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.