS VPN support for LDP. The vrf and all keywords were added.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(8)T	This command was modified for MPLS VPN support for LDP. The vrf and all keywords were added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(14)T	The **detail** keyword was added to the command to display information related to the LDP Autoconfiguration feature.
12.2(28)SB	The **detail** keyword was updated to display information related to LDP Message Digest 5 (MD5) password configuration.

Release	Modification
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.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S and LDP MD5 password rollover information displays in the command output when the **detail** keyword is used with the **show mpls ldp discovery** command.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Release 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

This command displays neighbor discovery information for LDP or Tag Distribution Protocol (TDP). It generates a list of interfaces over which the LDP discovery process is running.

Examples

The following is sample output from the **show mpls ldp discovery** command:

```
Router# show mpls ldp discovery
Local LDP Identifier:
    10.1.1.1:0
Discovery Sources:
    Interfaces:
        Ethernet1/1/3 (ldp): xmit/recv
            LDP Id: 172.23.0.77:0
            LDP Id: 10.144.0.44:0
            LDP Id: 10.155.0.55:0
        ATM3/0.1 (ldp): xmit/recv
            LDP Id: 10.203.0.7:2
        ATM0/0.2 (tdp): xmit/recv
            TDP Id: 10.119.0.1:1
Targeted Hellos:
        10.8.1.1 -> 10.133.0.33 (ldp): active, xmit/recv
            LDP Id: 10.133.0.33:0
        10.8.1.1 -> 192.168.7.16 (tdp): passive, xmit/recv
            TDP Id: 10.133.0.33:0
Router#
```

The following is sample output from the **show mpls ldp discovery all** command, which shows the interfaces engaged in LDP discovery activity for all the VPN routing and forwarding instances, including those in the default routing domain. In this example, note that the same neighbor LDP ID (10.14.14.14) appears in all the listed VRF interfaces, highlighting the fact that the same IP address can coexist in different VPN routing and forwarding instances.

```
Router# show mpls ldp discovery all

Local LDP Identifier:
    10.12.12.12:0
    Discovery Sources:
    Interfaces:
        ATM1/1/0.1 (tdp):xmit/recv
            TDP Id:10.11.11.11:0
VRF vpn1:Local LDP Identifier:
    172.30.7.2:0
```

```
    Discovery Sources:
    Interfaces:
        ATM3/0/0.1 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn2:Local LDP Identifier:
    172.30.13.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.2 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn3:Local LDP Identifier:
    172.30.15.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.3 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn4:Local LDP Identifier:
    172.30.17.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.4 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn5:Local LDP Identifier:
    172.30.19.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.5 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn6:Local LDP Identifier:
    172.30.21.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.6 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn7:Local LDP Identifier:
    172.23.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.7 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn8:Local LDP Identifier:
    172.30.25.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.8 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn9:Local LDP Identifier:
    172.30.27.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.9 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn10:Local LDP Identifier:
    172.30.29.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.10 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn11:Local LDP Identifier:
    172.30.31.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.11 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
```

```
VRF vpn12:Local LDP Identifier:
    172.30.33.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.12 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn13:Local LDP Identifier:

Router#
```

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

Table 140: show mpls ldp discovery Field Descriptions

Field	Description
Local LDP Identifier	The LDP identifier for the local router. An LDP identifier is 6-bytes displayed in the form "IP address:number." By convention, the first four bytes of the LDP identifier constitute the router ID; integers, starting with 0, constitute the final two bytes of the IP address:number construct.
Interfaces	Lists the interfaces that are engaging in LDP discovery activity: • The xmit field--Indicates that the interface is sending LDP discovery hello packets. • The recv field--Indicates that the interface is receiving LDP discovery hello packets. • The (LDP) or (TDP) field--Indicates the Label Distribution Protocol or Tag Distribution Protocol configured for the interface. The LDP (or TDP) identifiers indicate the LDP (or TDP) neighbors discovered on the interface.
Targeted Hellos	Lists the platforms to which targeted hello messages are being sent: • The xmit, recv, (ldp), and (tdp) fields are as described for the Interfaces field. • The active field indicates that this LSR has initiated targeted hello messages. • The passive field indicates that the neighbor LSR has initiated targeted hello messages and that this LSR is configured to respond to the targeted hello messages from the neighbor. **Note** The entry for a given target platform may indicate both active and passive.

The following is sample output from the **show mpls ldp discovery detail** command showing that LDP was enabled by the **mpls ip** command and the **mpls ldp autoconfig** command:

```
Router# show mpls ldp discovery detail
Local LDP Identifier:
    10.11.11.11:0
    Discovery Sources:
    Interfaces:
        Serial2/0 (ldp): xmit/recv
            Enabled: Interface config, IGP config;
            Hello interval: 5000 ms; Transport IP addr: 10.11.11.11
            LDP Id: 10.10.10.10:0
```

```
Src IP addr: 172.140.0.1; Transport IP addr: 10.10.10.10
Hold time: 15 sec; Proposed local/peer: 15/15 sec
```

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

Table 141: show mpls ldp discovery detail Field Descriptions

Field	Description
Local LDP Identifier	The LDP identifier for the local router. An LDP identifier is a 6-byte construct displayed in the form “IP address:number.” By convention, the first four bytes of the LDP identifier constitute the router ID; integers, starting with 0, constitute the final two bytes of the IP address:number construct.
Interfaces	Lists the interfaces that are engaging in LDP discovery activity: • The xmit field--Indicates that the interface is sending LDP discovery hello packets. • The recv field--Indicates that the interface is receiving LDP discovery hello packets. • The (LDP) or (TDP) field--Indicates the Label Distribution Protocol or Tag Distribution Protocol configured for the interface. The LDP (or TDP) identifiers indicate the LDP (or TDP) neighbors discovered on the interface.
Interface config, IGP config;	Describes how LDP is enabled: • Interface config--Enabled by the **mpls ip** command. • IGP config--Enabled by the **mpls ldp autoconfig** command. • Interface config, IGP config;--Enabled by the**mpls ip** command and the **mpls ldp autoconfig** command.
Hello interval	Period of time (in milliseconds) between the sending of consecutive hello messages.
Transport IP addr	Specifies that the interface address should be advertised as the transport address in the LDP discovery hello messages.
LDP Id	LDP ID of the peer router.
Src IP addr	Source IP address of the local router.
Transport IP addr	Specifies that the named IP address should be advertised as the transport address in the LDP discovery hello messages sent on an interface.
Hold time	Period of time (in seconds) a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor.
Proposed local/peer	Hold times (in seconds) proposed for LDP hello timer by the local router and the peer router. LDP uses the lower of these two values as the hold time.

The following is sample output from the **show mpls ldp discovery detail** command, which displays information related to LDP MD5 passwords. Information related to MD5 passwords is pointed out in bold text in the output.

```
Router# show mpls ldp discovery detail
 Local LDP Identifier:
    10.10.10.10:0
    Discovery Sources:
    Interfaces:
        Ethernet1/0 (ldp): xmit/recv
            Hello interval: 5000 ms; Transport IP addr: 10.10.10.10
            LDP Id: 10.4.4.4:0
              Src IP addr: 10.0.20.4; Transport IP addr: 10.4.4.4
              Hold time: 15 sec; Proposed local/peer: 15/15 sec

  Password: not required, none, stale       <-- LDP MD5 password information
    Targeted Hellos:
        10.10.10.10 -> 10.3.3.3 (ldp): passive, xmit/recv
            Hello interval: 10000 ms; Transport IP addr: 10.10.10.10
            LDP Id: 10.3.3.3:0
              Src IP addr: 10.3.3.3; Transport IP addr: 10.3.3.3
              Hold time: 90 sec; Proposed local/peer: 90/90 sec

        Password: required, neighbor, in use     <-- LDP MD5 password information
```

Password information displayed by this command includes:

- Password requirement for the neighbor (required or not required).
- Password source in the current configuration. The source is described by one of the following:
  - neighbor--The password for the neighbor is retrieved from the **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** [**0** | **7**] *password* command. The *ip-address* argument is the router ID of the neighbor.
  - num--The password for the neighbor is retrieved from **mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* [**0** | **7**] *password* command. The *number* argument is a number from 1 to 32767. The *acl* argument is the name or number of an IP standard access list that permits the neighbor router ID.
  - fallback--The password for the neighbor is retrieved from **mpls ldp** [**vrf** *vrf-name*] **password fallback** *password* command.
  - none--No password is configured for this neighbor.
- Password used by LDP sessions established with the neighbor is from current or previous configuration (in use or stale).

Related Commands

Command	Description
mpls label protocol (global configuration)	Specifies the LDP or TDP to be used on a platform.
mpls label protocol (interface configuration)	Specifies the LDP or TDP to be used on a given interface.
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp neighbor password fallback	Configures an MD5 password for LDP sessions with peers.

Command	Description
mpls ldp neighbor password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list.
mpls ldp neighbor password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp neighbor password rollover duration	Configures the duration before the new password takes effect on an MPLS label switch router (LSR).
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.

show mpls ldp graceful-restart

To display a summary of the Label Distribution Protocol (LDP) Graceful Restart status, use the **show mpls ldp graceful-restart** command in user EXEC or privileged EXEC mode.

show mpls ldp graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
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 shows the following information about LDP sessions:

- Configured parameters.
- The state of the LDP sessions (for which Graceful Restart was negotiated during initialization).
- The list of LDP sessions for which graceful recovery is pending. However, the router has retained the state information from those neighbors.

Examples

The following example shows a summary of the LDP Graceful Restart settings and configuration:

```
Router# show mpls ldp graceful-restart
LDP Graceful Restart is enabled
Neighbor Liveness Timer: 5 seconds
Max Recovery Time: 200 seconds
Down Neighbor Database (0 records):
Graceful Restart-enabled Sessions:
VRF default:
    Peer LDP Ident: 10.18.18.18:0, State: estab
    Peer LDP Ident: 10.17.17.17:0, State: estab
```

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

Table 142: show mpls ldp graceful-restart Field Descriptions

Field	Description
Neighbor Liveness Timer	The number of seconds the neighbor liveness timer is set for.
Max Recovery Time	The number of seconds the maximum recovery timer is set for.
Down Neighbor Database	Information about the down (failed or restarting) LDP neighbor.
Graceful Restart-enabled Sessions	Information about the LDP sessions that are enabled for Graceful Restart.
Peer LDP Ident	The LDP ID of the provider edge (PE) neighbor.
State	The state of the session with the neighbor.

Related Commands

Command	Description
show mpls ldp neighbor	Displays the status of LDP sessions.

show mpls ldp igp sync

To display the status of the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization process, use the **show mpls ldp igp sync** command in user EXEC or privileged EXEC mode.

show mpls ldp igp sync [{**all** | **interface** *type-number* | **vrf** *vrf-name*}]

Syntax Description

all	(Optional) Displays all the MPLS LDP-IGP synchronization information available.
interface *type-number*	(Optional) Displays the MPLS LDP-IGP synchronization information for the specified interface.
vrf *vrf-name*	(Optional) Displays the MPLS LDP-IGP synchronization information for the specified Virtual Private Network (VPN) routing and forwarding instance (*vpn-name*).

Command Default

If an optional argument is not specified, this command displays LDP synchronization for all interfaces enabled for MPLS LDP-IGP synchronization.

Command Modes

User EXEC(>)
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.
12.0(32)S	This command was integrated into Cisco IOS Release 12.0(32)S. The output of this command was changed to display the configured delay time and the time remaining on the delay timer.
12.4(12)	This command was integrated into Cisco IOS Release 12.4(12).
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Examples

The following is sample output from the **show mpls ldp igp sync** command when LDP-IGP synchronization is not enabled on an interface:

```
Router# show mpls ldp igp sync
Ethernet0/0:
 LDP configured;  SYNC enabled.
```

```
 SYNC status: sync achieved; peer reachable.
 IGP holddown time: infinite.
 Peer LDP Ident: 10.130.0.1:0
 IGP enabled: OSPF 1
```

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

Table 143: show mpls ldp igp sync Field Descriptions

Field	Description
Ethernet0/0	Interface name and type.
LDP configured	Label Distribution Protocol is configured.
SYNC enabled	Synchronization is active.
SYNC status	Synchronization is successful. **Note** Peer reachable is an LDP internal state used only for MPLS LDP synchronization. Do not use it to verify that LDP can reach the peer or to troubleshoot LDP functionality.
IGP holddown time	Interior Gateway Protocol hold-down time. • Infinite--No specific time is set.
Peer LDP Ident	IP address of the peer.
IGP enabled	Interior Gateway Protocol is enabled for the specified Open Shortest Path First (OSPF) protocol.

If LDP-IGP synchronization is not enabled on an interface, the output looks like the following:

```
Router# show mpls ldp igp sync
Ethernet5/1:
 LDP configured; LDP-IGP Synchronization not enabled.
```

The following is sample output from the **show mpls ldp igp sync** command when you configured a time delay for MPLS LDP-IGP synchronization:

```
Router# show mpls ldp igp sync
Ethernet0/0:
 LDP configured; LDP-IGP Synchronization enabled.
 Sync status: sync achieved; peer reachable.
 Sync delay time: 20 seconds (10 seconds left)
 IGP holddown time: infinite.
 IGP enabled: OSPF 1
```

Related Commands

Command	Description
debug mpls ldp igp sync	Displays events related to MPLS LDP -IGP synchronization.
mpls ldp igp sync	Enables MPLS LDP-IGP synchronization on an interface that belongs to an OSPF process.

Command	Description
mpls ldp igp sync holddown	Specifies how long an IGP should wait for LDP synchronization to be achieved.
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process or an IS-IS process.

show mpls ldp neighbor

To display the status of Label Distribution Protocol (LDP) sessions, use the **show mpls ldp neighbor** command in user EXEC or privileged EXEC mode.

show mpls ldp neighbor [{**vrf** *vrf-name* | **all**}] [{*addressinterface*}] [**detail**] [**graceful-restart**] [**capabilities**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the LDP neighbors for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.
all	(Optional) Displays LDP neighbor information for all VPNs, including those in the default routing domain.
address	(Optional) IP address of this neighbor.
interface	(Optional) Interface over which the LDP neighbors are accessible.
detail	(Optional) Displays information in long form, including password information for this neighbor.
graceful-restart	(Optional) Displays per-neighbor graceful restart information.
capabilities	(Optional) Displays LDP announce and receive information for an LDP neighbor.

Command Default

This command displays information about LDP neighbors for the default routing domain if you do not specify the optional **vrf** keyword.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	The command was modified to reflect Multiprotocol Label Switching (MPLS) IETF command syntax and terminology.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP and the **vrf** and **all** keywords were added.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(26)S	This command was modified. The **detail** keyword was updated to display information about inbound filtering.

Release	Modification
12.2(25)S	This command was modified. The graceful-restart keyword was added.
12.3(14)T	This command was modified. The command output was updated so that the **detail** keyword displays information about MPLS LDP Session Protection.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(28)SB	This command was modified. The **detail** keyword was updated to include Message Digest 5 (MD5) password information and the command was 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.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SRE4	The command was modified. The **detail** keyword displays LDP capabilities announce and receive information. The capabilities keyword was added.

Usage Guidelines

The **show mpls ldp neighbor** command can provide information about all LDP neighbors, or the information can be limited to the following:

- Neighbor with specific IP address
- LDP neighbors known to be accessible over a specific interface

Note This command displays information about LDP and Tag Distribution Protocol (TDP) neighbor sessions.

Examples

The following is sample output from the **show mpls ldp neighbor** command:

```
Device# show mpls ldp neighbor

Peer LDP Ident: 10.0.7.7:2; Local LDP Ident 10.1.1.1:1
        TCP connection: 10.0.7.7.11032 - 10.1.1.1.646
        State: Oper; Msgs sent/rcvd: 5855/6371; Downstream on demand
        Up time: 13:15:09
        LDP discovery sources:
          ATM3/0.1
Peer LDP Ident: 10.1.1.1:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.1.1.1.646 - 10.1.1.1.11006
        State: Oper; Msgs sent/rcvd: 4/411; Downstream
        Up time: 00:00:52
        LDP discovery sources:
          Ethernet1/0/0
        Addresses bound to peer LDP Ident:
          10.0.0.29       10.1.1.1        10.0.0.199      10.10.1.1
          10.205.0.9
```

The following is sample output from the **show mpls ldp neighbor** command, in which duplicate addresses are detected. They indicate an error because a given address should be bound to only one peer.

```
Device# show mpls ldp neighbor

Peer LDP Ident: 10.0.7.7:2; Local LDP Ident 10.1.1.1:1
        TCP connection: 10.0.7.7.11032 - 10.1.1.1.646
        State: Oper; Msgs sent/rcvd: 5855/6371; Downstream on demand
        Up time: 13:15:09
        LDP discovery sources:
          ATM3/0.1
Peer LDP Ident: 10.1.1.1:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.1.1.1.646 - 10.1.1.1.11006
        State: Oper; Msgs sent/rcvd: 4/411; Downstream
        Up time: 00:00:52
        LDP discovery sources:
          Ethernet1/0/0
        Addresses bound to peer LDP Ident:
          10.0.0.29 10.1.1.1 10.0.0.199 10.10.1.1
          10.205.0.9
        Duplicate Addresses advertised by peer:
          10.10.8.111
```

The following is sample output from the **show mpls ldp neighbor vrf vpn10** command, which displays the LDP neighbor information for the specified VPN routing and forwarding instance named vpn10:

```
Device# show mpls ldp neighbor vrf vpn10

Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.29.0.2:0
        TCP connection:10.14.14.14.646 - 10.29.0.2.11384
        State:Oper; Msgs sent/rcvd:1423/800; Downstream
        Up time:02:38:11
        LDP discovery sources:
          ATM3/0/0.10
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
```

The following is sample output from the **show mpls ldp neighbor vrf vpn1 detail** command, which displays information about inbound filtering:

```
Device# show mpls ldp neighbor vrf vpn1 detail

 Peer LDP Ident: 10.13.13.13:0; Local LDP Ident 10.33.0.2:0
   TCP connection: 10.13.13.13.646 - 10.33.0.2.31581
   State: Oper; Msgs sent/rcvd: 11/10; Downstream; Last TIB rev sent 13
   Up time: 00:02:25; UID: 26; Peer Id 0;
```

```
   LDP discovery sources:
    Ethernet1/0/2; Src IP addr: 10.33.0.1
     holdtime: 15000 ms, hello interval: 5000 ms
   Addresses bound to peer LDP Ident:
    10.3.105.1       10.13.13.13     10.33.0..1
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
   LDP inbound filtering accept acl:1
 Peer LDP Ident: 10.14.14.14:0; Local LDP Ident 10.33.0.2:0
   TCP connection: 10.14.14.14.646 - 10.33.0.2.31601
   State: Oper; Msgs sent/rcvd: 10/9; Downstream; Last TIB rev sent 13
   Up time: 00:01:17; UID: 29; Peer Id 3;
   LDP discovery sources:
    Ethernet1/0/3; Src IP addr: 10.33.0.1
     holdtime: 15000 ms, hello interval: 5000 ms
   Addresses bound to peer LDP Ident:
    10.3.104.1       10.14.14.14     10.32.0.1
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
   NSR: Not Ready
   Capabilities Sent:
    [ICCP (type 0x0405) MajVer 1 MinVer 0]
    [Dynamic Announcement (0x0506)]
    [mLDP Point-to-Multipoint (0x0508)]
    [mLDP Multipoint-to-Multipoint (0x0509)]
    [Typed Wildcard (0x050B)]
   Capabilities Received:
    [ICCP (type 0x0405) MajVer 1 MinVer 0]
    [Dynamic Announcement (0x0506)]
    [mLDP Point-to-Multipoint (0x0508)]
    [mLDP Multipoint-to-Multipoint (0x0509)]
    [Typed Wildcard (0x050B)]
   LDP inbound filtering accept acl:1
```

The following is sample output from the **show mpls ldp neighbor all** command, which displays the LDP neighbor information for all VPN routing and forwarding instances, including those in the default routing domain. In this example, note that the same neighbor LDP ID (10.14.14.14) appears in all the listed VRF interfaces, highlighting the fact that the same IP address can coexist in different VPN routing and forwarding instances.

```
Device# show mpls ldp neighbor all

Peer TDP Ident:10.11.11.11:0; Local TDP Ident 10.12.12.12:0
        TCP connection:10.11.11.11.711 - 10.12.12.12.11003
        State:Oper; PIEs sent/rcvd:185/187; Downstream
        Up time:02:40:02
        TDP discovery sources:
          ATM1/1/0.1
        Addresses bound to peer TDP Ident:
          10.3.38.3        10.1.0.2        10.11.11.11
VRF vpn1:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.7.0.2:0
        TCP connection:10.14.14.14.646 - 10.7.0.2.11359
        State:Oper; Msgs sent/rcvd:952/801; Downstream
        Up time:02:38:49
        LDP discovery sources:
          ATM3/0/0.1
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
```

```
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn2:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.13.0.2:0
        TCP connection:10.14.14.14.646 - 10.13.0.2.11361
        State:Oper; Msgs sent/rcvd:964/803; Downstream
        Up time:02:38:50
        LDP discovery sources:
          ATM3/0/0.2
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn3:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.15.0.2:0
        TCP connection:10.14.14.14.646 - 10.15.0.2.11364
        State:Oper; Msgs sent/rcvd:1069/800; Downstream
        Up time:02:38:52
        LDP discovery sources:
          ATM3/0/0.3
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.17.0.1       10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn4:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.17.0.2:0
        TCP connection:10.14.14.14.646 - 10.17.0.2.11366
        State:Oper; Msgs sent/rcvd:1199/802; Downstream
```

The following is sample output from the **show mpls ldp neighbor graceful-restart** command, which shows the Graceful Restart status of the LDP neighbors:

```
Device# show mpls ldp neighbor graceful-restart

Peer LDP Ident: 10.20.20.20:0; Local LDP Ident 10.17.17.17:0
   TCP connection: 10.20.20.20.16510 - 10.17.17.17.646
```

```
    State: Oper; Msgs sent/rcvd: 8/18; Downstream
    Up time: 00:04:39
    Graceful Restart enabled; Peer reconnect time (msecs): 120000
Peer LDP Ident: 10.19.19.19:0; Local LDP Ident 10.17.17.17:0
    TCP connection: 10.19.19.19.11007 - 10.17.17.17.646
    State: Oper; Msgs sent/rcvd: 8/38; Downstream
    Up time: 00:04:30
    Graceful Restart enabled; Peer reconnect time (msecs): 120000
```

The following sample output from the **show mpls ldp neighbor detail** command, which displays information about the MD5 password configuration:

```
Device# show mpls ldp neighbor detail

    Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 167/167; Downstream; Last TIB rev sent 9
        Up time: 02:24:02; UID: 5; Peer Id 3;
        LDP discovery sources:
          Targeted Hello 10.1.1.1 -> 10.3.3.3, passive;
            holdtime: 90000 ms, hello interval: 10000 ms
        Addresses bound to peer LDP Ident:
          10.3.3.3         10.0.30.3
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 9/9; Downstream; Last TIB rev sent 9
        Up time: 00:05:35; UID: 6; Peer Id 1;
        LDP discovery sources:
          Ethernet1/0; Src IP addr: 10.0.20.4
            holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
          10.0.40.4       10.4.4.4         10.0.20.4
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
```

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

Table 144: show mpls ldp neighbor Field Descriptions

Field	Description
Peer LDP Ident	LDP (or TDP) identifier of the neighbor (peer) for this session.
Local LDP Ident	LDP (or TDP) identifier for the local label switch router (LSR) for this session.
TCP connection	TCP connection used to support the LDP session, shown in the following format: • peer IP address.peer port • local IP address.local port

Field	Description
Password	Indicates if password protection is being used. Password status is as follows: • Required or not required—Indicates whether password configuration is required. • Neighbor, none, option #, or fallback—Indicates the password source when the password was configured. • In use (current) or stale (previous)—Indicates the current LDP session password usage status.
State	State of the LDP session. Generally, this is Oper (operational), but transient is another possible state.
Msgs sent/rcvd	Number of LDP messages sent to and received from the session peer. The count includes the transmission and receipt of periodic keepalive messages, which are required for maintenance of the LDP session.
Downstream on demand	Indicates that the Downstream on Demand method of label distribution is being used for this LDP session. When the Downstream on Demand method is used, an LSR advertises its locally assigned (incoming) labels to its LDP peer only when the peer requests them.
Downstream	Indicates that the downstream method of label distribution is being used for this LDP session. When the downstream method is used, an LSR advertises all of its locally assigned (incoming) labels to its LDP peer (subject to any configured access list restrictions).
Up time	Length of time (in hours, minutes, seconds) the LDP session has existed.
Graceful Restart enabled	Indicates whether the LDP session has Graceful Restart enabled.
Peer reconnect time	The length of time, in milliseconds (ms), the peer device waits for a device to reconnect.
LDP discovery sources	Sources of LDP discovery activity that led to the establishment of this LDP session.
Targeted Hello	Lists the platforms to which targeted hello messages are being sent: • The active field indicates that this LSR has initiated targeted hello messages. • The passive field indicates that the neighbor LSR has initiated targeted hello messages and that this LSR is configured to respond to the targeted hello messages from the neighbor.
holdtime	Period of time, in milliseconds (ms), a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor.
hello interval	Period of time, in milliseconds (ms), between the sending of consecutive hello messages.

Field	Description
Addresses bound to peer LDP Ident	Known interface addresses of the LDP session peer. These are addresses that might appear as “next hop” addresses in the local routing table. They are used to maintain the Label Forwarding Information Base (LFIB).
Duplicate Addresses advertised by peer	IP addresses that are bound to another peer. They indicate an error because a given address should be bound to only one peer.
Peer holdtime	The time, in milliseconds (ms), that the neighbor session is retained without the receipt of an LDP message from the neighbor.
KA Interval	Keepalive interval. The amount of time, in milliseconds (ms), that a device lets pass without sending an LDP message to its neighbor. If this time elapses and the device has nothing to send, it sends a keepalive message.
Peer state	State of the peer; estab means established.
LDP inbound filtering accept acl:1	Access list that is permitted for inbound label-binding filtering.

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp neighbor password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp neighbor password option	Configures an MD5 password for LDP sessions with neighbors whose LDP device IDs are permitted by a specified access list.
mpls ldp neighbor password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp neighbor password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.

show mpls ldp neighbor password

To display password information used in established Label Distribution Protocol (LDP) sessions, use the **show mpls ldp neighbor password** command in user EXEC mode or privileged EXEC mode.

show mpls ldp neighbor [**vrf** *vrf-name*] [{*ip-addressinterface*}] **password** [{**pending** | **current**}] [**all**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the LDP neighbors for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.
ip-address	(Optional) Identifies the neighbor that has this IP address.
interface	(Optional) Identifies the LDP neighbors accessible over this interface.
pending	(Optional) Displays LDP sessions whose password is different from that in the current configuration.
current	(Optional) Displays LDP sessions whose password is the same as that in the current configuration.
all	(Optional) When the **all** keyword is specified alone in this command, the command displays LDP password information for all neighbors in all VPNs, including those in the global routing table.

Command Default

If you do not specify an optional keyword for this command, password information for all established LDP sessions is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to display password information for established LDP sessions. If you do not specify an option, password information for all established LDP sessions is displayed. To display LDP sessions whose password is the same as that in the current configuration, use the **current** keyword with the command. To display LDP sessions whose password is different from that in the current configuration, use the **pending** keyword with the command.

Examples

The following is sample output from the **show mpls ldp neighbor password** command, which displays information for all established LDP sessions:

```
Router# show mpls ldp neighbor password
    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.10.01.10.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 57/57
    Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 216/215
```

The following is sample output from the **show mpls ldp neighbor password pending** command, which displays information for LDP sessions whose passwords are different from those in the current configuration:

```
Router# show mpls ldp neighbor password pending
    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 57/57
```

The following is sample output from the **show mpls ldp neighbor password current** command, which displays information for LDP sessions whose passwords are the same as those in the current configuration:

```
Router# show mpls ldp neighbor password current
    Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 216/215
```

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

Table 145: show mpls ldp neighbor password Field Descriptions

Field	Description
Peer LDP Ident	LDP identifier of the neighbor (peer) for this session.
Local LDP Ident	LDP identifier for the local label switch router (LSR) for this session.
TCP connection	TCP connection used to support the LDP session, shown in the following format: • peer IP address.peer port • local IP address.local port
Password	Indicates the password source and status. • Required or not required indicates whether password configuration is required or not. • Neighbor, none, option #, or fallback indicates the password source when the password was configured. None indicates that no password was configured. • In use (current) or stale (previous) is the usage status of the current LDP session password.

Field	Description
State	State of the LDP session. Generally this is Oper (operational), but transient is another possible state.
Msgs sent/rcvd	Numbers of LDP messages sent to and received from the session peer. The count includes the transmission and receipt of periodic keepalive messages, which are required for maintaining the LDP session.

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.

show mpls ldp parameters

To display current Label Distribution Protocol (LDP) parameters, use the **show mpls ldp parameters** command in user EXEC or privileged EXEC mode.

show mpls ldp parameters

Syntax Description

This command has no arguments or keywords.

Command Default

This command displays LDP parameters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST. The command was modified to reflect Multiprotocol Label Switching (MPLS) IETF command syntax and terminology.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
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 ldp parameters** command:

```
Device# show mpls ldp parameters

Protocol version: 1
Downstream label pool: min label 16; max label 100000
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 180 sec; interval: 5 sec
LDP for targeted sessions; peer acl: 1
LDP initial/maximum backoff: 30/240 sec
Device#
```

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

Table 146: show mpls ldp parameters Field Descriptions

Field	Description
Protocol version	Indicates LDP version running on the platform.
Downstream label pool	Describes the range of labels available to the platform to assign for label-switching purposes. The available labels range from the smallest label value (min label) to the largest label value (max label), with a modest number of labels at the low end of the range (reserved labels) reserved for diagnostic purposes.
Session hold time	Indicates the time (in seconds) to maintain an LDP session with an LDP peer without receiving LDP traffic or an LDP keepalive message from the peer.
keep alive interval	Indicates time (in seconds) between consecutive transmission of LDP keepalive messages to an LDP peer.
Discovery hello	Indicates time (in seconds) that a neighbor platform continues an LDP session without receiving an LDP hello message from the neighbor (hold time), and the seconds between the transmission of consecutive LDP hello messages to neighbors (interval).
Discovery targeted hello	Indicates the time a neighbor platform continues an LDP session when: **1.** The neighbor platform is not directly connected to the device. **2.** The neighbor platform has not sent an LDP hello message. This intervening interval is known as hold time. This field also indicates the time interval between the transmission of consecutive hello messages to a neighbor not directly connected to the device.
LDP for targeted sessions	Reports the parameters that have been set by the **show mpls atm-ldp bindings** command.
LDP initial/maximum backoff	Reports the parameters that have been set by the **mpls ldp backoff** command.

Related Commands

Command	Description
mpls ldp holdtime	Changes the time that an LDP session is maintained in the absence of LDP messages from the session peer.

show mpls memory

To display information about the Multiprotocol Label Switching (MPLS) Label Distribution Protocol memory usage, use the **show mpls memory** command in user EXEC or privileged EXEC mode.

show mpls memory [**all**] [{**component** *string* | **detailed**}]

Syntax Description

all	(Optional) Specifies all the related memory of other modules.
component *string*	(Optional) Specifies the sorted output based on component names.
detailed	(Optional) Specifies the details about the memory usage.

Command Modes

User EXEC(>)
Privileged EXEC(#)

Command History

Release	Modification
12.4(22)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show mpls memory** command:

```
Router: show mpls memory
  Allocator-Name                  In-use/Allocated            Count
  ------------------------------------------------------------------------------
  LFD: AToM pwid             :          0/67232      (  0%) [      0] Chunk
  LFD: FPI LBL               :        144/22424      (  0%) [      4] Chunk
  LFD: LTE                   :        192/35704      (  0%) [      4] Chunk
  LFD: MOI DEAG              :         96/22704      (  0%) [      3] Chunk
  LFD: MOI DROP              :         20/24208      (  0%) [      1] Chunk
  LFD: RW NONE               :        160/36248      (  0%) [      4] Chunk
  LSD: FPI FRR               :      22312/22424      ( 99%) [      2]
  LSD: FPI LBL               :      22312/22424      ( 99%) [      2]
  LSD: MOI DEAG              :      23424/23536      ( 99%) [      2]
  LSD: MOI DROP              :      13424/13536      ( 99%) [      2]
  LSD: RW NONE               :      36136/36248      ( 99%) [      2]
  LSD: intf                  :      33512/33624      ( 99%) [      2]
  LSD: label tbl             :      22704/35952      ( 63%) [    516] Chunk
  LSD: label tbl             :         64/1800       (  3%) [      1] Chunk
  MFI: Clnt CMsg             :          0/65592      (  0%) [      0] Chunk
  MFI: Clnt SMsg             :      71200/131184     ( 54%) [      4] Chunk
  MFI: InfoReq               :          0/808        (  0%) [      0] Chunk
  MFI: InfoRply              :          0/65592      (  0%) [      0] Chunk
  Total allocated: 0.629 Mb, 645 Kb, 661240 bytes
```

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

Table 147: show mpls memory Field Descriptions

Field	Description
Allocator-Name	The specific name of the allocator.
In-use/Allocated	The details of usage of the allocators.
Count	The number of allocators used.

Related Commands

Command	Description
debug mpls ldp igp sync	Displays events related to MPLS LDP-IGP synchronization.
mpls ldp igp sync	Enables MPLS LDP-IGP synchronization on an interface that belongs to an OSPF process.
mpls ldp igp sync holddown	Specifies how long an IGP should wait for LDP synchronization to be achieved.
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process or an IS-IS process.

show mpls oam echo statistics through switching tlv

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 148: 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* | **stats** [**reset**] | **vpls** *vlan-id* | **vpn**}

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.
stats	Displays information about the RP-control plane statistics.
reset	(Optional) Resets the statistics counters.
vpls *vlan-id*	Displays Virtual Private LAN Services (VPLS)-related information; valid values are from 1 to 4095.
vpn	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 on 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:

```
Device# 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
```

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

```
Device# show mpls platform eompls

Interface        VLAN
GigabitEthernet  101
FastEthernet6/1  2022
```

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

```
Device# show mpls platform gbte-tunnels

To            From          InLbl   I/I/F kbps     Kbits    H/W Info
```

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

```
Device# 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:

```
Device# show mpls platform stats

              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
```

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

```
Device# show mpls platform stats 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
```

This example shows how to display information about a VPLS instance:

```
Device# show mpls platform vpls 100

----------------------------
VPLS VLAN 100 (BD 100):
VC info (#spoke VCs 0) :
Imp: tcam 224 (68 ) adj 131076 (0x20004) [peer 1.1.1.1 ID vc_id 100 2:1] stats 0/0 0/0
Disp: tcam 324 (66 ) adj 114692 (0x1C004) [in_label 16] stats 6/448
------------------------------
BD Flood Manager: VLAN/BD 100, 1 peers
CMET handle 0x6 top 6 (0x6) bottom 6 (0x6)
Ingr flood: tcam 64/0x40 (sw 15) adj 196608 (0x30000) elif 0x701C0064 stats 0/0
Egr flood: tcam 65/0x41 (sw 72) adj 32868 (0x8064) elif 0x20000064 stats 1/94
Ingr local: tcam 32/0x20 (sw 13) adj 180224 (0x2C000) elif 0x20000064 stats 0/0
Egr local: tcam 33/0x21 (sw 14) adj 180225 (0x2C001) elif 0x20000064 stats 0/0
BD Flood Manager: 1 BDs, LTL base 0x90E, LTL clients: VPLS
: Wildcard entry tcam 288 (12) adj 78089 (0x13109)
```

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

```
Device# show mpls platform vpn

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
```

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 149: 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-lengthmask*}}][{**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 150: 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.
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 151: show mpls tp link-management admission-control failures Field Descriptions

Field	Description
Tun Num	Tunnel number.
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.

Field	Description
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 152: 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.
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.

Field	Description
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 153: 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 154: 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.
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.

Field	Description
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 155: show mpls traffic-eng auto-tunnel mesh Field Descriptions

Field	Description
Auto-Template1	Name of the autotemplate.
Destination	Destination addresses for the mesh tunnel interface cloned from access list 1.
Interface	Mesh tunnel interfaces cloned from access list 1.

Field	Description
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 156: 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 157: 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 primary 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 primary 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.
tunnel mpls traffic-eng exp-bundle master	Configures the primary tunnel.
tunnel mpls traffic-eng exp-bundle member	Identifies which tunnel is a member (bundled tunnel) of the primary 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

Sample Output for Cisco IOS Releases 12.0S and 12.2S

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 158: show mpls traffic-eng fast-reroute database Field Descriptions

Field	Description
Prefix	Address to which packets with this label are going.

Field	Description
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.
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 159: 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.

Field	Description
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.
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
```

MPLS Traffic Engineering Point-to-Multipoint Fast Reroute Information

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 160: 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 161: 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.
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.

Field	Description
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 feature-control

To display a list of the Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) features that are supported on a specific platform or image, use the **show mpls traffic-eng feature-control** command in privileged EXEC mode.

show mpls traffic-eng feature-control

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.12S	This command was introduced in a release earlier than Cisco IOS XE Release 3.12S.

Usage Guidelines

The **show mpls traffic-eng feature-control** command provides visibility to the MPLS TE feature control support.

Examples

The following is sample output from the **show mpls traffic-eng feature-control** command. The field descriptions are self-explanatory.

```
Device# show mpls traffic-eng feature-control

MPLS-TE Feature                                              Configurable
---------------                                              ------------
Basic Feature Set                                            yes
Auto-Bandwidth                                               yes
Auto-Bandwidth Enhancements                                  yes
Auto-Tunnel Meshgroups                                       yes
Auto-Route Destination                                       yes
Auto-Tunnel Primary and Backup                               yes
Class-Based Tunnel Selection (CBTS)                          yes
IETF Diff-Serv Aware TE (DSTE)                               yes
Fast-Reroute: Link, Node and Bandwidth Protection            yes
Fast-Reroute Integration over ATM                            yes
Fast-Reroute Node Protection Desired                         yes
Fast-Reroute Triggered by BFD                                yes
RSVP Graceful Restart Help Neighbor                          yes
TE Support over Etherchannel Interface                       yes
TE Support over Multilink Interface                          yes
Inter-AS TE                                                  yes
LSP Attributes and Bandwidth Override                        yes
MPLS Transport Profile (MPLS-TP)                             yes
MPLS Transport Profile (MPLS-TP) Bandwidth Manager           yes
MPLS Transport Profile (MPLS-TP) support on BDI interfaces   yes
MPLS Transport Profile (MPLS-TP) support on ethernet subinteyes
MPLS Transport Profile (MPLS-TP) support on SVI interfaces   yes
MPLS Transport Profile (MPLS-TP) Non-IP                      yes
TE Point-to-Multipoint (P2MP)                                yes
Path-option Protect                                          yes
Path-option Protect Enhancements                             yes
Shared Risk Link Group (SRLG)                                yes
Stateful Switchover (SSO)                                    yes
```

```
TE Fast Tunnel Interface Down                                   yes
Verbatim LSPs                                                   yes
```

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.

Command	Description
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 162: 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 163: 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 164: 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.

Field	Description
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 165: 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 166: 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

Interface Example

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 167: 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.
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.

Field	Description
BW TOTAL LOCKED	Bandwidth locked at this priority and those above it.

Summary Example for Regular TE (or Russian Dolls Model [RDM] DiffServ-Aware TE) with Multiple Interfaces

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 168: 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.

Summary Example for Regular TE (or Russian Dolls Model [RDM] DiffServ-Aware (DS) TE) with a Single Interface

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.

Summary Example with a Specified Interface for Maximum Allocation Model (MAM) DS-TE

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 169: 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 170: 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 171: 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.
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 172: 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.
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 173: 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 174: 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

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.

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 175: 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.

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 176: 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.

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 177: 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).

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 178: 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 179: 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.

Release	Modification
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 180: 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.
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.
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 181: 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.
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 182: 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 183: 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.
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.

Field	Description
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 (TE) tunnels, use the **show mpls traffic-eng tunnels statistics** command in user EXEC or 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.
Cisco IOS XE Release 3.12S	This command was modified. The output was updated to display reoptimization statistics 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:

```
Device# 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


Device# 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

...


Device# 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 reoptimization statistics information under label switched path (LSP) activations. The text ‘No better/reopt path that satisfies tunnel constraints’ indicates a scenario in which an attempt to reoptimize the tunnel and check for the availability of a better path is performed. If there is no better path, there will be no new activation.

```
Device# show mpls traffic-eng tunnels statistics
```

```
Tunnel0 (Destination 10.4.0.1;Name p2mp-1_t0)
  Management statistics:
    Path:   6 no path, 0 path no longer valid, 0 missing ip exp path
            1 path changes, 8 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: 1 succeeded
        Last Failure: No path that satisfy tunnel constraints
        Failures stats:
          6: No path that satisfy tunnel constraints
        Reoptimization stats:
          1: No better/reopt path that satisfies tunnel constraints
    Errors: 0 no b/w, 0 no route, 0 admin, 0 remerge detected
            0 bad exp route, 0 rec route loop, 0 frr activated
            0 bad label, 0 other
```

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

```
Device# 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 184: 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.

Field	Description
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 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 185: 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.)
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.

Field	Description
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.
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 hardware pp active feature mpls mtu-table

To display the MPLS MTU on the router, use the **show platform hardware pp active feature mpls mtu-table** command in privileged EXEC mode.

show platform hardware pp active feature mpls mtu-table

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.10.2S	This command was introduced on the Cisco ASR 900 Series Router.

Usage Guidelines

Use the **show platform hardware pp active active feature mpls mtu-table** command to view the MPLS MTU configured values.

Examples

The following is sample output from the **show platform hardware pp active feature mpls mtu-table** command:

```
Router# show platform hardware pp active feature mpls mtu-table

MPLS MTU Table

Index    MTU  Ref-Count
------------------------
0        1504  1
1         704  0
2           0  0
3           0  0
4           0  0
5           0  0
6           0  0
7           0  0
```

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

Table 186: show platform hardware pp active feature mpls mtu-table Field Descriptions

Field	Description
MTU	Configured MTU values.
Ref-Count	Displays the counters.

Related Commands

Command	Description
platform mpls mtu-enable	Enables MPLS MTU configuration on the router.

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.

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 187: 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.

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 188: 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.
Cisco IOS XE Release 3.8S	This command was modified. The *pseudowire* interface type was added on Cisco 1000 Series Routers.

Release	Modification
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.

Weighted Fair Queueing (WFQ) on Serial Interface: Example

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
```

Traffic Shaping on Serial Interface: Example

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 189: show policy-map interface Field Descriptions

Field	Description
Fields Associated with Classes or Service Policies	

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. **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.	

Field	Description
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)	
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.

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.
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.

Precedence-Based Aggregate WRED on ATM Shared Port Adapter: Example

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
```

DSCP-Based Aggregate WRED on ATM Shared Port Adapter: Example

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 190: 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.

Field	Description
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 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.

Frame Relay Voice-Adaptive Traffic-Shaping: Example

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 191: 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.

Two-Rate Traffic Policing: Example

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 192: 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.
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.

Multiple Traffic Policing Actions: Example

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 193: 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.

Explicit Congestion Notification: Example

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 194: 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.

Field	Description
Minimum threshold	Minimum WRED threshold in number of packets.
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.

Class-Based RTP and TCP Header Compression: Example

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 195: 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.
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.

Modular QoS CLI (MQC) Unconditional Packet Discard: Example

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 196: 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.
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
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.

Percentage-Based Policing and Shaping: Example

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 197: 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.
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.

Traffic Shaping: Example

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 198: 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.

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 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.

Field	Description
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.
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.

Packet Classification Based on Layer 3 Packet Length: Example

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 199: 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.

Enhanced Packet Marking: Example

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 200: 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.

Traffic Policing: Example

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.

Formula for Calculating the CIR: Example

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

Formula for Calculating the PIR: Example

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.

Formula for Calculating the Committed Burst (bc): Example

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

Formula for Calculating the Excess Burst (be): Example

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 201: 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.

Bandwidth Estimation: Example

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
```

Shaping with HQF Enabled: Example

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
```

Packets Matched on the Basis of VLAN ID Number: Example

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 202: 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* .

Cisco 7600 Series Routers: Example

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
policed-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
policed-dscp-transmit
```

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

Table 203: 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.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.

Field	Description
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.

Cisco 7200 Series Routers: Example

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
```

Multiple Priority Queues on Serial Interface: Example

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
```

Bandwidth-Remaining Ratios: Example

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 204: 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.

Tunnel Marking: Example

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 205: 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.

Traffic Shaping Overhead Accounting for ATM: Example

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 206: 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.

HQF: Example

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

Field	Description
FastEthernet	Name of the interface.

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. **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.
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.

Account QoS Statistics for the Cisco ASR 1000 Series Aggregation Services Routers: Example

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
```

Cisco Catalyst 4000 Series Routers: Example

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
```

Cisco CMTS Routers: Example

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 208: 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.
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.

Displaying Pseudowire Policy Map Information: Example

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 209: 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.
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.

Command	Description
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 210: 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 211: 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.
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.

Field	Description
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 212: 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.
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.

Field	Description
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.
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 sdm prefer current

Use the **show sdm prefer current** privileged EXEC command to display the current Switch Database Management (SDM) template configured on the device.

show sdm prefer current

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.10S	This command was implemented on Cisco ASR 900 Series Aggregation Services Routers.

Usage Guidelines

If you did not reload the device after entering the **sdm prefer** global configuration command, the **show sdm prefer current** privileged EXEC command displays the template currently in use and not the newly configured template.

Examples

The following is sample output from the **sdm prefer current** command displaying the template currently in use.

```
Device# show sdm prefer current

The current template is "video" template.
```

Related Commands

Command	Description
sdm prefer	Configures the template used in SDM resource allocation.

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 primary 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 213: 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.
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*.
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 214: 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 215: 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 216: 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 217: show vfi memory detail Field Descriptions

Field	Description
VFI memory	Amount of memory available for use.
In-use	Amount of memory actively used.

Field	Description
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.
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.

Release	Modification
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 218: 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 219: 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
```

Sample Output for All Xconnect Attachment Circuits and Pseudowires on a Cisco uBR10012 Router in the Brief Display Format

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
```

Sample Output for All Xconnect Attachment Circuits and Pseudowires on a Cisco uBR10012 Router in the Brief Display Format in Cisco IOS Release 12.2(33)SCF

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
```

Sample Output for All Xconnect Attachment Circuits and Pseudowires on a Cisco uBR10012 Router in the Detailed Display Format

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:
```

Sample Output for All Xconnect Attachment Circuits and Pseudowires on a Cisco uBR10012 Router in the Detailed Display Format in Cisco IOS Release 12.2(33)SCF

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 220: 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.

Field	Description
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.

VPLS Autodiscovery Feature Example

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 221: 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 222: 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.

L2VPN VPLS Inter-AS Option B 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 223: 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.

Field	Description
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 224: 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.

Field	Description
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.
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 225: 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.

Field	Description
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.
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 226: 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 227: 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 228: show xtagatm cross-connect Field Descriptions

Field	Description
Phys desc	Physical descriptor. A switch-supplied string identifying the interface on which the endpoint exists.
VPI/VCI	Virtual path identifier and virtual channel identifier for this endpoint.
Type	The type can be one of the following: A right arrow (->) indicates an ingress endpoint, where traffic is received into the switch. A left arrow (<-) indicates an egress endpoint, where traffic is transmitted from the interface. A bidirectional arrow (<->) indicates that traffic is both transmitted and received at this endpoint.
X-Phys Desc	Physical descriptor for the interface of the other endpoint belonging to the cross-connect.
X-VPI/VCI	Virtual path identifier and virtual channel identifier of the other endpoint belonging to the cross-connect.
State	Indicates the status of the cross-connect to which this endpoint belongs. The state is typically UP; other values, all of which are transient, include the following: • 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 229: show xtagatm cross-connect descriptor Field Descriptions

Field	Description
Phys desc	Physical descriptor. A switch-supplied string identifying the interface on which the endpoint exists.
Interface	The (Cisco IOS) interface name.
Intf type	Interface type. Can be either extended Multiprotocol Label Switched (MPLS) ATM (XTagATM) or a switch control port.
VPI/VCI	Virtual path identifier and virtual channel identifier for this endpoint.
X-Phys desc	Physical descriptor for the interface of the other endpoint belonging to the cross-connect.
X-Interface	The (Cisco IOS) name for the interface of the other endpoint belonging to the cross-connect.
X-Intf type	Interface type for the interface of the other endpoint belonging to the cross-connect.
X-VPI/VCI	Virtual path identifier and virtual channel identifier of the other endpoint belonging to the cross-connect.

Field	Description
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
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 230: 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-numberextended-access-list-numberaccess-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.

Release	Modification
12.0(17)S	This command was integrated into Cisco IOS Release 12.0(17)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The access list values were enhanced to support the expanded range of standard access list values and to support named standard access lists.
12.0(27)S	The **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.
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 2001:DB8:0:12::/64 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.

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.
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.

Release	Modification
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.

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-numberacl-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.

Release	Modification
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

Create an SNMP Group

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
```

Remove an SNMP Server Group

The following example shows how to remove the SNMP server group "public" from the configuration:

```
Router(config)# no snmp-server group public v2c
```

Associate an SNMP Server Group with Specified Views

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 {*hostnameip-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 {*hostnameip-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.
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.

Release	Modification
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.
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.

Release	Modification
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
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 commands 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) 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 231: 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 [2]	**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**]

[2] 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.
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 Guidelines

⚠

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 primary one 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 the subordinate, use the **no** form of this command.

status redundancy master
no status redundancy master

Syntax Description

master	Designates a pseudowire to work as the primary.

Command Default

The pseudowire is in the subordinate or secondary 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 primary one and the other must be the subordinate. You cannot configure both pseudowires as the primary or the subordinate.

Examples

The following example shows how to designate the pseudowire as the primary 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 primary 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 primary one 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.

T through X

terminating-pe tie-breaker

To negotiate the behavior mode (either active or passive) for a terminating provider edge (TPE) router, use the **terminating-pe tie-breaker** command in Layer 2 pseudowire routing configuration mode. To remove the TPE tie breaker identification, use the **no** form of this command.

terminating-pe tie-breaker
no terminating-pe tie-breaker

Syntax Description

This command has no arguments or keywords.

Command Default

A behavior mode is not specified for the TPE.

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 **terminating-pe tie-breaker** command is used in Layer 2 pseudowire routing configuration mode. To enter Layer 2 pseudowire routing configuration mode, use the **l2 pseudowire routing** command.

Active and Passive PEs in an L2VPN VPLS Inter-AS Option B Configuration

A TPE terminates a multisegment pseudowire. By default, the TPEs on both ends of a multisegmented pseudowire are in active mode. The L2VPN VPLS Inter-AS Option B feature requires that one of the TPEs be in passive mode. The system determines which PE is the passive TPE based on a comparison of the Target Attachment Individual Identifier (TAII) received from Border Gateway Protocol (BGP) and the Source Attachment Individual Identifier (SAII) of the local router. The TPE with the numerically higher identifier assumes the active role.

When you are configuring the PEs for the L2VPN VPLS Inter-AS Option B feature, use the **terminating-pe tie-breaker** command to negotiate the mode of the TPE. Then use the **mpls ldp discovery targeted-hello accept** command to ensure that a passive TPE can accept Label Distribution Protocol (LDP) sessions from the LDP peers.

Examples

In the following example, the **terminating-pe** command has been used to configure the TPE to negotiate an active or passive role:

```
Router>enable
Router#  configure terminal
Router(config)# l2 pseudowire routing
Router(config-l2_pw_rtg)# terminating-pe tie-breaker
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.
mpls ldp discovery	Configures the interval between transmission of consecutive LDP discovery hello messages, or the hold time for a discovered LDP neighbor, or the neighbors from which requests for targeted hello messages may be honored.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

tlv

To use the pseudowire type-length-value (TLV) parameters, use the **tlv** command, in virtual forwarding interface (VFI) neighbor interface configuration mode or pseudowire TLV template configuration mode. To remove the TLV parameters, use the **no** form of this command.

tlv *[type-name] type-value length* [{**dec** | **hexstr** | **str**}] *value*
no tlv *[type-name] type-value length* [{**dec** | **hexstr** | **str**}] *value*

Syntax Description

type-name	The name of the TLV.
type-value	A number designating the type of TLV. Valid values are from 1 to 40.
length	The TLV length. Valid values are from 1 to 255.
dec	The TLV value in decimal.
hexstr	The TLV value in hex string.
str	The TLV value in string.
value	The TLV value.

Command Default

No defaults.

Command Modes

VFI neighbor interface configuration (config-vfi-neighbor-interface)

Pseudowire template configuration (config-pw-tlv-template)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Examples

The following example specifies TLV values:

```
l2 vfi atom point-to-point  (static-dynamic MSPW)

neighbor 116.116.116.116 4294967295 pw-class dypw     (dynamic)

neighbor 111.111.111.111 123 pw-class stpw            (static)

  mpls label 101 201

  mpls control-word

   local interface 4

     tlv mtu 1 4  1500

     tlv descr 3 6 str abcd
```

```
tlv descr C 4 hexstr 0505
```

Related Commands

Command	Description
pseudowire tlv-template	Creates a template of TLV parameters to use in an MPLS-TP configuration.

tlv template

To use the pseudowire type-length-value (TLV) parameters created with the **pseudowire-tlv template** or the **l2vpn pseudowire tlv template** command, use the **tlv template** command in the appropriate configuration mode. To remove the template, use the **no** form of this command.

tlv template *template-name*
no tlv template *template-name*

Syntax Description

template-name	Name for the TLV template.

Command Default

TLV values are not specified.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

VFI neighbor interface configuration (config-vfi-neighbor-interface)

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 Layer 2 VPN (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 create a TLV template named net:

```
Device(config-vfi-neighbor-interface)# tlv template net
```

The following example shows how to apply a TLV template named tlv3:

```
Device(config)# interface pseudowire 100
Device(config-if)# tlv template tlv3
```

The following example shows how to apply a TLV template named tlv3 in pseudowire class configuration mode:

```
Device(config)# pseudowire-class bfdclass
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# tlv template tlv3
```

The following example shows how to apply a TLV template named tlv3 in template configuration mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# tlv template tlv3
```

Related Commands

Command	Description
l2vpn pseudowire tlv template	Creates a template of pseudowire TLV parameters to be used in a MPLS-TP configuration.

tag-control-protocol vsi

Note Effective with Cisco IOS Release 12.4(20)T, the **tag-control-protocol vsi** command is not available in Cisco IOS software.

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

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

Syntax Description

base-vc *vpi vci*	(Optional) Determines the VPI/VCI value for the channel to the first subordinate. The default is 0/40. Together with the subordinate value, this value determines the VPI/VCI values for the channels to all of the subordinates, which are as follows: • *vpi/vci* • *vpi/vci*+ 1, and so on • *vpi/vci*+*slave-count*- 1
delay *seconds*	(Optional) Specifies the delay time to start a new VSI session after the system comes up or after you enter the command. If a VSI session is already running, the delay keyword has no effect for the current session. The delay is implemented when a new VSI session starts. The default is 0. The valid range of values is 0 to 300.
id *controller-id*	(Optional) Determines the value of the controller-id field present in the header of each VSI message. The default is 1.
keepalive *timeout*	(Optional) Determines the value of the keepalive timer (in seconds). Make sure that the keepalive timer value is greater than the value of the retry timer> times the retry timer> + 1. The default is 15 seconds.

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

Command Default

VSI is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(15)T	The delay keyword was added.
12.3(2)T	The **nak** keyword was added.
12.4(20)T	This command was removed.

Usage Guidelines

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

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

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

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

Examples

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

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

The following example enables extended NAK support:

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

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

```
Router# show running-config interface atm0/0
Building configuration...
Current configuration : 113 bytes
interface ATM0/0
 no ip address
 shutdown
 label-control-protocol vsi nak extended
 no atm ilmi-keepalive
end
```

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

```
Router# show controllers vsi session
Interface    Session  VCD    VPI/VCI    Switch/Slave Ids   Session State
ATM0/0       0        1      0/40       0/0                UNKNOWN
ATM0/0       1        2      0/41       0/0                UNKNOWN
ATM0/0       2        3      0/42       0/0                UNKNOWN
ATM0/0       3        4      0/43       0/0                UNKNOWN
ATM0/0       4        5      0/44       0/0                UNKNOWN
ATM0/0       5        6      0/45       0/0                UNKNOWN
ATM0/0       6        7      0/46       0/0                UNKNOWN
ATM0/0       7        8      0/47       0/0                UNKNOWN
ATM0/0       8        9      0/48       0/0                UNKNOWN
ATM0/0       9        10     0/49       0/0                UNKNOWN
ATM0/0       10       11     0/50       0/0                UNKNOWN
ATM0/0       11       12     0/51       0/0                UNKNOWN
ATM0/0       12       13     0/52       0/0                UNKNOWN
ATM0/0       13       14     0/53       0/0                UNKNOWN
Extended NAK support is enabled on LSC
```

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

Table 232: show controllers vsi session Field Descriptions

Field	Description
Interface	Control interface name.
Session	Session number (from 0 to <*n* -1>), where *n* is the number of sessions on the control interface.
VCD	Virtual circuit descriptor (virtual circuit number). Identifies the VC carrying the VSI protocol between the primary and the subordinate for this session.
VPI/VCI	Virtual path identifier or virtual channel identifier (for the VC used for this session).
Switch/Slave Ids	Switch and subordinate identifiers supplied by the switch.
Session State	Indicates the status of the session between the primary and the subordinate. • ESTABLISHED is the fully operational steady state. • UNKNOWN indicates that the subordinate is not responding. Other possible states include the following: • CONFIGURING • RESYNC-STARTING • RESYNC-UNDERWAY • RESYNC-ENDING • DISCOVERY • SHUTDOWN-STARTING • SHUTDOWN-ENDING • INACTIVE

traceroute mpls

To discover Multiprotocol Label Switching (MPLS) label switched path (LSP) routes that packets actually take when traveling to their destinations, use the **traceroute mpls** command in privileged EXEC mode.

traceroute mpls {**ipv4** *destination-address/destination-mask-length* | **traffic-eng Tunnel** *tunnel-number tunnel-number* | **pseudowire** *destination-address vc-id* **segment** *segment-number*[{*segment-number*}] | **tp**}[{**timeout** *seconds*}][{**destination** *address-start*[{*address-endincrement*}]}][{**revision**{**1** | **2** | **3** | **4**}}][{**source** *source-address*}][{**exp** *exp-bits*}][{**ttl** *maximum-time-to-live*}][{**reply**{**dscp** *dscp-bits* | **mode** *reply-mode*{**ipv4** | **no-reply** | **router-alert**} | **pad-tlv**}}][{**force-explicit-null** }][{**output interface** *tx-interface*[{**nexthop** *ip-address*}]}][{**flags fec**}][{**revision** *tlv-revision-number*}]

Syntax Description

ipv4	Specifies the destination type as a Label Distribution Protocol (LDP) IPv4 address.
destination-address	Address prefix of the target to be tested.
/ *destination-mask-length*	Number of bits in the network mask of the target address. The slash is required.
traffic-eng Tunnel *tunnel-number*	Specifies the destination type as an MPLS traffic engineering (TE) tunnel.
pseudowire	Specifies the destination type as an Any Transport over MPLS (AToM) virtual circuit (VC).
tp	Verifies MPLS-TP connectivity by displaying TP tunnel identifiers throughout the path.
ipv4-address	IPv4 address of the AToM VC to be tested.
vc-id	Specifies the VC identifier of the AToM VC to be tested.
segment	Specifies a segment of a multisegment pseudowire.
segment-number	A specific segment of the multisegment pseudowire or a range of segments, indicated by two segment numbers.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds. The range is from 0 to 3600. The default is 2 seconds.
destination	(Optional) Specifies a network 127 address.
address-start	(Optional) The beginning network 127 address.
address-end	(Optional) The ending network 127 address.
address-increment	(Optional) Number by which to increment the network 127 address.

revision {**1** | **2** | **3**| **4**}	(Optional) Selects the type, length, values (TLVs) version of the implementation. Use the **revision 4** default unless attempting to interoperate with devices running Cisco IOS Release 12.0(27)S1 or 12.0(27)S2. If you do not select a **revision** keyword, the software uses the latest version. See the table in the ﷺ section for information on when to select the **1**, **2**, **3**, and **4** keywords.
source *source-address*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. Valid values are from 0 to 7. Default is 0.
ttl *maximum-time-to-live*	(Optional) Specifies a maximum hop count. Default is 30.
reply dscp *dscp-bits*	(Optional) Provides the capability to request a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value. The echo reply is returned with the IP header ToS byte set to the value specified in the **reply dsco** keyword.
reply mode *reply-mode*	(Optional) Specifies the reply mode for the echo request packet. The **reply mode** is one of the following: **ipv4** --Reply with an IPv4 User Datagram Protocol (UDP) packet (default). **no-reply** --Do not send an echo request packet in response. **router-alert** --Reply with an IPv4 UDP packet with router alert.
reply pad-tlv	(Optional) Tests the ability of the sender of an echo reply to support the copy pad TLV to echo reply.
force-explicit-null	(Optional) Forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.
output interface *tx-interface*	(Optional) Specifies the output interface for echo requests.
nexthop *ip-address*	(Optional) Causes packets to go through the specified next-hop address.
flags fec	(Optional) Requests that target Forwarding Equivalence Class (FEC) stack validation be done at the egress router. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Be sure to use this keyword with the **ttl** keyword.
revision *tlv-revision-number*	(Optional) Cisco TLV revision number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(18)SXE	The **reply dscp** and **reply pad-tlv** keywords were added.
12.4(6)T	The following keywords were added: **force-explicit-null**, **output interface**, **flags fec**, and **revision**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.0(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. The **nexthop** keyword was added.
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.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.4(20T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.3	The **segment** keyword was added.
12.2(33)SRE	This command was modified. Restrictions were added to the **pseudowire**keyword.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS XE 3.8	This command was modified. The **tp** keyword was added.
Cisco IOS XE 3.8	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

Use the **traceroute mpls** command to validate, test, or troubleshoot IPv4 LDP LSPs and IPv4 Resource Reservation Protocol (RSVP) TE tunnels.

UDP Destination Address Usage

The destination address is a valid 127/8 address. You can specify a single address or a range of numbers from 0.0.0 to *x.y.z* , where *x* , *y* , and *z* are numbers from 0 to 255 and correspond to the 127.*x.y.z* destination address.

The MPLS echo request destination address in the UDP packet is not used to forward the MPLS packet to the destination router. The label stack that is used to forward the echo request routes the MPLS packet to the destination router. The 127/8 address guarantees that the packets are routed to the localhost (the default loopback address of the router processing the address) if the UDP packet destination address is used for forwarding.

In addition, the destination address is used to adjust load balancing when the destination address of the IP payload is used for load balancing.

Time-to-Live Keyword Usage

The time-to-live value indicates the maximum number of hops a packet should take to reach its destination. The value in the TTL field in a packet is decremented by 1 each time the packet travels through a router.

For MPLS LSP ping, the TTL is a value after which the packet is discarded and an MPLS echo reply is sent back to the originating router.

For MPLS Multipath LSP Traceroute, the TTL is a maximum time-to-live value and is used to discover the number of downstream hops to the destination router. MPLS LSP Traceroute incrementally increases the TTL value in its MPLS echo requests (TTL = 1, 2, 3, 4, ...) to accomplish this.

Pseudowire Usage

The following keywords are not available with the **traceroute mpls pseudowire** command:

- **flags**
- **force-explicit-null**
- **output**
- **revision**
- **ttl**

Revision Keyword Usage

The **revision** keyword allows you to issue a **traceroute mpls ipv4** or **traceroute mpls traffic-eng** command based on the format of the TLV. The table below lists the revision option and usage guidelines for each option.

Table 233: Revision Options and Option Usage Guidelines

Revision Option	Option Usage Guidelines
1[3]	Not supported in Cisco IOS Release 12.4(11)T or later releases. Version 1 (draft-ietf-mpls-ping-03) For a device running Cisco IOS Release 12.0(27)S3 or a later release, you must use the **revision 1** keyword when you send LSP ping or LSP traceroute commands to devices running Cisco IOS Release 12.0(27)S1 or 12.0(27)S2.
2	Version 2 functionality was replaced by Version 3 functionality before any images were shipped.
3	Version 3 (draft-ietf-mpls-ping-03). • For a device implementing Version 3 (Cisco IOS Release 12.0(27)S3 or a later release), you must use the **revision 1** keyword when you send the LSP **ping** or LSP **traceroute** command to a device implementing Version 1 (that is, either Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2). • A **ping mpls pseudowire** command does not work with devices running Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2.

Revision Option	Option Usage Guidelines
4	• Version 8 (draft-ietf-mpls-ping-08)--Applicable before Cisco IOS Release 12.4(11)T. All echo packet's TLVs are formatted as specified in Version 8. • RFC 4379 compliant--Applicable after Cisco IOS Release 12.4(11)T. All echo packet's TLVs are formatted as specified in RFC 4379.

[3] If you do not specify the revision keyword, the software uses the latest version.

Examples

The following example shows how to trace packets through an MPLS LDP LSP:

```
Router# traceroute mpls ipv4 10.131.191.252/32
```

Alternatively, you can use the interactive mode:

```
Protocol [ip]: mpls
Target IPv4, pseudowire or traffic-eng [ipv4]: <ipv4 |pseudowire |tunnel> ipv4
Target IPv4 address: 10.131.191.252
Target mask: /32
Repeat [1]:
Packet size [100]:
Timeout in seconds [2]:
Extended commands? [no]: yes
Destination start address:
Destination end address:
Source address:
EXP bits in mpls header [0]:
TimeToLive [255]:
Reply mode (2-ipv4 via udp, 3-ipv4 via udp with router alert) [2]:
Reply ip header DSCP bits [0]:
Tracing MPLS Label Switched Path to 10.131.191.252/32, timeout is 2 seconds
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
  0 10.131.159.245 mtu 1500 []
! 1 10.131.191.252 100 ms
```

The following example shows how to trace packets through an MPLS TE tunnel:

```
Router# traceroute mpls traffic-eng Tunnel 0
Tracing MPLS TE Label Switched Path on Tunnel0, timeout is 2 seconds
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
  0 10.131.159.230 mtu 1500 [Labels: 22 Exp: 0]
R 1 10.131.159.225 mtu 1500 [Labels: 22 Exp: 6] 72 ms
```

```
R 2 10.131.191.229 mtu 1504 [implicit-null] 72 ms
! 3 10.131.191.252 92 ms
```

Alternatively, you can use the interactive mode:

```
Router# traceroute

Protocol [ip]: mpls
Target IPv4 or tunnel [ipv4]: traffic-eng
Tunnel number [0]:
Repeat [1]:
Timeout in seconds [2]:
Extended commands? [no]:
Tracing MPLS TE Label Switched Path on Tunnel0, timeout is 2 seconds
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
  0 10.131.159.230 mtu 1500 [Labels: 22 Exp: 0]
R 1 10.131.159.225 mtu 1500 [Labels: 22 Exp: 6] 72 ms
R 2 10.131.191.229 mtu 1504 [implicit-null] 72 ms
! 3 10.131.191.252 92 ms
```

Use the **show running-config** command to verify the configuration of Tunnel 0 (shown in bold). The tunnel destination has the same IP address as the one in the earlier trace IPv4 example, but the trace takes a different path, even though tunnel 0 is not configured to forward traffic by means of autoroute or static routing. The **trace mpls traffic-eng** command is powerful; it enables you to test the tunnels to verify that they work before you map traffic onto them.

```
Router# show running-config interface tunnel 0
Building configuration...
Current configuration : 210 bytes
!
interface Tunnel0
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.131.191.252       <----
Tunnel destination IP address.
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng path-option 5 explicit name as1pe-long-path
end
Router# show mpls traffic-eng tunnels tunnel 0 brief
Signalling Summary:
    LSP Tunnels Process:            running
    RSVP Process:                   running
    Forwarding:                     enabled
    Periodic reoptimization:        every 3600 seconds, next in 1369 seconds
    Periodic FRR Promotion:         Not Running
    Periodic auto-bw collection:    disabled
TUNNEL NAME               DESTINATION      UP IF     DOWN IF   STATE/PROT
PE_t0                     10.131.191.252   -         Et0/0     up/up
Router# show ip cef 10.131.191.252
10.131.191.252/32, version 37, epoch 0, cached adjacency 10.131.159.246
0 packets, 0 bytes
  tag information set, all rewrites owned
    local tag: 21
  via 10.131.159.246, Ethernet1/0, 0 dependencies
    next hop 10.131.159.246, Ethernet1/0
```

```
    valid cached adjacency
    tag rewrite with Et1/0, 10.131.159.246, tags imposed {}
```

The following example performs a trace operation on a multisegment pseudowire. The trace operation goes to segment 2 of the multisegment pseudowire.

```
Router# traceroute mpls pseudowire 10.10.10.9 220 segment 2
Tracing MS-PW segments within range [1-2] peer address 10.10.10.9 and timeout 2 seconds
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
L 1 10.10.9.9 4 ms [Labels: 18 Exp: 0]
    local 10.10.10.22 remote 10.10.10.9 vc id 220
! 2 10.10.3.3 4 ms [Labels: 16 Exp: 0]
    local 10.10.10.9 remote 10.10.10.3 vc id 220
```

Related Commands

Command	Description
ping mpls	Checks MPLS LSP connectivity.

traceroute mpls multipath

To discover all Multiprotocol Label Switching (MPLS) label switched paths (LSPs) from an egress router to an ingress router, use the **trace mpls multipath** command in privileged EXEC mode.

trace mpls multipath ipv4 *destination-address/destination-mask-length* [**timeout** *seconds*] [**interval** *milliseconds*] [**destination** *address-start address-end*] [**source** *source-address*] [**exp** *exp-bits*] [**ttl** *maximum-time-to-live*] [**reply mode** {**ipv4** | **router-alert**}] [**reply dscp** *dscp-value*] [**retry-count** *retry-count-value*] [**force-explicit-null**] [**output interface** *tx-interface* [**nexthop** *ip-address*]] [**hashkey ipv4 bitmap** *bitmap-size*] [**flags fec**] [**verbose**]

Syntax Description

ipv4	Specifies the destination type as a Label Distribution Protocol (LDP) IPv4 address.
destination-address	Address prefix of the target to be tested.
/ *destination-mask-length*	Number of bits in the network mask of the target address. The slash is required.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds. The range is from 0 to 3600. The default is 2 seconds.
interval *milliseconds*	(Optional) Sets the time between successive MPLS echo requests in milliseconds. This allows you to pace the transmission of packets so that the receiving router does not drop packets. The default is 0 milliseconds. Valid values are from 0 to 3500000 milliseconds.
destination	(Optional) Specifies a network 127 address.
address-start	(Optional) The beginning network 127 address.
address-end	(Optional) The ending network 127 address.
source	(Optional) Specifies the source address or name.
source-address	(Optional) Source address or name.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. Valid values are from 0 to 7. Default is 0.
ttl *maximum-time-to-live*	(Optional) Specifies a maximum hop count. The maximum time-to-live hop count allowed is 30.
reply mode {**ipv4** | **router-alert**}	(Optional) Specifies the reply mode for the echo request packet. The reply mode is one of the following: • **ipv4** = Reply with an IPv4 User Datagram Protocol (UDP) packet (default). • **router-alert** = Reply with an IPv4 UDP packet with router alert.

reply dscp *dscp-value*	(Optional) Controls the differentiated services codepoint (DSCP) value of an echo reply. Allows the support of a class of service (CoS) in an echo reply.
retry-count *retry-count-value*	(Optional) Sets the number of timeout retry attempts during a multipath LSP trace. A retry is attempted if an outstanding echo request times out waiting for the corresponding echo reply. A *retry-count-value* of 0 means infinite retries. Valid values are from 0 to 10.
force-explicit-null	(Optional) Forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.
output interface *tx-interface*	(Optional) Specifies the output interface for MPLS echo requests.
nexthop *ip-address*	(Optional) Causes packets to go through the specified next hop address.
hashkey ipv4 bitmap *bitmap-size*	(Optional) Allows you to control the hash key and multipath settings. • **ipv4** --Indicates an IPv4 address, which is the only hashkey type valid for multipath (type 8). • **bitmap** *bitmap-size* --Size of the bitmap IPv4 addresses.
flags fec	(Optional) Requests that target Forwarding Equivalence Class (FEC) stack validation of a transit router be done at the egress router. **Note** Be sure to use the **flags fec** keywords in conjunction with the **ttl** keyword.
verbose	(Optional) Displays the MPLS echo reply sender address of the packet and displays return codes.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **traceroute mpls multipath** command to discover all possible paths between an egress and ingress router in multivendor networks that use IPv4 load balancing at the transit routers.

Use the **destination** *address-start address-end* keyword and arguments to specify a valid 127/8 address. You have the option to specify a single *x.y.z-address* or a range of numbers from 0.0.0 to *x.y.z* , where *x* , *y* , and *z* are numbers from 0 to 255 and correspond to the 127.*x.y.z* destination address. The MPLS echo request

destination address in the UDP packet is not used to forward the MPLS packet to the destination router. The label stack that is used to forward the echo request routes the MPLS packet to the destination router. The 127/8 address guarantees that the packets are routed to the localhost (the default loopback address of the router processing the address) if the UDP packet destination address is used for forwarding. In addition, the destination address is used to adjust load balancing when the destination address of the IP payload is used for load balancing.

Examples

The following example shows how to discover all IPv4 LSPs to a router whose IP address is 10.1.1.150:

```
Router# traceroute mpls multipath ipv4 10.1.1.150/32
Starting LSP Multipath Traceroute for 10.1.1.150/32
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
LLLL!
Path 0 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.0 LLL!
Path 1 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.1 L!
Path 2 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.5 LL!
Path 3 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.7
Paths (found/broken/unexplored) (4/0/0)
  Echo Request (sent/fail) (14/0)
  Echo Reply (received/timeout) (14/0)
  Total Time Elapsed 472 ms
```

The following example shows how to set the number of timeout retry attempts to 4 during a multipath LSP trace:

```
Router# traceroute mpls multipath ipv4 10.1.1.150/32 retry-count 4

Starting LSP Multipath Traceroute for 10.1.1.150/32
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
LLLL!
Path 0 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.0 LLL!
Path 1 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.1 L!
Path 2 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.5 LL!
Path 3 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.7
Paths (found/broken/unexplored) (4/0/0)
 Echo Request (sent/fail) (14/0)
```

```
 Echo Reply (received/timeout) (14/0)
 Total Time Elapsed 460 ms
```

The following example shows that outgoing MPLS Operation, Administration, and Management (OAM) echo request packets will go through the interface e0/0 and will be restricted to the path with the next hop address of 10.0.0.3:

```
Router# traceroute multipath ipv4 10.4.4.4/32 output interface e0/0 nexthop 10.0.0.3
Starting LSP Multipath Traceroute for 10.4.4.4/32
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
L!
Path 0 found,
 output interface Et0/0 nexthop 10.0.0.3
 source 10.0.0.1 destination 127.0.0.0
Paths (found/broken/unexplored) (1/0/0)
 Echo Request (sent/fail) (2/0)
 Echo Reply (received/timeout) (2/0)
 Total Time Elapsed 728 ms
```

Related Commands

Command	Description
echo	Customizes the default behavior of echo packets.
mpls oam	Enters MPLS OAM configuration mode for customizing the default behavior of echo packet.
ping mpls	Checks MPLS LSP connectivity.
trace mpls	Discovers MPLS LSP routes that packets will actually take when traveling to their destinations.

traffic-engineering filter

To specify a filter with the given number and properties, use the **traffic-engineering filter** command in router configuration mode. To disable this function, use the **no** form of this command.

traffic-engineering filter *filter-number* **egress** *ip-address mask*
no traffic-engineering filter

Syntax Description

filter-number	A decimal value representing the number of the filter.
egress *ip-address mask*	IP address and mask for the egress port.

Command Default

Disabled

Command Modes

Router configuration

Command History

Release	Modification
11.1 CT	This command was introduced.
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

You must specify that the egress is the indicated address or mask, where egress is either the destination or the Border Gateway Protocol (BGP) next hop.

Examples

The following example shows how to configure a traffic engineering filter and a traffic engineering route for that filter over a label switched path (LSP)-encapsulated tunnel for the traffic engineering routing process:

```
Router(config)# router traffic-engineering
Router(config-router)# traffic-engineering filter 5 egress 10.0.0.1 255.255.255.255

Router(config-router)# traffic-engineering route 5 tunnel 5
```

Related Commands

Command	Description
show ip traffic-engineering routes	Displays information about the requested filters configured for traffic engineering.
traffic-engineering route	Configures a route for a specified filter, through a specified tunnel.

traffic-engineering route

To configure a route for a specified filter through a specified tunnel, use the **traffic-engineering route** command in router configuration mode. To disable this function, use the **no** form of this command.

traffic-engineering route *filter-number interface* [**preference** *number*] [**loop-prevention** {**on** | **off**}]
no traffic-engineering route *filter-number interface* [**preference** *number*] [**loop-prevention** {**on** | **off**}]

Syntax Description

filter-number	The number of the traffic engineering filter to be forwarded through the use of this traffic engineering route, if the route is installed.
interface	Label switched path (LSP)-encapsulated tunnel on which the traffic-passing filter should be sent, if this traffic engineering route is installed.
preference *number*	(Optional) This is a number from 1 to 255, with a lower value being more desirable. The default is 1.
loop-prevention	(Optional) A setting of **on** or **off**. The default is **on**.

Command Default

preference : 1**loop-prevention**: on

Command Modes

Router configuration

Command History

Release	Modification
11.1 CT	This command was introduced.
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 traffic engineering process is used to decide if a configured traffic engineering route should be installed in the forwarding table.

The first step is to determine if the route is up. If the route is enabled, the LSP tunnel interface is up, the loop prevention check is either disabled or passed, and the traffic engineering route is up.

If multiple routes for the same filter are up, a route is selected based on administrative preference.

If loop prevention is enabled, metrics are solicited from the tunnel tail, and the loop prevention algorithm is run on the result. For a discussion of the loop prevention algorithm, see the **show ip traffic-engineering metrics** command.

Examples

The following example shows how to configure a traffic engineering filter and a traffic engineering route for that filter through an LSP-encapsulated tunnel for the traffic engineering routing process:

```
Router(config)# router traffic-engineering
```

```
Router(config-router)# traffic-engineering filter 5 egress 10.0.0.1 255.255.255.255
Router(config-router)# traffic-engineering route 5 tunnel 5
```

Related Commands

Command	Description
show ip traffic-engineering configuration	Displays information about configured traffic engineering filters and routes.
show ip traffic-engineering routes	Displays information about the requested filters configured for traffic engineering.

transport vpls mesh

To create a full mesh of pseudowires under a virtual private LAN switching (VPLS) domain, use the **transport vpls mesh** command in interface configuration mode. To remove the mesh of pseudowires, use the **no** form of this command.

transport vpls mesh
no transport vpls mesh

Syntax Description

This command has no arguments or keywords.

Command Default

The transport type is not specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

This command creates a full mesh of pseudowires under a VPLS domain.

Examples

The following example creates a virtual Ethernet interface and then specifies a full mesh of pseudowires:

```
Router(config)# interface virtual-ethernet 1
Router(config-if)# transport vpls mesh
```

Related Commands

Command	Description
interface virtual-ethernet	Create a virtual Ethernet interfaces

tunnel destination access-list

To specify the access list that the template interface uses for obtaining the mesh tunnel interface destination address, use the **tunnel destination access-list** command in interface configuration mode. To remove the access list from this template interface, use the **no** form of this command.

tunnel destination access-list *num*
no tunnel destination access-list *num*

Syntax Description

num	Number of the access list.

Command Default

No default behavior or values to specify access lists.

Command Modes

Interface configuration (config-if)#

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

This command can be used only on template interfaces.

If you specify an access list that does not exist, no tunnels are set up. You need an access list to set up the destination addresses for the mesh tunnel interfaces.

If you enter the **shutdown** command on the autotemplate interface, the command is executed on all the cloned tunnel interfaces. To delete all the cloned tunnel interfaces, enter the **no tunnel destination** command on the autotemplate. To delete tunnel interfaces for a particular autotemplate, go to the particular interface and enter the **no tunnel destination** command.

Examples

The following example shows how to configure the template interface to use access-list 1 to obtain the tunnel destination address:

```
Router(config)# interface auto-template 1
Router(config-if)# tunnel destination access-list 1
```

Related Commands

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

tunnel destination list mpls traffic-eng

To specify a list of Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) destinations, use the **tunnel destination list mpls traffic-eng** command in interface configuration mode. To remove the destination list, use the **no** form of this command.

tunnel destination list mpls traffic-eng {**id** *destination-list-number* | **name** *destination-list-name*}
no tunnel destination list mpls traffic-eng {**id** *dest-list-number* | **name** *dest-list-name*}

Syntax Description

id *destination-list-identifier*	Specifies the number of a destination list. Valid range of numbers is 1-65535.
name *destination-list-name*	Specifies the name of a destination list.

Command Default

No destination list is specified.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **tunnel destination list mpls traffic-eng** command to specify a list point-to-multipoint tunnels.

Examples

The following example configures point-to-multipoint traffic engineering on tunnel interface 1:

```
Router# interface tunnel1
Router(config-if)# tunnel mode mpls traffic-eng point-to-multipoint
Router(config-if)# tunnel destination list mpls traffic-eng name P2MP-DYN-DST-LIST
```

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays MPLS TE tunnels.
tunnel destination list mpls traffic-eng	Specifies the list of MPLS TE P2MP destinations.

tunnel destination mesh-group

To specify a mesh group that an autotemplate interface uses to signal tunnels for all mesh group members, use the **tunnel destination mesh-group** command in interface configuration mode. To remove a mesh group from the template, use the **no** form of this command.

tunnel destination mesh-group *mesh-group-id*
no tunnel destination mesh-group *mesh-group-id*

Syntax Description

mesh-group-id	Number that identifies a specific mesh group.

Command Default

Mesh-groups are not advertised.

Command Modes

Interface configuration (config-if)#

Command History

Release	Modification
12.0(29)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

Use this command to associate a specific mesh group with an autotemplate. When a mesh group is associated with an autotemplate, the template interface signals tunnels for all mesh group members.

Examples

The following example shows how to configure an autotemplate to signal tunnels for mesh group 10:

```
Router(config)# interface auto-template 1
Router(config-if)# tunnel destination mesh-group 10
```

Related Commands

Command	Description
mpls traffic-eng mesh-group	Configures an IGP to allow MPLS TE LSRs that belong to the same mesh group to signal tunnels to the local router.

tunnel flow egress-records

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

tunnel flow egress-records
no tunnel flow egress-records

Syntax Description

This command has no arguments or keywords.

Command Default

A NetFlow record for encapsulated packets is not created.

Command Modes

Interface configuration

Command History

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

When this command is enabled on a GRE tunnel with both Cisco Express Forwarding and NetFlow enabled, a NetFlow record is created for packets that are encapsulated by the tunnel.

Examples

The following example shows how to enable NetFlow record creation:

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

Related Commands

Command	Description
show ip cache flow	Displays NetFlow switching statistics.

tunnel mode mpls traffic-eng

To set the mode of a tunnel to Multiprotocol Label Switching (MPLS) for traffic engineering, use the **tunnel mode mpls traffic-eng** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mode mpls traffic-eng
no tunnel mode mpls traffic-eng

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

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 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
tunnel mpls traffic-eng affinity	Configures an affinity for an MPLS traffic engineering tunnel.
tunnel mpls traffic-eng autoroute announce	Instructs the IGP to use the tunnel in its enhanced SPF algorithm calculation (if the tunnel is up).
tunnel mpls traffic-eng bandwidth	Configures the bandwidth required for an MPLS traffic engineering tunnel.
tunnel mpls traffic-eng path-option	Configures a path option.

Command	Description
tunnel mpls traffic-eng priority	Configures setup and reservation priority for an MPLS traffic engineering tunnel.

tunnel mode mpls traffic-eng point-to-multipoint

To enable the configuration of a Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) tunnel, use the **tunnel mode mpls traffic-eng point-to-multipoint** command in interface configuration mode. To remove the tunnel, use the **no** form of this command.

tunnel mode mpls traffic-eng point-to-multipoint
no tunnel mode

Syntax Description

This command has no arguments or keywords.

Command Default

No point-to-multipoint tunnel mode is enabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the command to differentiate point-to-multipoint tunnels from point-to-point tunnels.

Examples

The following example configures point-to-multipoint traffic engineering on tunnel interface 1:

```
Router# interface Tunnel1
Router(config-if)# tunnel mode mpls traffic-eng point-to-multipoint
Router(config-if)# tunnel destination list mpls traffic-eng name P2MP-DYN-DST-LIST
```

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays MPLS TE tunnels.
tunnel destination list mpls traffic-eng	Specifies the list of MPLS TE P2MP destinations.

tunnel mpls traffic-eng affinity

To configure an affinity (the properties the tunnel requires in its links) for a Multiprotocol Label Switching (MPLS) traffic engineering tunnel, use the **tunnel mpls traffic-eng affinity** command in interface configuration mode. To disable the MPLS traffic engineering tunnel affinity, use the **no** form of this command.

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

Syntax Description

properties	Attribute values required for links carrying this tunnel. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.
mask *mask value*	(Optional) Link attribute to be checked. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

Command Default

properties : 0X00000000 *mask value* : 0X0000FFFF

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
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 affinity determines the attributes of the links that this tunnel will use (that is, the attributes for which the tunnel has an affinity). The attribute mask determines which link attribute the router should check. If a bit in the mask is 0, an attribute value of a link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of a link and the required affinity of the tunnel for that bit must match.

A tunnel can use a link if the tunnel affinity equals the link attributes and the tunnel affinity mask.

Any properties set to 1 in the affinity should also be 1 in the mask. In other words, affinity and mask should be set as follows:

```
tunnel_affinity = (tunnel_affinity and tunnel_affinity_mask)
```

Examples

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

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

Related Commands

Command	Description
mpls traffic-eng attribute-flags	Sets the attributes for the interface.
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng autoroute destination

To automatically route traffic through a traffic engineering (TE) tunnel, use the **tunnel mpls traffic-eng autoroute destination** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mpls traffic-eng autoroute destination
no tunnel mpls traffic-eng autoroute destination

Syntax Description

This command has no arguments or keywords.

Command Default

If you do not enter this command, manually-configured static routes are required.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(1)S	This command was integrated into Cisco IOS 15.2(1)S.

Usage Guidelines

The **tunnel mpls traffic-eng autoroute destination** command prevents you from having to manually configure static routes. Use the **tunnel mpls traffic-eng autoroute destination** command because interarea TE tunnels cross areas.

For interarea tunnels, the **tunnel mpls traffic-eng autoroute announce** command and the **tunnel mpls traffic-end forwarding-adjacency** command are not operational.

Note The **tunnel mpls traffic-eng autoroute destination** command is not supported with SRTE.

Examples

The following example specifies that tunnel 103 has autoroute destination enabled:

```
Router(config)# interface Tunnel103
Router(config-if)# ip unnumbered Loopback0
Router(config-if)# tunnel destination 10.1.0.3
Router(config-if)# tunnel mode mpls traffic-end
Router(config-if)# tunnel mpls traffic-eng autoroute destination
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name 111-103
```

Related Commands

Command	Description
tunnel mpls traffic-eng autoroute announce	Specifies that the IGP should use the tunnel (if the tunnel is up) in its enhanced SPF calculation.

Command	Description
tunnel mpls traffic-end forwarding-adjacency	Advertises a TE tunnel as a link in an IGP network.

tunnel mpls traffic-eng auto-bw

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

tunnel mpls traffic-eng auto-bw [**collect-bw**] [**frequency** *seconds*] [**max-bw** *number*] [**min-bw** *number*]
no tunnel mpls traffic-eng auto-bw

Syntax Description

collect-bw	(Optional) Collects output rate information for the tunnel, but does not adjust the tunnel's bandwidth.
frequency *seconds*	(Optional) The interval between bandwidth adjustments. The specified interval can be from 300 to 604800 seconds. Do not specify a value lower than the output rate sampling interval specified in the **mpls traffic-eng auto-bw** command.
max-bw *number*	(Optional) Maximum automatic bandwidth, in kbps, for this tunnel. The range is 0 to 4294967295.
min-bw *number*	(Optional) Minimum automatic bandwidth, in kbps, for this tunnel. The range is 0 to 4294967295. For information about the default, see "Usage Guidelines."

Command Default

You cannot control the manner in which the bandwidth for a tunnel is adjusted.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)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.

Usage Guidelines

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

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

If you do not specify the **collect-bw** keyword, the tunnel's bandwidth is adjusted to the largest average output rate sampled for the tunnel since the last bandwidth adjustment for the tunnel was made. If you do not specify the **collect-bw** keyword but you do enter some but not all of the other keywords, the defaults for the options not entered are: **frequency**, every 24hours; **min-bw**, unconstrained (0); and **max-bw**, unconstrained.

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

The following rules apply to adjusting bandwidth on a tunnel:

- If the current bandwidth is less than 50 kbps, you can change the bandwidth only if the changed bandwidth is 10 kbps or more.
- If the current bandwidth is more than 50 kbps, you can change the bandwidth regardless of what percent it is of the current bandwidth.
- If the minimum or maximum bandwidth values are configured for a tunnel, the bandwidth stays between those values.
- If you configure a tunnel's bandwidth (in the **tunnel mpls traffic-eng bandwidth** command) and the minimum amount of automatic bandwidth (in the **tunnel mpls traffic-eng auto-bw** command), the minimum amount of automatic bandwidth adjustment is the lower of those two configured values. The default value of the **tunnel mpls traffic-eng bandwidth** command is 0.

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
mpls traffic-eng auto-bw timers	Enables automatic bandwidth adjustment on a platform for tunnels configured for bandwidth adjustment.
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.
tunnel mpls traffic-eng bandwidth	Configures bandwidth required for an MPLS traffic engineering tunnel,

tunnel mpls traffic-eng autoroute announce

To specify that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation, use the **tunnel mpls traffic-eng autoroute announce** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mpls traffic-eng autoroute announce

no tunnel mpls traffic-eng autoroute announce

Syntax Description

This command has no arguments or keywords.

Command Default

The IGP does not use the tunnel in its enhanced SPF calculation.

Command Modes

Interface configuration (config-if)

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 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

The only way to forward traffic onto a tunnel is by enabling this command or by explicitly configuring forwarding (for example, with an interface static route).

Examples

The following example shows how to specify that the IGP should use the tunnel in its enhanced SPF calculation if the tunnel is up:

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

Related Commands

Command	Description
ip route	Establishes static routes.
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng autoroute metric

To specify the Multiprotocol Label Switching (MPLS) traffic engineering tunnel metric that the Interior Gateway Protocol (IGP) enhanced shortest path first (SPF) calculation uses, use the **tunnel mpls traffic-eng autoroute metric** command in interface configuration mode. To disable the specified MPLS traffic engineering tunnel metric, use the **no** form of this command.

tunnel mpls traffic-eng autoroute metric {**absolute** | **relative**} *value*
no tunnel mpls traffic-eng autoroute metric

Syntax Description

absolute	Absolute metric mode; you can enter a positive metric value.
relative	Relative metric mode; you can enter a positive, negative, or zero value.
value	The metric that the IGP enhanced SPF calculation uses. The **relative** value can be from -10 to 10. **Note** Even though the value for a relative metric can be from -10 to 10, configuring a tunnel metric with a negative value is considered a misconfiguration. If from the routing table the metric to the tunnel tail appears to be 4, then the cost to the tunnel tail router is actually 3 because 1 is added to the cost for getting to the loopback address. In this instance, the lowest value that you can configure for the relative metric is -3.

Command Default

The default is metric relative 0.

Command Modes

Interface configuration (config-if)

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.

Examples

The following example shows how to specify the use of MPLS traffic engineering tunnel metric negative 1 for the IGP enhanced SPF calculation:

```
Router(config-if)# tunnel mpls traffic-eng autoroute metric relative -1
```

Related Commands

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

Command	Description
tunnel mpls traffic-eng autoroute announce mpls	Instructs the IGP to use the tunnel (if it is up) in its enhanced SPF calculation.

tunnel mpls traffic-eng backup-bw

To specify what types of label-switched paths (LSPs) can use a backup tunnel or whether the backup tunnel should provide bandwidth protection, and if so, how much, use the **tunnel mpls traffic-eng backup-bw** command in interface configuration mode.

tunnel mpls traffic-eng backup-bw {*kbps* | [**sub-pool** {*kbps* | **Unlimited**}]} [**global-pool** {*kbps* | **Unlimited**}] {*kbps* | [**class-type** {*kbps* | **Unlimited**}]}

Syntax Description

kbps	Amount of bandwidth in kilobits per second (kbps), that this backup tunnel can protect. The router limits the number of LSPs that can use this backup tunnel so that the sum of the bandwidth of the LSPs does not exceed the specified amount of bandwidth. If there are multiple backup tunnels, the router will use the best-fit algorithm.
sub-pool	Only LSPs using bandwidth from the subpool can use the backup tunnel.
global-pool	Only LSPs using bandwidth from the global pool can use the backup tunnel.
class-type	Enter the class type.
Unlimited	Backup tunnel does not provide bandwidth protection. Any number of LSPs can use the backup tunnel, regardless of their bandwidth.

Command Default

If neither the **sub-pool** nor **global-pool** keyword is entered, any LSP (those using bandwidth from the subpool or global pool) can use this backup tunnel.

Command Modes

Interface configuration (config-if)

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.

Usage Guidelines

If both the **sub-pool** and **global-pool** keywords are specified, **sub-pool** keyword must be specified first on the command line. For example, **tunnel mpls traffic eng backup-bw subpool 100 global-pool Unlimited** is legal, but it is not legal to specify **tunnel mpls traffic eng backup-bw global-pool Unlimited sub-pool 100**.

To limit the number of both subpool and global pool LSPs, enter the **tunnel mpls traffic eng backup-bw sub-pool** *kbps* **global-pool** *kbps* command.

The Unlimited keyword cannot be used for both the subpool and global pool.

Examples

In the following example, backup tunnel 1 is to be used only by LSPs that take their bandwidth from the global pool. The backup tunnel does not provide bandwidth protection. Backup tunnel 2 is to be used only by LSPs that take their bandwidth from the subpool. Backup tunnel 2 provides bandwidth protection for up to 1000 units.

```
Router(config)# interface Tunnel1
Router(config-if)# tunnel mpls traffic-eng backup-bw global-pool Unlimited
Router(config-if)# end
Router(config)# interface Tunnel2
Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000
Router(config-if)# end
```

Related Commands

Command	Description
mpls traffic-eng backup path	Assigns one or more backup tunnels to a protected interface.

tunnel mpls traffic-eng bandwidth

To configure the bandwidth required for a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, use the **tunnel mpls traffic-eng bandwidth** command in interface configuration mode. To disable this bandwidth configuration, use the **no** form of this command.

tunnel mpls traffic-eng bandwidth {*kbps* [**class-type** *value*] | **sub-pool** *kbps*}
no tunnel mpls traffic-eng bandwidth

Syntax Description

sub-pool	(Optional) Indicates a subpool tunnel.
class-type	(Optional) IETF-Standard syntax to indicate a subpool tunnel.
kbps	The bandwidth, in kilobits per second, set aside for the MPLS TE tunnel. The range is from 1 to 4294967295. The default value is 0.
value	The type of subpool tunnel. The valid entries fo this value are 0 and 1.

Command Default

The default tunnel is a global pool tunnel.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(11)ST	The **sub-pool** keyword was added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
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.
12.2(33)SRB	The **class-type** keyword was added and the **global** keyword was removed.
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 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Enter the bandwidth for either a global pool (BC0) or a subpool (BC1) tunnel, but not for both in the same statement. To specify both pools, you need to use this command twice, once with the **sub-pool** or **class-type** keyword to specify the narrower tunnel, and once without those keywords to specify the larger tunnel.

Examples

The following example shows how to configure 100 kbps of bandwidth for the MPLS traffic engineering tunnel:

```
Router(config-if)# tunnel mpls traffic-eng bandwidth 100
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
show mpls traffic-eng tunnel	Displays information about tunnels.

tunnel mpls traffic-eng exp

To specify the experimental (EXP) bits that will be forwarded over a member tunnel that is part of the Class-Based Tunnel Selection (CBTS) bundle, use the **tunnel mpls traffic-eng exp** command in interface configuration mode. To disable forwarding of the EXP bits, use the **no** form of this command.

tunnel mpls traffic-eng exp {*list-of-exp-values* | **default**}
no tunnel mpls traffic-eng exp {*list-of-exp-values* | **default**}

Syntax Description

list-of-exp-values	EXP bits allowed for the interface. Enter up to eight EXP values separated by spaces. Values range from 0 to 7. The default is the EXP values that were not configured or a specific member tunnel.
default	The member tunnel will forward the packets with the EXP bits that are not being forwarded by other member tunnels that are part of the same bundle.

Command Default

No EXP value is assigned to a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(29)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.

Usage Guidelines

You should enter the **tunnel mpls traffic-eng exp** command to specify the EXP bits for at least one member tunnel.

With the **tunnel mpls traffic-eng exp** command, you can configure each tunnel with any of the following:

- No EXP-related information
- One or more EXP values for the tunnel to carry (*list-of-exp-values* argument)
- All EXP values not currently allocated to any up tunnel (**default** keyword)
- One or more EXP values for the tunnel to carry, and the property that allows the carrying of all EXP values not currently allocated to any up tunnel (*list-of-exp-values* **default** argument and keyword pair)

The **default** keyword allows you to avoid explicitly listing all possible EXP values. You indicate a preference as to which tunnel to use for certain EXP values, should a tunnel other than the default tunnel go down.

This command allows configurations where:

- Not all EXP values are explicitly allocated to tunnels.
- Multiple tunnels have the default property.
- Some tunnels have EXP values configured and others do not have any configured.
- A given EXP value is configured on multiple tunnels.

The configuration of each tunnel is independent of the configuration of any other tunnel.

Examples

The following example shows how to specify an EXP value of 5 for MPLS TE tunnel Tunnel1:

```
interface Tunnel1
 tunnel destination 10.0.1.1
 tunnel mpls traffic-eng exp 5
```

Related Commands

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.

tunnel mpls traffic-eng exp-bundle master

To configure the primary tunnel, use the **tunnel mpls traffic-eng exp-bundle master** command in the interface configuration mode. To unconfigure the primary tunnel, use the **no** form of this command.

tunnel mpls traffic-eng exp-bundle master
no tunnel mpls traffic-eng exp-bundle master

Syntax Description

This command has no arguments or keywords.

Command Default

There is no primary tunnel for the bundle.

Command Modes

Interface configuration (config-if)

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

Use the **tunnel mpls traffic-eng exp-bundle master** command to configure the primary tunnel. Then specify the **tunnel mpls traffic-eng exp-bundle member** command to identify which tunnels belong to that primary tunnel. On the member tunnels, define which experimental (EXP) bit values should be used.

Examples

The following example specifies that there is a primary tunnel that includes tunnels Tunnel20000 through Tunnel20007:

```
interface Tunnel200
 ip unnumbered Loopback0
 ip ospf cost 1
 mpls ip
 tunnel destination 10.10.10.10
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng exp-bundle master
 tunnel mpls traffic-eng exp-bundle member Tunnel20000
 tunnel mpls traffic-eng exp-bundle member Tunnel20001
 tunnel mpls traffic-eng exp-bundle member Tunnel20002
 tunnel mpls traffic-eng exp-bundle member Tunnel20003
 tunnel mpls traffic-eng exp-bundle member Tunnel20004
 tunnel mpls traffic-eng exp-bundle member Tunnel20005
 tunnel mpls traffic-eng exp-bundle member Tunnel20006
 tunnel mpls traffic-eng exp-bundle member Tunnel20007
```

Related Commands

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

tunnel mpls traffic-eng exp-bundle member

To identify which tunnel is a member (bundled tunnel) of a primary tunnel, use the **tunnel mpls traffic-eng exp-bundle member** command in interface configuration mode. To remove the specified tunnel from being a member of the primary tunnel, use the **no** form of this command.

tunnel mpls traffic-eng exp-bundle member *tunnel-number*
no tunnel mpls traffic-eng exp-bundle member *tunnel-number*

Syntax Description

tunnel-number	The tunnel that belongs to the primary tunnel.

Command Default

The primary tunnel has no member tunnels.

Command Modes

Interface configuration (config-if)

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

Enter the **tunnel mpls traffic-eng exp-bundle member** command for each tunnel that you want to be a member of the primary tunnel. You should enter this command at least once.

Examples

The following example specifies that Tunnel1 is a member of the primary tunnel:

```
interface Tunnel200
 ip unnumbered Loopback0
 ip ospf cost 1
 mpls ip
 tunnel destination 10.10.10.10
 tunnel mode mpls traffic-eng
tunnel mpls traffic-eng exp-bundle master
 tunnel mpls traffic-eng exp-bundle member Tunnel1
```

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.
tunnel mpls traffic-eng exp-bundle master	Configures the primary tunnel.

tunnel mpls traffic-eng fast-reroute

To enable a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel to use an established backup tunnel in the event of a link or node failure, use the **tunnel mpls traffic-eng fast-reroute** command in interface configuration mode. To disable this capability, use the **no** form of this command.

tunnel mpls traffic-eng fast-reroute [**bw-protect**] [**node-protection**]

no tunnel mpls traffic-eng fast-reroute

Syntax Description

bw-protect	(Optional) Sets the "bandwidth protection desired" bit so that backup bandwidth protection is enabled.
node-protection	(Optional) Sets the "node protection desired" bit so that backup bandwidth protection is enabled.

Command Default

There is no backup bandwidth protection.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(08)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 Cisco Catalyst 6000 series with the SUP720 processor.
12.0(29)S	The **bw-protect** keyword was added.
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.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was integrated into Cisco IOS 15.2(1)T

Usage Guidelines

If you specify the **bw-protect** keyword, all path messages for the tunnel's label-switched path (LSP) are sent with the bandwidth protection bit set.

After you enter the command, with or without the **bw-protect** keyword, the requested action or change propagates along all hops of the LSP. Midpoint routers that are point of local repairs (PLRs) for the LSP take the appropriate action based on whether the bit was just set or cleared. If the bit was just set or cleared, a new backup tunnel selection happens for the LSP because the LSP now has a higher or lower priority in the backup tunnel selection process.

To unconfigure only backup bandwidth protection, enter the **tunnel mpls traffic-eng fast-reroute** command.

To disable an MPLS TE tunnel from using an established backup tunnel in the event of a link or node failure, enter the **no** form of the command.

Examples

In the following example, backup bandwidth protection is enabled:

```
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
```

Related Commands

Command	Description
mpls traffic-eng backup-path tunnel	Configures the interface to use a backup tunnel in the event of a detected failure on the interface.
mpls traffic-eng fast-reroute backup-prot-preemption	Changes the backup protection preemption algorithm to minimize the amount of bandwidth that is not used.
show tunnel mpls traffic-eng fast-reroute	Displays information about fast reroute for MPLS traffic engineering.

tunnel mpls traffic-eng forwarding-adjacency

To advertise a traffic engineering (TE) tunnel as a link in an Interior Gateway Protocol (IGP) network, use the **tunnel mpls traffic-eng forwarding-adjacency** command in interface configuration mode. To disable the functionality, use the **no** form of this command.

tunnel mpls traffic-eng forwarding-adjacency [**holdtime** *milliseconds*]
no tunnel mpls traffic-eng forwarding-adjacency

Syntax Description

holdtime *milliseconds*	(Optional) Specifies the time, in milliseconds (ms), that a TE tunnel waits after going down before informing the network. The range is 0 to 4294967295 ms. The default value is 0.

Command Default

A TE tunnel is not advertised as a link in an IGP network.

Command Modes

Interface configuration

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 12.2(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 **tunnel mpls traffic-eng forwarding-adjacency** command with the **isis metric** command to avoid inefficient forwarding behavior. Ensure that any nodes traversed by the TE tunnel being advertised do not consider the TE tunnel as part of the shortest path to the destination.

Note The **tunnel mpls traffic-eng forwarding-adjacency** command requires Intermediate System-to-Intermediate System (IS-IS) support.

Examples

In the following example, the holdtime is set to 10,000 milliseconds:

```
Router(config-if)# tunnel mpls traffic-eng forwarding-adjacency holdtime 10000
```

In the following example, the holdtime defaults to 0:

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

Related Commands

Command	Description
debug mpls traffic-eng forwarding-adjacency	Displays debug messages for traffic engineering, forwarding adjacency events.
isis metric	Configures the cost metric for an interface.
show mpls traffic-eng forwarding-adjacency	Displays TE tunnels being advertised as links in an IGP network.

tunnel mpls traffic-eng interface down delay

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

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

Syntax Description

time	Time, in minutes. The only valid value is 0.

Command Default

There is a delay before the tunnel goes down.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

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

Examples

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

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

tunnel mpls traffic-eng load-share

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

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

Syntax Description

value	A value from which the head-end router will calculate the proportion of traffic to be sent down each of the parallel tunnels. Range is from 1 to 1000000.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
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

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

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

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

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

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

Examples

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

```
interface Tunnel1
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination 41.41.41.41
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng load-share 2
interface Tunnel2
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination 41.41.41.41
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng load-share 1
interface Tunnel3
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination 41.41.41.41
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng load-share 1
```

Related Commands

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

tunnel mpls traffic-eng name

To provide a name for a Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) point-to-point (P2P) or point-to-multipoint (P2MP) tunnel, use the **tunnel mpls traffic-eng name** command in tunnel interface configuration mode. To remove the name from the tunnel, use the **no** form of this command.

tunnel mpls traffic-eng name *signaled-tunnel-name*
no tunnel mpls traffic-eng name *signaled-tunnel-name*

Syntax Description

signaled-tunnel-name	Name of the tunnel. Limit: 63 characters Spaces are not allowed.

Command Default

The TE tunnel name is either the interface description or is *hostname* _ttunnel id.

Command Modes

Tunnel interface configuration mode

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

When configuring the tunnel name, consider the following:

- If tunnel name is configured, it overrides the default names, which are either the tunnel interface description or *hostname* _ttunnel id. If the TE tunnel name configuration is removed, TE resignals the LSP using the next preferred tunnel name source (the interface description or the default host name and tunnel ID). This is completed in break-before-make fashion; therefore, traffic may be lost.
- The TE tunnel name must be unique. It cannot be the same name as the interface description or the hostname and tunnel id.
- The command is available for tunnels that are configured in TE P2P tunnel mode or TE P2MP tunnel mode.
- In releases previous to Cisco IOS 15.1(1)S, changing the interface description does NOT result in the LSP being resignaled. The introduction of the**tunnel mpls traffic-eng name** command requires that the tunnel state be flapped before the signaled name is updated.

Examples

The following example specifies the name of tunnel0 as “MYTUNNEL” and tunnel1 as “MYOTHERTUNNEL”:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel mpls traffic-eng name
 MYTUNNEL
.
.
.
Router(config)# interface tunnel1
Router(config-if)# tunnel mpls traffic-eng name
 MYOTHERTUNNEL
```

The **show mpls traffic-eng tunnel** command displays the names of the P2P and P2MP tunnels.

```
Router# show mpls traffic-eng tunnel
 tunnel0
Name: MYTUNNEL                        (Tunnel0) Destination: 10.3.0.1
Router# show mpls traffic-eng tunnel
 tunnel1
Tunnel1     (p2mp),  Admin: up, Open: up
  Name: MYOTHERTUNNEL
```

The **show mpls traffic-eng tunnel brief** command displays the name of P2P tunnels, However, for P2MP tunnels, the command displays the tunnel ID and not the name. In the following example, the output displays the name of the P2P tunnel0 and the tunnel ID of P2MP tunnel1.

```
Router# show mpls traffic-eng tunnel brief
P2P TUNNELS/LSPs:
TUNNEL NAME             DESTINATION      UP IF     DOWN IF   STATE/PROT
MYTUNNEL                10.3.0.1         -         Et0/0     up/up
Displayed 1 (of 1) heads, 0 (of 0) midpoints, 0 (of 0) tails
P2MP TUNNELS:
                         DEST        CURRENT
INTERFACE   STATE/PROT  UP/CFG     TUNID  LSPID
Tunnel1     up/up       2/3        1      1
Displayed 1 (of 1) P2MP heads
```

Related Commands

Command	Description
show mpls traffic-eng tunnel	Displays information about the MPLS Traffic Engineering P2P or P2MP tunnels.

tunnel mpls traffic-eng path-option

To configure a path option for a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, use the **tunnel mpls traffic-eng path-option** command in interface configuration mode. To disable this function, use the **no** form of this command.

tunnel mpls traffic-eng path-option *number* {**dynamic** [{**attributes** *lsp-attributes* | **bandwidth** {*kbps* | **subpool** *kbps*} [**lockdown**] | **lockdown** [**bandwidth** {*kbps* | **subpool** *kbps*}] | **explicit** {**identifier** *path-number* | **name** *path-name*} [**attributes** *lsp-attributes* [**verbatim**]] | **bandwidth** {*kbps* | **subpool** *kbps*} [**lockdown**] [**verbatim**]}] | **lockdown bandwidth** {*kbps* | **subpool** *kbps*} [**verbatim**] | **verbatim bandwidth** {*kbps* | **subpool** *kbps*} [**lockdown**]}

no tunnel mpls traffic-eng path-option *number*

Syntax Description

number	Preference for this path option. When you configure multiple path options, lower numbered options are preferred. Valid values are from 1 to 1000.
dynamic	Dynamically calculates the path of the label switched path (LSP)
attributes *lsp-attributes*	(Optional) Identifies an LSP attribute list. **Note** The attribute list used should be the same as the primary path option being configured.
bandwidth *kbps*	(Optional) Overrides the bandwidth configured on the tunnel or the attribute list. The *kbps* is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295. **Note** The bandwidth value should be the same as the primary path option being configured.
subpool *kbps*	(Optional) Indicates that the bandwidth override value uses the subpool bandwidth. The *kbps* argument is the number of kilobits per second of the subpool bandwidth set aside for the path option. The range is 1 to 4294967295.
lockdown	(Optional) Indicates that the LSP cannot be reoptimized.
explicit	Specifies that the path of the LSP is an IP explicit path.
identifier *path-number*	Specifies the path number of the IP explicit path that the tunnel uses with this option. The range is from 1 to 65535.
name *path-name*	Specifies the path name of the IP explicit path that the tunnel uses with this option.
verbatim	(Optional) Bypasses the topology database verification process.

Command Default

No path option for an MPLS TE tunnel is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

You can configure multiple path options for a single tunnel. For example, there can be several explicit path options and a dynamic option for one tunnel. Path setup preference is for lower (not higher) numbers, so option 1 is preferred.

If you specify the **dynamic** keyword, the software checks both the physical bandwidth of the interface and the available TE bandwidth to be sure that the requested amount of bandwidth does not exceed the physical bandwidth of any link. To oversubscribe links, you must specify the **explicit** keyword. If you use the **explicit** keyword, the software only checks how much bandwidth is available on the link for TE; the amount of bandwidth you configure is not limited to how much physical bandwidth is available on the link.

Examples

The following example shows how to configure the tunnel to use a named IP explicit path:

```
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name test
```

Related Commands

Command	Description
ip explicit-path	Enters the command mode for IP explicit paths and creates or modifies the specified path.
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show ip explicit-paths	Displays the configured IP explicit paths.
tunnel mpls traffic-eng path-option protect	Configures a secondary path option for an MPLS TE tunnel.

tunnel mpls traffic-eng path-option protect

To configure a secondary path option for a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, use the **tunnel mpls traffic-eng path-option protect** command in interface configuration mode. To disable this function, use the **no** form of this command.

Cisco IOS Release 12.0(30)S and Later

tunnel mpls traffic-eng path-option protect *number*[{**attributes** *lsp-attributes* | **bandwidth**{*kbps* | **sub-pool** *kbps*} | **explicit**{**identifier** *path-number* | **name** *path-name*} | [{**attributes** *lsp-attributes*[{**verbatim**}] | **bandwidth**{*kbps* | **sub-pool** *kbps*}[{**verbatim**}] | **verbatim** | [{**bandwidth**{*kbps* | **sub-pool** *kbps*}}]}] | **list**{**identifier** *path-number* | **name** *path-name*}[{**attributes** *lsp-attributes* | **bandwidth**{*kbps* | **sub-pool** *kbps*}}]}]

Cisco IOS Release 12.4(20)T and Later

tunnel mpls traffic-eng path-option protect *number*{**dynamic** | [{**attributes** *lsp-attributes* | **bandwidth**{**kbps** | **sub-pool** *kbps*}}] | **explicit**{**identifier** *path number* | **name** *path-name*}[{**attributes** *lsp-attributes*[{**verbatim**}] | **bandwidth**{*kbps* | **sub-pool** *kbps*}[{**verbatim**}] | **verbatim** | [{**bandwidth**{*kbps* | **bandwidth** *kbps*}}]}]}

Cisco IOS Release 12.2(50)SY and Later

tunnel mpls traffic-eng path-option protect *number* **explicit**
identifier *path-number* | **name** *path-name*
attributes *lsp-attributes*[{**verbatim**}] | **bandwidth**{*kbps* | **sub-pool** *kbps*}[{**verbatim**}] | **verbatim** | [{**bandwidth**{*kbps* | **sub-pool** *kbps*}}]

no tunnel mpls traffic-eng path-option protect *number*

Syntax Description

number	The primary path option being protected. Valid values are from 1 to 1000.
dynamic	Part of the label switched path (LSP) is dynamically calculated.
attributes *lsp-attributes*	(Optional) Identifies an LSP attribute list. **Note** The attribute list used should be the same as the primary path option being protected.
bandwidth *kbps*	(Optional) Overrides the bandwidth configured on the tunnel or the attribute list. The value *kbps* is the number of kilobits per second set aside for the path option. The range is 1 to 4294967295. **Note** The bandwidth value should be the same as the primary path option being protected.
sub-pool *kbps*	(Optional) Indicates that the bandwidth override value uses sub-pool bandwidth. The value *kbps* is the number of kilobits per second of sub-pool bandwidth set aside for the path option. The range is 1 to 4294967295.

explicit	Indicates that the path of the LSP is an IP-explicit path.
identifier *path-number*	Specifies the path number of the IP-explicit path that the tunnel uses with this option. The range is 1 to 65535.
name *path-name*	Specifies the path name of the IP-explicit path that the tunnel uses with this option.
verbatim	(Optional) Bypasses the topology database verification process.

Command Default

The MPLS TE tunnel does not have a secondary path option.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(26)S	This command was modified. LSP-related keywords and arguments for path options were added.
12.0(30)S	This command was modified. The **protect** keyword was added.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T. The **dynamic** keyword is not available on Cisco Catalyst 6000 platforms.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY. The **dynamic** keyword is not available on Cisco Catalyst 6000 platforms.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

Cisco recommends that the primary path options being protected use explicit paths.

Calculation of a dynamic path for the path protected LSP is not available. When configuring the IP explicit path for the path protected LSP, choose hops that minimize the number of links and nodes shared with the primary path option that is being protected.

If the path option being protected uses an attribute list, configure path protection to use the same attribute list.

If the path option being protected uses bandwidth override, configure path protection to use bandwidth override with the same values.

Examples

The following example shows how to configure the tunnel to use a named IP-explicit path:

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 1 explicit name test
```

The following example shows how to configure path option 1 to use an LSP attribute list identified with the numeral 1:

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 1 explicit name test attributes
 1
```

The following example shows how to configure bandwidth for a path option to override the bandwidth configured on the tunnel:

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 3 explicit name test bandwidth
 0
```

The following example shows how to configure path protection on a standby LSP:

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit pri-path

Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit name alt-path
```

Every path option that needs to be protected must have its protection path configured immediately after the path option is configured, as shown in the above example.

Related Commands

Command	Description
ip explicit-path	Enters the command mode for IP explicit paths and creates or modifies the specified path.
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show ip explicit-paths	Displays the configured IP explicit paths.
tunnel mpls traffic-eng path-option	Configures a primary path for an MPLS TE tunnel.

tunnel mpls traffic-eng path-selection metric

To specify the metric type to use for path calculation for a tunnel, use the **tunnel mpls traffic-eng path-selection metric** command in interface configuration mode. To remove the specified metric type, use the **no** form of this command.

tunnel mpls traffic-eng path-selection metric {**igp** | **te**}
no tunnel mpls traffic-eng path-selection metric

Syntax Description

igp	Use the Interior Gateway Protocol (IGP) metric.
te	Use the traffic engineering (TE) metric.

Command Default

The default is the **te** metric.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(18)ST	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)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.

Usage Guidelines

The metric type to be used for path calculation for a given tunnel is determined as follows:

- If the **tunnel mpls traffic-eng path-selection metric** command was entered to specify a metric type for the tunnel, use that metric type.
- Otherwise, if the **mpls traffic-eng path-selection metric** was entered to specify a metric type, use that metric type.
- Otherwise, use the default (**te**) metric.

Examples

The following commands specify that the igp metric should be used when you are calculating the path for Tunnel102:

```
Router(config)# interface tunnel102
Router(config-if)# tunnel mpls traffic-eng path-selection metric igp
```

Related Commands

Command	Description
mpls traffic-eng path-selection metric	Specifies the metric type to use for path calculation for TE tunnels for which no metric has been explicitly configured.

tunnel mpls traffic-eng priority

To configure the setup and reservation priority for Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, use the **tunnel mpls traffic-eng priority** command in interface configuration mode. To remove the specified setup and reservation priority, use the **no** form of this command.

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

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

Syntax Description

setup-priority	The priority used when signaling an link-state packet (LSP) for this tunnel to determine which existing tunnels can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.
hold-priority	(Optional) The priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.

Command Default

By default, the setup priority is 7. The value of hold priority is the same as the value of setup priority.

Command Modes

Interface configuration (config-if)

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 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was integrated into Cisco IOS 15.2(1)T.

Usage Guidelines

When an LSP is being signaled and an interface does not currently have enough bandwidth available for that LSP, the call admission software preempts lower-priority LSPs so that the new LSP can be admitted. (LSPs are preempted if that allows the new LSP to be admitted.)

The new LSP's priority is its setup priority and the existing LSP's priority is its hold priority. The two priorities enables the signaling of an LSP with a low setup priority (so that the LSP does not preempt other LSPs on setup) but a high hold priority (so that the LSP is not preempted after it is established).

Setup priority and hold priority are typically configured to be equal, and setup priority cannot be better (numerically smaller) than the hold priority.

Examples

The following example shows how to configure a tunnel with a setup and hold priority of 1:

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

Related Commands

Command	Description
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng record-route

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

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

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

Command	Description
show ip rsvp reservation	Displays current RSVP related receiver information in the database.

Command	Description
show mpls traffic-eng tunnels	Displays information on the source, destination, path and interface of MPLS TE tunnels.
tunnel mpls traffic-eng fast-reroute	Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.

tunnel tsp-hop

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

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

Syntax Description

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

Command Default

No hops are defined.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CT	This command was introduced.
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 list of tunnel hops must specify a strict source route for the tunnel. In other words, the router at hop <*n* > must be directly connected to the router at hop <*n* >+1.

Examples

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

```
Router(config)# interface tunnel 5
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# ip unnumbered e0/1
Router(config-if)# tunnel tsp-hop 1 172.16.0.2
Router(config-if)# tunnel tsp-hop 2 172.17.0.2 lasthop
```

Related Commands

Command	Description
tunnel mpls traffic-eng affinity	Sets the encapsulation mode of the tunnel to label switching.

tunnel vrf

To associate a VPN routing and forwarding (VRF) instance with a specific tunnel destination, interface, or subinterface, use the **tunnel vrf** command in global configuration or interface configuration mode. To disassociate a VRF from the tunnel destination, interface, or subinterface, use the **no** form of this command.

tunnel vrf *vrf-name*
no tunnel vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

The default destination is determined by the global routing table.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. Support was added for the Cisco 10000 Series Routers.
12.2(31)SB5	This command was integrated into Cisco IOS Release 12.2(31)SB5.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

To associate a VRF instance with a specific tunnel destination, ensure that the tunnel source and destination are in the same VRF.

Use the **ip vrf forwarding** command to associate a VRF instance with an interface or a subinterface other than a tunnel interface.

Use the **no ip vrf forwarding** *vrf-name* command or the **no tunnel vrf** *vrf-name* command to set either the IP VRF or the tunnel VRF to the global routing table.

The tunnel is disabled if no route to the tunnel destination is defined. If the tunnel VRF is set, you must configure a route to that destination in the VRF.

Cisco 10000 Series Routers and Cisco ASR 1000 Series Aggregation Services Routers

The VRF associated with the tunnel through the **tunnel vrf** command is the same as the VRF associated with the physical interface over which the tunnel sends packets (outer IP packet routing).

Examples

The following example shows how to associate a VRF with a tunnel destination. The tunnel endpoint 10.5.5.5 is looked up in the VRF named vrf2.

```
Device(config)# interface tunnel0
Device(config-if)# ip vrf forwarding vrf1
Device(config-if)# ip address 10.3.3.3 255.255.255.0
Device(config-if)# tunnel source loop 0
Device(config-if)# tunnel destination 10.5.5.5
Device(config-if)# tunnel vrf vrf2
```

Related Commands

Command	Description
ip route vrf	Establishes static routes for a VRF.
ip vrf	Configures a VRF routing table.
ip vrf forwarding	Associates a VRF instance with an interface or subinterface.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

type copy

To configure copy-based sampling that allows sampled packets to be copied to software for accounting, use the **type copy** command in Flexible NetFlow sampler configuration mode. To disable copy-based sampling, use the **no** form of this command.

type copy
no type copy

Syntax Description

This command has no arguments or keywords.

Command Default

Copy-based sampling is not configured.

Command Modes

Flexible NetFlow sampler configuration (config-sampler)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

The **type copy** command enables the copying of sampled packets to the software or Route Processor. Features that are not available in hardware can then be applied on those packets.

Examples

Flow samplers are used to reduce the load placed by flexible NetFlow on the networking device to monitor traffic by limiting the number of packets that are analyzed. When you apply the copy type command to a flow sampler you enable the sampled packets to be copied to Cisco software for accounting.

```
Router(config)# sampler SAMPLER-1
Router(config-sampler)# type copy
Router(config-sampler)#  mode rand 1 out 10
Router(config-sampler)# exit
```

Related Commands

Command	Description
sampler	Creates a flexible NetFlow flow sampler, or modifies an existing flexible NetFlow flow sampler, and enters flexible NetFlow sampler configuration mode.

udp port

To configure the User Datagram Protocol (UDP) port information on the xconnect class, use the **udp port** command in xconnect configuration mode. To revert to the default settings, use the **no** form of this command.

udp port local *local-udp-port* **remote** *remote-udp-port*
no udp port local *local-udp-port* **remote** *remote-udp-port*

Syntax Description

local *local-udp-port*	The local UDP port number. The range is 49152 to 57343.
remote *remote-udp-port*	Specifies the remote UDP port number. The range is 49152 to 57343.

Command Default

The virtual circuit will not be enabled.

Command Modes

Xconnect configuration mode (config-if-xconn)

Command History

Release	Modification
15.1(2)S	This command was introduced.
15.1(2)SNH	This command was integrated into Cisco IOS Release 15.1(2)SNH. This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example shows how to configure the local and remote UDP port numbers:

```
Router# configure terminal
Router(config)# interface cem 0/13
Router(config-if)# xconnect 10.2.2.9 200 pw-class udpClass
Router(config-if-xconn)# udp port local 50000 remote 57343
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
show pw-udp vc	Displays information about pseudowire UDP VC.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

vc type

To specify the type of virtual circuit (VC) for a pseudowire class, use the **vc type** command in interface configuration or template configuration mode. To remove the VC type configuration, use the **no** form of this command.

vc type {**ethernet** | **vlan**}
no vc type

Syntax Description

ethernet	Specifies Ethernet as the VC type.
vlan	Specifies VLAN as the VC type.

Command Default

The VC type is auto-detected by the device. Initially, the VC type advertised by the device is Ethernet, but it switches to VLAN if the peer advertises VLAN as the VC type.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
15.4(1)S	This command was introduced.

Usage Guidelines

Use the **vc type** command for pseudowire classes where the pseudowire is a member of a virtual forwarding interface (VFI).

Examples

The following example shows how to specify the type of VC as Ethernet in interface configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# interface pseudowire1
Device(config-if)# encapsulation mpls
Device(config-if)# vc type ethernet
Device(config-if)# exit
```

The following example shows how to specify the type of VC as VLAN in template configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# vc type vlan
Device(config-template)# exit
```

Related Commands

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

ve

To specify the Virtual Private LAN Service (VPLS) endpoint (VE) ID value or ID range value for a VPLS configuration, use the **ve** command in L2VPN VFI autodiscovery configuration mode. To remove the entry, use the **no** form of this command.

ve {**id** *id-value* | **range** *range-value*}
no ve {**id** | **range**}

Syntax Description

id *id-value*	ID value of the VE device. The range is from 1 to 16384.
range *range-value*	ID range value of the VE device. The range is from 11 to 512.

Command Default

No VE ID value or ID range value is specified.

Command Modes

L2VPN VFI autodiscovery configuration (config-vfi-autodiscovery)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

The **ve id** *id-value* command specifies the local VE identifier for the VFI for a VPLS configuration.

The VE ID identifies a VFI within a VPLS service. This means that VFIs in the same VPLS service cannot share the same VE ID. The scope of the VE ID is only within a bridge domain. Therefore, VFIs in different bridge domains within a PE can still use the same VE ID.

The **ve range** *range-value* command overrides the minimum size of the VE block. The default minimum size is 10. Any configured VE range must be higher than 10.

Examples

The following example specifies the VE with the ID value of 1001:

```
Device(config-vfi-autodiscovery)# ve id 1001
```

The following example specifies an ID range of 12:

```
Device(config-vfi-autodiscovery)# ve range 12
```

Related Commands

Command	Description
autodiscovery (MPLS)	Designates a Layer 2 VFI as having BGP autodiscovered pseudowire members.

vpls-id

To assign an identifier to the Virtual Private LAN Services (VPLS) domain, use the **vpls-id** command in L2 VFI configuration or VFI autodiscovery configuration mode. To revert to the default VPLS ID, use the **no** form of this command.

vpls-id {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
no vpls-id {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

Syntax Description

autonomous-system-number:*nn*	Specifies a 16-bit autonomous system number (ASN) and 32-bit arbitrary number. The ASN need not match the local ASN.
ip-address:*nn*	Specifies a 32-bit IP address and a 16-bit arbitrary number. Only IPv4 addresses are supported.

Command Default

The VPLS ID is generated automatically by VPLS autodiscovery.

Command Modes

L2 VFI configuration (config-vfi)

VFI autodiscovery configuration (config-vfi-autodiscovery)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into a release prior to Cisco IOS XE Release 3.6S.
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 VFI autodiscovery configuration mode.

Usage Guidelines

VPLS autodiscovery automatically generates a VPLS ID using the Border Gateway Protocol (BGP) ASN and the configured virtual forwarding instance (VFI) VPN ID. You can use the **vpls-id** command to change the automatically generated VPLS ID.

The Label Distribution Protocol (LDP) uses the VPLS ID when signaling VPLS autodiscovered neighbors. The VPLS ID identifies the VPLS domain.

Only one VPLS ID can be configured per VFI. The same VPLS ID cannot be configured in multiple VFIs on the same provider edge (PE) router.

The manually configured VPLS ID replaces the internally generated VPLS ID. The manually configured VPLS ID also changes the automatically generated route target (RT).

The **vpls-id** command defines the attachment group identifier (AGI) for the VPLS domain. Therefore, all PE routers in the same VPLS domain must use the same VPLS ID.

For interautonomous system configurations, you must manually configure the VPLS ID instead of using the automatically generated VPLS ID, because all PE routers do not share the same autonomous system number.

Examples

The following example shows how to set a VPLS ID to the autonomous system and network number 5:300:

```
Device(config)# l2 vfi SP2 autodiscovery
Device(config-vfi)# vpn id 200
Device(config-vfi)# vpls-id 5:300
```

The following example shows how to set the VPLS ID to IP address and network number 10.4.4.4:70

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 200
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi-autodiscovery)# rd 2:3
Device(config-vfi-autodiscovery)# vpls-id 10.4.4.4:70
```

Related Commands

Command	Description
autodiscovery (l2vpn vfi)	Designates a VFI as having BGP autodiscovered pseudowire members.
rd	Creates routing and forwarding tables for a VRF.

vpn

To specify that the source and destination IPv4 addresses of a given virtual private dialup network (VPDN) group belong to a specified Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **vpn** command in VPDN group or VPDN template configuration mode. To disassociate all IPv4 addresses in a VPDN group from a VRF, use the **no** form of this command.

vpn {**vrf** *vrf-name* | **id** *vpn-id*}
no vpn

Syntax Description

vrf *vrf-name*	Name of the VRF instance to be associated with the IPv4 addresses of the VPDN group.
id *vpn-id*	VPN ID of the VRF to be associated with the IPv4 addresses of the VPDN group.

Command Default

VPDN groups are not associated with a VRF.

Command Modes

VPDN group configuration
VPDN template configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI7	This command was integrated into Cisco IOS Release 12.3(7)XI7 and implemented on the Cisco 10000 series routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB for the PRE2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **vpn**command to configure the Cisco IOS software to look up a VPDN source or destination IPv4 address in a specific VPN routing table instead of the global routing table.

Before you can issue the **vpn** command, a VRF instance must be created using the **ip vrf** command.

The **vpn** command can be used with both dial-in and dial-out VPDN scenarios.

Examples

The following example associates the IP addresses configured in the VPDN group named group1 with the VRF named vrf-second:

```
vpdn-group group1
 request-dialin
 protocol l2tp
!
 vpn vrf vrf-second
```

```
 source-ip 172.16.1.9
 initiate-to ip 172.16.1.1
```

The following example associates the IP addresses configured in the VPDN group named group2 with the VPN ID 11:2222:

```
vpdn-group group2
 request-dialin
 protocol l2tp
!
 vpn id 11:2222
 source-ip 172.16.1.9
 initiate-to ip 172.16.1.1
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a VPDN.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

vpn id

To set or update a VPN ID on a VPN routing and forwarding (VRF) instance, use the **vpn id** command in VRF configuration or L2VFI configuration mode. To return to the default setting, use the **no** form of this command.

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

Syntax Description

oui **:**	Organizationally unique identifier (OUI). The IEEE organization assigns this identifier to companies. The OUI is restricted to three octets and followed by a colon.
vpn-index	Index of the VPN within the company. This VPN index is restricted to four octets.

Command Default

The VPN ID is not set.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(17)ST	This command was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

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

Once configured, a VPN ID cannot be removed, however, it can be changed. To change the VPN ID, issue the command again. The new ID overwrites the existing ID.

Examples

The following example shows how to assign the VPN ID of 0000a100003f6c to a VRF called vpn1 by using the **ip vrf** command:

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

The following example shows how to assign the VPN ID of 0000a100003f6c to a VRF called vpn1 by using the **vrf definition** command:

```
Device(config)# vrf definition vpn1
Device(config-vrf)# vpn id a1:3f6c
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
l2vpn vfi context	Establishes a Layer 2 VPN VFI context.
show ip vrf detail	Displays all the VRFs on a router.
show ip vrf id	Displays all the VPN IDs that are configured in the router and their associated VRF names and VRF RDs.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

vpn id (mpls)

To set or update a VPN ID on a Virtual Private LAN Services (VPLS) instance, use the **vpn id** command in L2 VFI configuration mode.

vpn id *vpn-id*

Syntax Description

vpn-id	VPN ID value. The range is from 1 to 4294967295.

Command Default

The VPN ID is not set.

Command Modes

L2 VFI configuration (config-vfi)

Command History

Release	Modification
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
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the same VPN ID for the provider edge (PE) routers that belong to the same VPN. Make sure the VPN ID is unique for each VPN in the service provider network.

Once configured, a VPN ID cannot be removed. However, it can be changed. To change the VPN ID, issue the command again. The new ID overwrites the existing ID.

Note The **no** form of this command throws the following error:

```
% VPN id must be configured
```

You must configure a VPN ID before you can use a virtual forwarding interface (VFI).

Examples

The following examples show how to assign the VPN ID of 100 to a VFI named vfi1:

```
Device(config)# l2 vfi vfi2 autodiscovery
Device(config-vfi)# vpn id 100
```

vrf definition

To configure a virtual routing and forwarding (VRF) routing table instance and enter VRF configuration mode, use the **vrf definition** command in global configuration mode. To remove a VRF routing table, use the **no** form of this command.

vrf definition *vrf-name*
no vrf definition *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes

Global configuration (config)

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.
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.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.2S	This command was modified. Its use was expanded to support virtual networks.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Use the **vrf definition** command to give a VRF a name and to enter VRF configuration mode. Once the router is in VRF configuration mode, use the **rd** command to give the VRF a route distinguisher (RD). The **rd** command creates the routing and forwarding tables and associates the RD with the VRF instance named in the *vrf-name* argument.

Users can configure shared route targets (import and export) between IPv4 and IPv6. This feature is useful in a migration scenario, where IPv4 policies already are configured and IPv6 policies should be the same as the IPv4 policies. You can configure separate route-target policies for IPv4 and IPv6 VPNs in address family configuration mode. Enter address family configuration mode from VRF configuration mode.

In VRF configuration mode, you can also associate a Simple Network Management Protocol (SNMP) context with the named VRF and configure or update a VPN ID.

The **vrf definition default** command can be used to configure a VRF name that is a NULL value until a default VRF name can be configured. This is typically before any VRF-related AAA commands are configured.

Virtual Network Use of vrf definition Command

Use the **vrf definition** command to give a VRF a name and to enter VRF configuration mode. By default, each virtual network trunk interface on the router is able to carry traffic for every VRF defined by the **vrf definition** command. If you want to enable only a subset of VRFs on a trunk interface, use the **vrf list** command.

Note We recommend you do not define a virtual network with the name "global," because the system predefines **vnet global** and it is best to avoid conflict with the predefined version.

Examples

The following example assigns the name vrf1 to a VRF, enters VRF configuration mode, and configures a route distinguisher, 100:20:

```
Router(config)# vrf definition vrf1
Router(config-vrf)# rd 100:20
```

The following virtual network example defines VRF red, enters VRF configuration mode, and assigns virtual network tag 100 to VRF red:

```
Router(config)# vrf definition red
Router(config-vrf)# vnet tag 100
```

Related Commands

Command	Description
address-family (VRF)	Enters VRF address family configuration mode to select an address family type for a VRF table.
context	Associates an SNMP context with a particular VRF.
rd	Specifies a route distinguisher.
route-target	Creates a route-target extended community for a VPN VRF.
vnet	Configures overrides of an interface's attributes on a per-VRF basis
vnet tag	Assigns a tag to a virtual network.
vpn id	Sets or updates a VPN ID on a VRF.
vrf forwarding	Associates a VRF instance with an interface or subinterface.
vrf list	Defines a list of VRFs.

vrf forwarding

To associate a VRF instance or a virtual network with an interface or subinterface, use the **vrf forwarding** command in interface configuration mode. To disassociate a VRF or virtual network from an interface or subinterface, use the **no** form of this command.

vrf forwarding *vrf-name* [**downstream** *vrf-name2*]
no vrf forwarding

Syntax Description

vrf-name	The interface name to be associated with the specified VRF.
downstream	(Optional) Enables the half-duplex VRF (HDVRF) functionality on the interface and associates the interface with the downstream VRF.
vrf-name2	The interface name to be associated with the specified downstream VRF.

Command Default

The default for an interface is the global routing table.

Command Modes

Interface configuration (config-if)

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. The **downstream** *vrf-name2* keyword-argument pair was added to support Multiprotocol Label Switching (MPLS) HDVRFs.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.2S	This command was modified. Its use was expanded to support virtual networks.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Use the **tunnel vrf** command to associate tunnel interface with a VRF. Use the **vrf forwarding** command to associate any interface other than a tunnel interface, with a VRF. Use the **vrf definition** command in global configuration mode to configure a VRF routing table instance. When the interface is bound to a VRF, previously configured IPv4 and IPv6 addresses are removed, and they must be reconfigured.

The **downstream** keyword associates the interfaces with a downstream VRF, which enables the HDVRF functionality on the interface. Some functions operate in the upstream VRFs, and others operate in the downstream VRFs.

The following functions operate in the downstream VRFs:

- PPP peer routes are installed in the downstream VRFs.
- Authentication, authorization, and accounting (AAA) per-user routes are installed in the downstream VRFs.
- A Reverse Path Forwarding (RPF) check is performed in the downstream VRFs.

In the virtual network environment, the **vrf forwarding** command is supported on an edge interface; it is not supported on a trunk interface.

A VRF and a virtual network are mutually exclusive on an interface. In other words, an interface can be a VRF interface or a virtual network edge interface, but not both.

Examples

The following example shows how to associate a VRF named site1 to serial interface 0/0 and configure an IPv6 and an IPv4 address:

```
Device(config)# vrf definition site1
Device(config-vrf)# exit
Device(config)# interface Serial0/0
Device(config-if)# vrf forwarding site1
Device(config-if)# ipv6 address 2001:DB8:1:1000::72b/64
Device(config-if)# ip address 10.11.11.1 255.255.255.0
```

The following example shows how to associate the VRF named vrf1 with the virtual-template 1 interface and specify the downstream VRF named vrf2:

```
Device(config)# interface virtual-template 1
Device(config-if)# vrf forwarding vrf1 downstream vrf2
Device(config-if)# ip unnumbered Loopback1
```

The following example shows how to configure an edge interface:

```
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# vrf forwarding vrf2
Device(config-if)# ip address 10.12.12.1 255.255.255.0
```

Related Commands

Command	Description
vrf definition	Configures a VRF routing table instance.

vrf selection source

To populate a single source IP address, or range of source IP addresses, to a VRF Selection table, use the **vrf selection source** command in global configuration mode. To remove a single source IP address or range of source IP addresses from a VRF Selection table, use the **no** form of this command.

vrf selection source *source-IP-address source-IP-mask* **vrf** *vrf-name*
no vrf selection source *source-IP-address source-IP-mask* **vrf** *vrf-name*

Syntax Description

source-IP-address	New source IP address to be added to the VRF Selection table.
source-IP-mask	IP mask for the source IP address or range of single source IP addresses to be added to the VRF Selection table.
vrf *vrf-name*	Name of the VRF Selection table to which the single source IP address or range of source IP addresses should be added.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)SZ	This command was integrated into Cisco IOS Release 12.2(14)SZ to support the Cisco 7304 router.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S to support the Cisco 7304 router.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S to support the Cisco 7200 and 7500 series routers.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S to support the Cisco 7200 and 7500 series routers.
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.
12.2SX	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

If a VRF table is removed by using the **no ip vrf** *vrf-name* command in global configuration mode, all configurations associated with that VRF will be removed including those configurations added with the **vrf selection source** command.

Examples

The following example shows how to populate the VRF Selection table vpn1 with a source IP network address 10.0.0.0 and the IP mask 255.0.0.0, which would forward any packets with the source IP address 10.0.0.0 into the VRF instance vpn1:

```
Router(config)#
 vrf selection source 10.0.0.0 255.0.0.0 vrf vpn1
```

The following example shows the message you receive after you have removed the source IP network address 107.1.1.1 and the IP mask 255.255.255.255 from the VRF Selection table vpn1:

```
Router (config)# no vrf selection source 10.1.1.1 255.255.255.255 vrf vpn1
Router (config)#
VRF Selection Configuration: addr:10.1.1.1, mask:255.255.255.255, vrf_name:vpn1
5d13h: VRF Selection Remove Configuration: addr:10.1.1.1, mask: 255.255.255.255
Router (config)#
```

The following example shows the message you receive after you have added the source IP network address 10.1.1.1 and the IP mask 255.255.255.255 to the VRF Selection table vpn1:

```
Router (config)# vrf selection source 10.1.1.1 255.255.255.255 vrf vpn1
Router (config)#
VRF Selection Configuration: addr:10.1.1.1, mask:255.255.255.255, vrf_name:vpn1
VRF Selection: VRF table vpn1, id is: 1
```

Related Commands

Command	Description
ip vrf receive	Adds all the IP addresses that are associated with an interface into a VRF table.
ip vrf select source	Enables VRF Selection on an interface.

vrf upgrade-cli

To upgrade a Virtual Private Network (VPN) routing and forwarding (VRF) instance or all VRFs on the router to support multiple address families (multi-AFs) for the same VRF, use the **vrf upgrade-cli** command in global configuration mode. To remove the upgrade, use the **no** form of this command.

vrf upgrade-cli multi-af-mode {**common-policies** | **non-common-policies**} [**vrf** *vrf-name*]
no vrf upgrade-cli multi-af-mode {**common-policies** | **non-common-policies**} [**vrf** *vrf-name*]

Syntax Description

multi-af-mode	Specifies an upgrade of a single-protocol VRF or all VRFs to a multiprotocol VRF that supports multi-AFs configuration.
common-policies	Specifies to copy the route-target policies to the common part of the VRF configuration so that the policies apply to all address families configured in the multi-AF VRF.
non-common-policies	Specifies to copy the route-target policies to the IPv4 address family part of the VRF configuration so that the policies apply only to an IPv4 VRF.
vrf	(Optional) Specifies a VRF for the upgrade to a multi-AF VRF configuration.
vrf-name	(Optional) The name of the single-protocol VRF to upgrade to a multi-AF VRF configuration.

Command Default

If you do not enter the name of a specific single-protocol VRF, all VRFs defined on the router are upgraded to the multi-AF VRF configuration.

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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **vrf upgrade-cli** command is used to upgrade a specified single-protocol VRF (IPv4-only VRF) configuration or all single-protocol VRF configurations on the router to a multiprotocol VRF that supports multi-AF configuration.

The upgrade is automatic and does not require any further configuration. After you enter the **vrf upgrade-cli** command, the single-protocol VRF configuration is lost when you save the configuration to NVRAM. A multiprotocol VRF configuration is saved.

If your configuration requires that all route-target policies (import, export, both) apply to all address families, you enter the **vrf upgrade-cli multi-af-mode common-policies** command. If your configuration requires that these policies apply to IPv4 VPNs only, enter the **vrf upgrade-cli multi-af-mode non-common-policies** command.

After the upgrade to a multiprotocol VRF is complete, you can edit the VRF only with multiprotocol VRF configuration commands.

If you defined a VRF through the **vrf definition** command, have configured the IPv6 address-family type in that VRF, and you use the **no** form of this command, that part of the configuration will be lost. For example, if you have:

```
vrf definition foo
rd 1:1
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
```

And then you execute this command:

```
no vrf upgrade-cli multi-af-mode common-policies vrf foo
```

The configuration that remains is:

```
ip vrf foo
rd 1:1
```

If you configured *only* the IPv6 address-family type and you use the **no** form of this command, you lose the VRF because there is no IPv4 VRF, and the IPv6 VRF will not be left unchanged.

Examples

The following example shows how to upgrade a single-protocol VRF configuration named vrf1 to a multi-AF VRF configuration and apply the common policies of vrf1 to all address families defined for the VRF:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
!
Router(config)# vrf upgrade-cli multi-af-mode common-policies vrf vrf1
You are about to upgrade to the multi-AF VRF syntax commands.
You will lose any IPv6 address configured on interfaces
belonging to upgraded VRFs.
Are you sure ? [yes]: yes
Number of VRFs upgraded: 1

Router(config)# exit
```

The following is an example of the single-protocol VRF configuration for VRF vrf1 before you enter the **vrf upgrade-cli** command to upgrade to a multi-AF multiprotocol VRF configuration:

```
!
ip vrf vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
interface Loopback1
```

```
 ip vrf forwarding vrf1
 ip address 10.3.3.3 255.255.255.255
```

The following is an example of the multi-AF multiprotocol VRF configuration for VRF vrf1 after you enter the **vrf upgrade-cli common-policies** command:

```
!
vrf definition vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
 exit-address-family
!
interface Loopback1
 vrf forwarding vrf1
 ip address 10.3.3.3 255.255.255.255
```

Related Commands

Command	Description
show vrf	Displays the defined VRF instances.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.
vrf forwarding	Associates a VRF instance with an interface or subinterface.

xconnect

To bind an attachment circuit to a pseudowire, and to configure an Any Transport over MPLS (AToM) static pseudowire, use the **xconnect** command in one of the supported configuration modes. To restore the default values, use the **no** form of this command.

xconnect *peer-ip-address vc-id* {**encapsulation** {**l2tpv3** [{**manual**}] | **mpls** [{**manual**}]} | **pw-class** *pw-class-name*} [{**pw-class** *pw-class-name*}] [{**sequencing** {**transmit** | **receive** | **both**}}]
no xconnect

Cisco uBR10012 Router and Cisco uBR7200 Series Universal Broadband Routers
xconnect *peer-ip-address vc-id* **encapsulation mpls** [*pw-type*]
no xconnect *peer-ip-address vc-id* **encapsulation mpls** [*pw-type*]

Syntax Description

peer-ip-address	IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.
vc-id	The 32-bit identifier of the virtual circuit (VC) between the PE routers.
encapsulation	Specifies the tunneling method to encapsulate the data in the pseudowire: • **l2tpv3**--Specifies Layer 2 Tunneling Protocol, version 3 (L2TPv3), as the tunneling method. • **mpls**--Specifies Multiprotocol Label Switching (MPLS) as the tunneling method. • **manual**--(Optional) Specifies that no signaling is to be used in the attachment circuit. This keyword places the router in xconnect configuration mode for manual configuration of the attachment circuit. Use this keyword to manually configure an AToM or L2TPv3 static pseudowire.
pw-class *pw-class-name*	(Optional) Specifies the pseudowire class for advanced configuration.
sequencing	(Optional) Sets the sequencing method to be used for packets received or sent. This keyword is not supported with the AToM Static Pseudowire Provisioning feature.
transmit	Sequences data packets received from the attachment circuit.
receive	Sequences data packets sent into the attachment circuit.
both	Sequences data packets that are both sent and received from the attachment circuit.
pw-type	(Optional) Pseudowire type. You can specify one of the following types: • 4--Specifies Ethernet VLAN. • 5--Specifies Ethernet port.

Command Default

The attachment circuit is not bound to the pseudowire.

Command Modes

Connect configuration (config-conn)
Interface configuration (config-if)
ATM PVC l2transport configuration (cfg-if-atm-l2trans-pvc)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.0(28)S	Support was added for Multilink Frame Relay connections.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was updated to add support for AToM static pseudowires, and so that the remote router ID need not be the Label Distribution Protocol (LDP) router ID of the peer.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.
12.2(33)SXI5	This command was updated to add PFC3B or PFC3BXL restrictions for **xconnect**.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.1(2)S	This command was updated to allow IPv6 address configurations in the ethernet sub-interface when the **xconnect** command is configured under a service instance on the main interface. This change only applies to platforms that support the **service instance** command on ethernet interfaces.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The use of the **xconnect** command and the interface configuration mode bridge-group commands is not supported on the same physical interface.

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

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

The same *vcid* value that identifies the attachment circuit must be configured using the **xconnect** command on the local and remote PE router. The VC ID creates the binding between a pseudowire and an attachment circuit.

With the introduction of VPLS Autodiscovery in Cisco IOS Release 12.2(33)SRB, the remote router ID need not be the LDP router ID. The address you specify can be any IP address on the peer, as long as it is reachable. When VPLS Autodiscovery discovers peer routers for the VPLS, the peer router addresses might be any routable address.

Note The VPLS Autodiscovery feature is not supported with L2TPv3.

For L2TPv3, to manually configure the settings used in the attachment circuit, use the manual keyword in the **xconnect** command. This configuration is called a static session. The router is placed in xconnect configuration mode, and you can then configure the following options:

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

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

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

Software prior to Cisco IOS Release 12.2(33)SRB configured pseudowires dynamically using Label Distribution Protocol (LDP) or another directed control protocol to exchange the various parameters required for these connections. In environments that do not or cannot use directed control protocols, the **xconnect** command allows provisioning an AToM *static* pseudowire. Use the manual keyword in the **xconnect** command to place the router in xconnect configuration mode. MPLS pseudowire labels are configured using the **mpls label** and (optionally) **mpls control-word** commands in xconnect configuration mode.

The following restrictions apply only if EARL modes are either PFC3B or PFC3BXL and you are running Cisco IOS Release 12.2(33)SXI4 or later releases on your router:

- SPAN is not allowed on an inband port if any physical interface has **xconnect** configured.
- SPAN is not allowed on a physical interface that also has **xconnect** configured.
- If an inband port has SPAN configured, then configuring **xconnect** on any physical interface results in a warning message. You should not proceed with this configuration because it can create an infinite packet loop.
- If a physical port has SPAN configured and you add **xconnect** on that same interface, a warning message is displayed and we strongly recommend that you do not proceed with such a configuration.

Examples

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

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

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

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

The following example enters xconnect configuration mode and manually configures an AToM static pseudowire. The example shows the configuration for only one side of the connection; the configurations on each side of the connection must be symmetrical.

```
Device# configure terminal
Device(config)# interface Ethernet1/0
Device(config-if)# no ip address
Device(config-if)# xconnect 10.131.191.252 100 encapsulation mpls manual pw-class mpls
Device(config-if-xconn)# mpls label 100 150
Device(config-if-xconn)# exit
Device(config-if)# exit
```

The following example shows how to bind an attachment circuit to a pseudowire and configure an AToM service on a Cisco uBR10012 router:

```
Device# configure terminal
Device(config)# cable l2vpn 0000.396e.6a68 customer1
Device(config-l2vpn)# service instance 2000 Ethernet
Device(config-ethsrv)# xconnect 101.1.0.2 221 encapsulation mpls pw-type 4
```

Related Commands

Command	Description
l2tp cookie local	Configures the size of the cookie field used in the L2TPv3 headers of incoming packets received from the remote PE peer router.
l2tp cookie remote	Configures the size of the cookie field used in the L2TPv3 headers of outgoing packets sent from the local PE peer router.
l2tp hello	Specifies the use of a hello keepalive setting contained in a specified L2TP class configuration for a static L2TPv3 session.
l2tp id	Configures the identifiers used by the local and remote provider edge routers at each end of an L2TPv3 session.
l2tp class	Configures a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes.
mpls control-word	Enables the MPLS control word in an AToM static pseudowire connection.
mpls label	Configures an AToM static pseudowire connection by defining local and remote pseudowire labels.

Command	Description
mpls label range	Configures the range of local labels available for use on packet interfaces.
pseudowire-class	Configures a template of pseudowire configuration settings used by the attachment circuits transported over a pseudowire.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

xconnect logging pseudowire status

To enable system logging (syslog) reporting of pseudowire status events, use the **xconnect logging pseudowire status** command in global configuration mode. To disable syslog reporting of pseudowire status events, use the **no** form of this command.

xconnect logging pseudowire status
no xconnect logging pseudowire status

Syntax Description

This command has no arguments or keywords.

Command Default

Syslog reporting of pseudowire status events is off.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example enables syslog reporting of pseudowire status events:

```
Router# configure terminal
Router(config)# xconnect logging pseudowire status
```

Related Commands

Command	Description
xconnect	Binds an Ethernet, 802.1q VLAN, or Frame Relay attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.