

neighbor activate

To enable the exchange of information with a Border Gateway Protocol (BGP) neighbor, use the **neighbor activate** command in address family configuration mode or router configuration mode. To disable the exchange of an address with a BGP neighbor, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**

Syntax Description

<i>ip-address</i>	IP address of the neighboring router.
<i>peer-group-name</i>	Name of BGP peer group.
<i>ipv6-address</i>	IPv6 address of the BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Defaults

The exchange of addresses with BGP neighbors is enabled for the IPv4 address family. Enabling address exchange for all other address families is disabled.



Note

Address exchange for address family IPv4 is enabled by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-activate** command before configuring the **neighbor remote-as** command, or you disable address exchange for address family IPv4 with a specific neighbor by using the **no** form of the **neighbor activate** command.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	Support for address family configuration mode and the IPv4 address family were added.
12.2(2)T	The <i>ipv6-address</i> argument and support for the IPv6 address family were added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

Use this command to advertise address information in the form of an IP or IPv6 prefix. The address prefix information is known as Network Layer Reachability Information (NLRI) in BGP.

Examples**Address Exchange Example for Address Family vpnv4**

The following example shows how to enable address exchange for address family vpnv4 for all neighbors in the BGP peer group named PEPEER and for the neighbor 144.0.0.44:

```
Router(config)# address-family vpnv4
Router(config-router-af)# neighbor PEPEER activate
Router(config-router-af)# neighbor 144.0.0.44 activate
Router(config-router-af)# exit-address-family
```

Address Exchange Example for Address Family IPv4 unicast

The following example shows how to enable address exchange for address family IPv4 unicast for all neighbors in the BGP peer group named group1 and for the BGP neighbor 172.16.1.1:

```
Router(config)# address-family ipv4 unicast
Router(config-router-af)# neighbor group1 activate
Router(config-router-af)# neighbor 172.16.1.1 activate
```

Address Exchange Example for Address Family IPv6

The following example shows how to enable address exchange for address family IPv6 for all neighbors in the BGP peer group named group2 and for the BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group2 activate
Router(config-router-af)# neighbor 7000::2 activate
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
exit-address-family	Exits from the address family submode.

neighbor allowas-in

To configure provider edge (PE) routers to allow readvertisement of all prefixes containing duplicate autonomous system numbers (ASNs), use the **neighbor allowas-in** command in router configuration mode. To disable the readvertisement of the ASN of the PE router, use the **no** form of this command.

```
neighbor ip-address allowas-in [number]
```

```
no neighbor ip-address allowas-in [number]
```

Syntax Description		
	<i>ip-address</i>	IP address of the neighboring router.
	<i>number</i>	(Optional) Specifies the number of times to allow the advertisement of a PE router's ASN. Valid values are from 1 to 10. If no number is supplied, the default value of 3 times is used

Defaults Readvertisement of all prefixes containing duplicate ASNs is disabled by default.

Command Modes Router configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced.
	12.1	This command was integrated into Cisco IOS Release 12.1.
	12.2	This command was integrated into Cisco IOS Release 12.2.
	12.3T	This command was integrated into Cisco IOS Release 12.3T.

Usage Guidelines In a hub and spoke configuration, a PE router readvertises all prefixes containing duplicate autonomous system numbers. Use the **neighbor allowas-in** command to configure two VRFs on each PE router to receive and readvertise prefixes as follows:

- One Virtual Private Network routing and forwarding (VRF) instance receives prefixes with ASNs from all PE routers and then advertises them to neighboring PE routers.
- The other VRF receives prefixes with ASNs from the customer edge (CE) router and readvertises them to all PE routers in the hub and spoke configuration.

You control the number of times an ASN is advertised by specifying a number from 1 to 10.

Examples The following example shows how to configure the PE router with ASN 100 to allow prefixes from the VRF address family Virtual Private Network (VPN) IPv4 vrf1. The neighboring PE router with the IP address 192.168.255.255 is set to be readvertised to other PE routers with the same ASN six times.

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf vrf1
Router(config-router)# neighbor 192.168.255.255 allowas-in 6
```

Related Commands

Command	Description
address-family	Enters the address family configuration submode used to configure routing protocols such as BGP, OSPF, RIP, and static routing.

neighbor as-override

To configure a provider edge (PE) router to override the autonomous system number (ASN) of a site with the ASN of a provider, use the **neighbor as-override** command in router configuration mode. To remove Virtual Private Network (VPN) IPv4 prefixes from a specified router, use the **no** form of this command.

neighbor ip-address as-override

no neighbor ip-address as-override

Syntax Description	<i>ip-address</i>	Specifies the IP address of the router that is to be overridden with the ASN provided.
---------------------------	-------------------	--

Defaults	Automatic override of the ASN is disabled.
-----------------	--

Command Modes	Router configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(7)T	This command was introduced.

Usage Guidelines	This command is used in conjunction with the site-of-origin feature, identifying the site where a route originated, and preventing routing loops between routers within a VPN.
-------------------------	--

Examples	The following example shows how to configure a router to override the ASN of a site with the ASN of a provider:
-----------------	---

```
Router(config)# router bgp 100
Router(config-router)# neighbor 192.168.255.255 remote-as 109
Router(config-router)# neighbor 192.168.255.255 update-source loopback0
Router(config-router)# address-family ipv4 vrf vpn1
Router(config-router)# neighbor 192.168.255.255 activate
Router(config-router)# neighbor 192.168.255.255 as-override
```

Related Commands	Command	Description
	neighbor activate	Enables the exchange of information with a BGP neighboring router.
	neighbor remote-as	Allows a neighboring router's IP address to be included in the BGP routing table.
	neighbor update-source	Allows internal BGP sessions to use any operational interface for TCP/IP connections.
	route-map	Redistributes routes from one routing protocol to another.

neighbor send-label

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with BGP routes to a neighboring BGP router, use the **neighbor send-label** command in address family configuration mode or router configuration mode. To disable this feature, use the **no** form of this command.

neighbor ip-address send-label

no neighbor ip-address send-label

Syntax Description	<i>ip-address</i>	IP address of the neighboring router.
---------------------------	-------------------	---------------------------------------

Defaults BGP routers distribute only BGP routes.

Command Modes Address family configuration
Router configuration

Command History	Release	Modification
	12.0(21)ST	This command was introduced.
	12.0(22)S	Support for IPv6 was added.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines This command enables a router to use BGP to distribute MPLS labels along with the IPv4 routes to a peer router. You must issue this command on both the local router and the neighboring router.

This command has the following restrictions:

- If a BGP session is running when you issue the **neighbor send-label** command, the command does not take effect until the BGP session is restarted.
- In router configuration mode, only IPv4 addresses are distributed.

Use this command in IPv6 address family configuration mode to bind and advertise IPv6 prefix MPLS labels. Using this command in conjunction with the **mpls ipv6 source-interface** global configuration command allows IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers configured to run both IPv4 and IPv6 forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).

Examples The following example shows how to enable a router in the autonomous system 65000 to send MPLS labels with BGP routes to the neighbor BGP router at 192.168.0.1:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.0.1 remote-as 65001
Router(config-router)# neighbor 192.168.0.1 send-label
```

The following example shows how to enable a router in the autonomous system 65000 to bind and advertise IPv6 prefix MPLS labels and send the labels with BGP routes to the neighbor BGP router at 192.168.99.70:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.99.70 remote-as 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# neighbor 192.168.99.70 activate
Router(config-router-af)# neighbor 192.168.99.70 send-label
```

Related Commands

Command	Description
mpls ipv6 source-interface	Specifies the IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over a network running MPLS.
neighbor activate	Enables the exchange of information with a neighboring router.

next-address

To specify the next IP address in the explicit path, use the **next-address** command in IP explicit path configuration mode. To remove the specified next IP address in the explicit path, use the **no** form of this command.

```
next-address A.B.C.D
```

```
no next-address A.B.C.D
```

Syntax Description

<i>A.B.C.D</i>	Next IP address in the explicit path.
----------------	---------------------------------------

Defaults

Next IP address in the explicit path is not specified.

Command Modes

IP explicit path configuration

Command History

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

Examples

The following example shows how to assign the number 60 to the IP explicit path, enable the path, and specify 10.3.27.3 as the next IP address in the list of IP addresses:

```
Router(config)# ip explicit-path identifier 60 enable
Router(cfg-ip-expl-path)# next-address 10.3.27.3
```

```
Explicit Path identifier 60:
  1: next-address 10.3.27.3
Router(cfg-ip-expl-path)#
```

Related Commands

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

oam retry

To configure parameters related to Operation, Administration, and Maintenance (OAM) management for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), VC class, or VC bundle, or label-controlled ATM (LC-ATM) VC, use the **oam retry** command in the appropriate command mode. To remove OAM management parameters, use the **no** form of this command.

oam retry *up-count down-count retry-frequency*

no oam retry

Syntax Description		
	<i>up-count</i>	Number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a connection state to up. This argument does not apply to SVCs.
	<i>down-count</i>	Number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to change the state to down or tear down an SVC connection.
	<i>retry-frequency</i>	The frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up/down state is being verified. For example, if a PVC is up and a loopback cell response is not received after the <i>frequency</i> (in seconds) argument is specified using the oam-pvc command, loopback cells are sent at the <i>retry-frequency</i> to verify whether the PVC is down.

Defaults

ATM PVCs and SVCs

up-count: 3
down-count: 5
retry-frequency: 1 second

LC-ATM VCs

up-count: 2
down-count: 2
retry-frequency: 2 seconds

Command Modes

Interface-ATM-VC configuration (for an ATM PVC or SVC)
VC-class configuration (for a VC class)
Bundle configuration mode (for a VC bundle)
PVC range configuration (for an ATM PVC range)
PVC-in-range configuration (for an individual PVC within a PVC range)
Control-VC configuration (for an LC-ATM VC)

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(3)T	This command was modified to allow configuration parameters related to OAM management for ATM VC bundles.

Release	Modification
12.1(5)T	This command was implemented in PVC range and PVC-in-range configuration modes.
12.3(2)T	This command was implemented in control-VC configuration mode.

Usage Guidelines

The following guidelines apply to PVCs, SVCs, and VC classes. They do not apply to LC-ATM VCs.

- For ATM PVCs, SVCs, or VC bundles, if the **oam retry** command is not explicitly configured, the VC inherits the following default configuration (listed in order of precedence):
 - Configuration of the **oam retry** command in a VC class assigned to the PVC or SVC itself.
 - Configuration of the **oam retry** command in a VC class assigned to the PVC's or SVC's ATM subinterface.
 - Configuration of the **oam retry** command in a VC class assigned to the PVC's or SVC's ATM main interface.
 - Global default: *up-count* = 3, *down-count* = 5, *retry-frequency* = 1 second. This set of defaults assumes that OAM management is enabled using the **oam-pvc** or **oam-svc** command. The *up-count* and *retry-frequency* arguments do not apply to SVCs.
- To use this command in bundle configuration mode, enter the bundle command to create the bundle or to specify an existing bundle before you enter this command.
- If you use the **oam retry** command to configure a VC bundle, you configure all VC members of that bundle. VCs in a VC bundle are further subject to the following inheritance rules (listed in order of precedence):
 - VC configuration in bundle-vc mode
 - Bundle configuration in bundle mode (with the effect of assigned VC-class configuration)
 - Subinterface configuration in subinterface mode

Examples

The following example shows how to configure the OAM management parameters with an up count of 3, a down-count of 3, and the retry frequency set at 10 seconds:

```
Router(cfg-mpls-atm-cvc)# oam retry 3 3 10
```

Related Commands

Command	Description
broadcast	Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle.
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
encapsulation	Sets the encapsulation method used by the interface.
inarp	Configures the Inverse ARP time period for an ATM PVC, VC class, or VC bundle.
oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for a virtual circuit class that can be applied to a virtual circuit bundle.

Command	Description
oam-pvc	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM PVC or virtual circuit class.
oam-svc	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM SVC or virtual circuit class.
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.

oam-ac emulation-enable

To enable Operation, Administration, and Maintenance (OAM) cell emulation on ATM adaptation layer 5 (AAL5) over Multiprotocol Label Switching (MPLS), use the **oam-ac emulation-enable** command in the appropriate configuration mode on both provider edge (PE) routers. To disable OAM cell emulation, use the **no** form of this command on both routers.

oam-ac emulation-enable [*ais-rate*]

no oam-ac emulation-enable [*ais-rate*]

Syntax Description

<i>ais-rate</i>	(Optional) The rate (in seconds) at which the alarm indication signal (AIS) cells should be sent. The range is 0 to 60 seconds. If you specify 0, no AIS cells are sent. The default is 1 second, which means that one AIS cell is sent every second.
-----------------	---

Defaults

OAM cell emulation is disabled. If you enable OAM cell emulation without specifying an AIS rate, the default is to send one AIS cell every second.

Command Modes

L2transport VC configuration mode for an ATM PVC
 VC class configuration mode for a VC class

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(30)S	This command was updated to enable OAM cell emulation as part of a VC class.

Usage Guidelines

This command is only applicable to AAL5 over MPLS and is not supported with ATM Cell Relay over MPLS.

Examples

The following example shows how to enable OAM cell emulation on an ATM PVC:

```
Router# interface ATM 1/0/0
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable
```

The following example shows how to set the rate at which an AIS cell is sent to every 30 seconds:

```
Router# interface ATM 1/0/0
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable 30
```

The following example configures OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to an interface.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm oamclass
Router(config-vc-class)# encapsulation aal5
Router(config-vc-class)# oam-ac emulation-enable 30
Router(config-vc-class)# oam-pvc manage
Router(config)# interface atm1/0
Router(config-if)# class-int oamclass
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 13.13.13.13 100 encapsulation mpls
```

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.

oam-pvc

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM permanent virtual circuit (PVC), virtual circuit (VC) class, or label-controlled ATM (LC-ATM) VC, use the **oam-pvc** command in the appropriate command mode. To disable generation of OAM loopback cells and OAM management, use the **no** form of this command.

ATM VC or VC Class

oam-pvc [**manage**] [*frequency*]

no oam-pvc [**manage**]

LC-ATM VC

oam-pvc manage [*frequency*]

no oam-pvc manage

Loopback Mode Detection

oam-pvc manage [*frequency*] **loop-detection**

no oam-pvc manage loop-detection

Syntax Description	
manage	(Optional for ATM VCs or VC classes; required for LC-ATM VCs) Enables OAM management. The default is disabled.
<i>frequency</i>	(Optional) Time delay between transmitting OAM loopback cells. For ATM VCs or VC classes and loopback mode detection, the range of values is from 0 to 600 seconds. The default is 10 seconds. For LC-ATM VCs, the range of values is from 0 to 255 seconds. The default is 5 seconds.
loop-detection	Enables automatic detection of whether the physically connected ATM switch is in loopback mode. The default is disabled.

Command Default Disabled.

Command Modes Interface-ATM-VC configuration (for an ATM PVC or Loopback Mode Detection)
 VC-class configuration (for a VC class)
 PVC-in-range configuration (for an individual PVC within a PVC range)
 Control-VC configuration (for enabling OAM management on an LC-ATM VC)

Command History	Release	Modification
	11.3	This command was introduced.
	12.1(5)T	This command was implemented in PVC-in-range configuration mode.

Release	Modification
12.3(2)T	This command was implemented for LC-ATM VCs.
12.0(30)S	The loop-detection keyword was added.

Usage Guidelines

If OAM management is enabled, further control of OAM management is configured using the **oam retry** command.

ATM VCS or VC Classes

If the **oam-pvc** command is not explicitly configured on an ATM PVC, the PVC inherits the following default configuration (listed in order of precedence):

- Configuration of the **oam-pvc** command in a VC class assigned to the PVC itself.
- Configuration of the **oam-pvc** command in a VC class assigned to the PVC's ATM subinterface.
- Configuration of the **oam-pvc** command in a VC class assigned to the PVC's ATM main interface.
- Global default: End-to-end F5 OAM loopback cell generation and OAM management are disabled, but if OAM cells are received, they are looped back. The default value for the *frequency* argument is 10 seconds.

Loopback Mode Detection

When a PVC traverses an ATM cloud and OAM is enabled, the router sends a loopback cell to the other end and waits for a response to determine whether the circuit is up. If an intervening router within the ATM cloud is in loopback mode, however, the router considers the circuit to be up, when in fact the other end is not reachable.

When enabled, the Loopback Mode Detection Through OAM feature detects when an intervening router is in loopback mode, in which case it sets the OAM state to NOT_VERIFIED. This prevents traffic from being routed on the PVC for as long as any intervening router is detected as being in loopback mode.

Examples

The following example shows how to enable end-to-end F5 OAM loopback cell transmission and OAM management on an ATM PVC with a transmission frequency of 3 seconds:

```
Router(cfg-mpls-atm-cvc)# oam-pvc manage 3
```

The following example shows how to enable end-to-end F5 OAM loopback cell transmission and OAM management on an LC-ATM interface with a transmission frequency of 2 seconds:

```
Router(config)# interface Switch1.10 mpls
Router(config-subif)# ip unnumbered Loopback0
Router(config-subif)# mpls atm control-vc 0 32
Router(cfg-mpls-atm-cvc)# oam-pvc manage 2
```

The following example shows how to create a PVC and enable loopback detection:

```
Router(config)# interface ATM1/0
Router(config-if)# pvc 4/100
Router(config-if-atm-vc)# oam-pvc manage loop-detection
```

Related Commands

Command	Description
ilmi manage	Enables ILMI management on an ATM PVC.
oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or LC-ATM VC.
show atm pvc	Displays all ATM PVCs and traffic information.

pseudowire

To bind an attachment circuit to a Layer 2 pseudowire for xconnect service, use the **pseudowire** command in interface configuration mode.

```
pseudowire peer-ip-address vcid pw-class pw-class-name [sequencing { transmit | receive | both }]
```

Syntax Description		
<i>peer-ip-address</i>		The IP address of the remote peer.
<i>vcid</i>		The 32-bit identifier of the virtual circuit between the routers at each end of the Layer 2 control channel.
pw-class <i>pw-class-name</i>		The pseudowire class configuration from which the data encapsulation type will be taken.
sequencing { transmit receive both }	(Optional)	Sets the sequencing method to be used for packets received or sent in L2TP sessions: <ul style="list-style-type: none"> • transmit—Sequencing of Layer 2 Tunnel Protocol (L2TP) data packets received from the session. • receive—Sequencing of L2TP data packets sent into the session. • both—Sequencing of L2TP data packets that are both sent and received from the session.

Defaults No default behavior or values

Command Modes Interface configuration

Command History	Release	Modification
	12.3(2)T	This command was introduced.

Usage Guidelines

The combination of the *peer-ip-address* and *vcid* arguments must be unique on the router. Each pseudowire configuration must have a unique combination of *peer-ip-address* and *vcid* configuration. The same *vcid* value that identifies the attachment circuit must be configured using the **pseudowire** command on the local and remote router at each end of a Layer 2 session. The virtual circuit identifier creates the binding between a pseudowire and an attachment circuit.

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

Examples

The following example creates a virtual-PPP interface with the number 1, configures PPP on the virtual-PPP interface, and binds the attachment circuit to a Layer 2 pseudowire for xconnect service for the pseudowire class named pwclass1:

```
interface virtual-ppp 1
  ppp authentication chap
  ppp chap hostname peer1
  pseudowire 172.24.13.196 10 pw-class pwclass1
```

Related Commands

Command	Description
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

pseudowire-class

To specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode, use the **pseudowire-class** command in global configuration mode.

```
pseudowire-class [pw-class-name]
```

Syntax Description

<i>pw-class-name</i>	(Optional) The name of a Layer 2 pseudowire class. If you want to configure more than one pseudowire class, you must enter a value for the <i>pw-class-name</i> argument.
----------------------	---

Defaults

No pseudowire class is defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **pseudowire-class** command allows you to configure a pseudowire class template that consists of configuration settings used by all attachment circuits bound to the class. A pseudowire class includes the following configuration settings:

- Data encapsulation type
- Control protocol
- Sequencing
- IP address of the local Layer 2 interface
- Type of service (ToS) value in IP headers

After you enter the **pseudowire-class** command, the router switches to pseudowire class configuration mode, where pseudowire settings may be configured.

Examples

The following example shows how to enter pseudowire class configuration mode to configure a pseudowire configuration template named "ether-pw":

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)#
```

Related Commands	Command	Description
	l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.
	pseudowire	Binds an attachment circuit to a Layer 2 pseudowire for xconnect service.
	xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

rd

To create routing and forwarding tables for a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **rd** command in VRF configuration mode.

rd *route-distinguisher*

Syntax Description	<i>route-distinguisher</i>	Adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix.
---------------------------	----------------------------	---

Defaults There is no default. A route distinguisher (RD) must be configured for a VRF to be functional.

Command Modes VRF configuration

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

Usage Guidelines An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

Either RD is an ASN-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

16-bit AS number: your 32-bit number
For example, 101:3.

32-bit IP address: your 16-bit number
For example, 192.168.122.15:1.

Examples The following example shows how to configure a default RD for two VRFs. It illustrates the use of both AS-relative and IP-address-relative RDs:

```
Router(config)# ip vrf vrf_blue
Router(config-vrf)# rd 100:3
Router (config-vrf)# exit
Router(config)# ip vrf vrf_red
Router(config-vrf)# rd 173.13.0.12:200
```

Related Commands	Command	Description
	ip vrf	Configures a VRF routing table.
	show ip vrf	Displays the set of defined VRFs and associated interfaces.

route-target

To create a route-target extended community for a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **route-target** command in VRF configuration mode. To disable the configuration of a route-target community option, use the **no** form of this command.

route-target {**import** | **export** | **both**} *route-target-ext-community*

no route-target {**import** | **export** | **both**} *route-target-ext-community*

Syntax Description

import	Imports routing information from the target VPN extended community.
export	Exports routing information to the target VPN extended community.
both	Imports both import and export routing information to the target VPN extended community.
<i>route-target-ext-community</i>	Adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.

Defaults

There are no defaults. A VRF has no route-target extended community attributes associated with it until specified by the **route-target** command.

Command Modes

VRF configuration

Command History

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

Usage Guidelines

The **route-target** command creates lists of import and export route-target extended communities for the specified VRF. Enter the command one time for each target community. Learned routes that carry a specific route-target extended community are imported into all VRFs configured with that extended community as an import route target. Routes learned from a VRF site (for example, by Border Gateway Protocol (BGP), Routing Information Protocol (RIP), or static route configuration) contain export route targets for extended communities configured for the VRF added as route attributes to control the VRFs into which the route is imported.

The route target specifies a target VPN extended community. Like a route-distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number. You can enter the numbers in either of these formats:

16-bit AS number:your 32-bit number

For example, 101:3.

32-bit IP address:your 16-bit number

For example, 192.168.122.15: 1.

Examples

The following example shows how to configure route-target extended community attributes for a VRF. The result of the command sequence is that VRF named *vrf_blue* has two export extended communities (1000:1 and 1000:2) and two import extended communities (1000:1 and 173.27.0.130:200).

```
Router(config)# ip vrf vrf_blue
Router(config-vrf)# route-target both 1000:1
Router(config-vrf)# route-target export 1000:2
Router(config-vrf)# route-target import 173.27.0.130:200
```

Related Commands

Command	Description
import map	Configures an import route map for a VRF.
ip vrf	Configures a VRF routing table.

sequencing

To configure the direction in which sequencing is enabled for data packets in a Layer 2 pseudowire, use the **sequencing** command in pseudowire class configuration mode. To remove the sequencing configuration from the pseudowire class, use the **no** form of this command.

```
sequencing {transmit | receive | both | resync {number}}
```

```
no sequencing {transmit | receive | both | resync {number}}
```

Syntax Description

transmit	Updates the Sequence Number field in the headers of data packets sent over the pseudowire according to the data encapsulation method that is used.
receive	Keeps the value in the Sequence Number field in the headers of data packets received over the pseudowire. Out-of-order packets are dropped.
both	Enables both the transmit and receive options.
resync	Enables the reset of packet sequencing after the disposition router receives a specified number of out-of-order packets.
<i>number</i>	The number of out-of-order packets that cause a reset of packet sequencing. The range is 5 to 65535.

Defaults

Sequencing is disabled.

Command Modes

Pseudowire class configuration

Command History

Release	Modification
12.0(23)S	This command was introduced for Layer 2 Tunnel Protocol Version 3 (L2TPv3).
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.0(29)S	This command was updated to support Any Transport over MPLS (AToM).
12.0(30)S	The resync keyword was added.

Usage Guidelines

- When you enable sequencing using any of the available options, the sending of sequence numbers is automatically enabled and the remote provider edge (PE) peer is requested to send sequence numbers. Out-of-order packets received on the pseudowire are dropped only if you use the **sequencing receive** or **sequencing both** command.
- If sequencing is enabled for Layer 2 pseudowires on the Cisco 7500 series, all traffic on the pseudowires is switched through the Route Switch Processor (RSP) regardless of the setting configured with the **ip cef distributed** command.
- It is useful to specify the **resync** keyword for situations when the disposition router receives many out-of-order packets. It allows the router to recover from situations where too many out-of-order packets are dropped.

- Set the sequence number to 0 in the slow path before packets are punted to the local CPU, because packets may become out of order.

Examples

The following example shows how to enable sequencing in data packets in Layer 2 pseudowires that were created from the pseudowire class named “ether-pw” so that the Sequence Number field is updated in tunneled packet headers for data packets that are both sent and received over the pseudowire:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# encapsulation mpls
Router(config-pw)# sequencing both
```

The following example shows how to enable the disposition router to reset packet sequencing after it receives 1000 out-of-order packets:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# encapsulation mpls
Router(config-pw)# sequencing both
Router(config-pw)# sequencing resync 1000
```

Related Commands

Command	Description
ip cef	Enables CEF on the Route Processor card.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

set mpls experimental imposition

To set the value of the Multiprotocol Label Switching (MPLS) experimental (EXP) field on all imposed label entries, use the **set mpls experimental imposition** command in QoS policy-map class configuration mode. To disable the setting, use the **no** form of this command.

```
set mpls experimental imposition {mpls-exp-value | from-field [table table-map-name]}
```

```
no set mpls experimental imposition {mpls-exp-value | from-field [table table-map-name]}
```

Syntax Description		
<i>mpls-exp-value</i>		Specifies the value used to set MPLS EXP bits defined by the policy map. Valid values are numbers from 0 to 7.
<i>from-field</i>		Specific packet-marking category to be used to set the MPLS EXP imposition value. If you are using a table map for mapping and converting packet-marking values, this establishes the “map from” packet-marking category. Packet-marking category keywords are as follows: <ul style="list-style-type: none"> • precedence • dscp
table		(Optional) Used in conjunction with the <i>from-field</i> argument. Indicates that the values set in a specified table map will be used to set the MPLS EXP imposition value.
<i>table-map-name</i>		(Optional) Used in conjunction with the table keyword. Name of the table map used to specify the MPLS EXP imposition value. The name can be a maximum of 64 alphanumeric characters.

Defaults No MPLS EXP value is set.

Command Modes QoS policy-map class configuration

Command History	Release	Modification
	12.2(13)T	This command replaces (renames) the set mpls experimental command, introduced in 12.1(5)T. The set mpls experimental imposition command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.

Usage Guidelines The **set mpls experimental imposition** command is supported only on input interfaces. Use this command during label imposition. This command sets the MPLS EXP field on all imposed label entries.

Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the class of service (CoS) value. The “from-field” packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the “from-field” category as the MPLS EXP imposition value. For instance, if you configure the **set mpls experimental imposition precedence** command, the precedence value will be copied and used as the MPLS EXP imposition value.

You can configure the **set mpls experimental imposition dscp** command, and the DSCP value will be copied and used as the MPLS EXP imposition value.



Note

If you configure the **set mpls experimental imposition dscp** command, only the *first three bits* (the class selector bits) of the DSCP field are used.

Examples

The following example shows how to set the MPLS EXP value to 3 on all imposed label entries:

```
Router(config-pmap)# set mpls experimental imposition 3
```

The following example shows how to create the policy map named policy1 to use the packet-marking values defined in a table map named table-map1. The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

The following example sets the MPLS EXP imposition value according to the DSCP value defined in table-map1.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set mpls experimental imposition dscp table table-map1
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
set dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
set mpls experimental topmost	Sets the MPLS EXP field value in the topmost label on either an input or an output interface.
set precedence	Sets the precedence value in the packet header.
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set mpls experimental topmost

To set the Multiprotocol Label Switching (MPLS) experimental (EXP) field value in the topmost label on either an input or an output interface, use the **set mpls experimental topmost** command in QoS policy-map class configuration mode. To disable the setting, use the **no** form of this command.

```
set mpls experimental topmost {mpls-exp-value | qos-group [table table-map-name]}
```

```
no set mpls experimental topmost {mpls-exp-value | qos-group [table table-map-name]}
```

Syntax Description		
<i>mpls-exp-value</i>		Specifies the value used to set MPLS experimental bits defined by the policy map. Valid values are numbers from 0 to 7.
qos-group		Specifies that the qos-group packet-marking category is used to set the MPLS EXP imposition value. If you are using a table map for mapping and converting packet-marking values, this establishes the “map from” packet-marking category.
table		(Optional) Used in conjunction with the qos-group keyword. Indicates that the values set in a specified table map will be used to set the MPLS EXP value.
<i>table-map-name</i>		(Optional) Used in conjunction with the table keyword. Name of the table map used to specify the MPLS EXP value. The name can be a maximum of 64 alphanumeric characters.

Defaults No MPLS EXP value is set.

Command Modes QoS policy-map class configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines This command sets the MPLS EXP value only in the topmost label. This command does not affect an IP packet. The MPLS field in the topmost label header is not changed.

Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the qos-group packet-marking category to be used for mapping and setting the differentiated services code point (DSCP) value.

If you specify the qos-group category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the qos-group category as the MPLS EXP topmost value. For instance, if you configure the **set mpls experimental topmost qos-group** command, the QoS group value will be copied and used as the MPLS EXP topmost value.

The valid value range for the MPLS EXP topmost value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set mpls experimental topmost qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 6), the packet-marking value will be copied and the packets will be marked.
- If a QoS group value exceeds the MPLS EXP topmost range (for example, 10), the packet-marking value will not be copied and the packet will not be marked. No action is taken.

Examples

The following example shows how to set the MPLS EXP value to 3 in the topmost label of an input or output interface:

```
Router(config-pmap)# set mpls experimental topmost 3
```

The following example shows how to create the policy map named policy1 to use the packet-marking values defined in a table map named table-map1. The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the table-map (value mapping) command page.

The following example shows how to set the MPLS EXP value according to the QoS group value defined in table-map1.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set mpls experimental topmost qos-group table table-map1
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
match mpls experimental topmost	Matches the MPLS EXP field value in the topmost label.
set mpls experimental imposition	Sets the value of the MPLS EXP field on all imposed label entries.
set qos-group	Sets a group ID that can be used later to classify packets.
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set mpls-label

To enable a route to be distributed with a Multiprotocol Label Switching (MPLS) label if the route matches the conditions specified in the route map, use the **set mpls-label** command in route map configuration mode. To disable this function, use the **no** form of this command.

set mpls-label

no set mpls-label

Syntax Description This command has no arguments or keywords.

Defaults No route with an MPLS label is distributed.

Command Modes Route map configuration

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

Usage Guidelines This command can be used only with the **neighbor route-map out** command to manage outbound route maps for a Border Gateway Protocol (BGP) session.

Use the **route-map** global configuration command with **match** and **set route-map** configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Examples The following example shows how to create a route map that enables the route to be distributed with a label if the IP address of the route matches an IP address in ACL 1.

```
Router(config-router)# route-map incoming permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set mpls-label
```

Related Commands	Command	Description
	match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
	match mpls-label	Redistributes routes that contain MPLS labels and match the conditions specified in the route map.
	route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set ospf router-id

To set a separate Open Shortest Path First (OSPF) router ID for each interface or subinterface on a provider edge (PE) router for each directly attached customer edge (CE) router, use the **set ospf router-id** command in route map configuration mode.

set ospf router-id

Syntax Description This command has no arguments or keywords.

Defaults OSPF router ID is not set.

Command Modes Route map configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced.

Usage Guidelines To use this command, you must enable OSPF and create a routing process.

Examples The following example shows how to match the PE router IP address 192.168.0.0 against the interface in access list 1 and set to the OSPF router ID:

```
router ospf 2 vrfvpn1-site1
 redistribute bgp 100 metric-type 1 subnets
 network 202.0.0.0 0.0.0.255 area 1

router bgp 100
 neighbor 172.19.89. 62 remote-as 100
 access-list 1 permit 192.168.0.0
 route-map vpn1-site1-map permit 10
 match ip address 1
 set ospf router-id
```

Related Commands	Command	Description
	router ospf	Enables OSPF routing, which places the router in router configuration mode.

set vrf

To enable Virtual Private Network (VPN) routing/forwarding instance (VRF) selection within a route map for policy-based routing VRF selection, use the **set vrf** command in route-map configuration mode. To disable VRF selection within a route map, use the **no** form of this command.

set vrf *vrf-name*

no set vrf *vrf-name*

Syntax Description

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

Defaults

No default behavior or values

Command Modes

Route-map configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

The **set vrf** route-map configuration command was introduced with the *MPLS VPN—VRF Selection using Policy Based Routing* feature to provide a PBR mechanism for VRF selection. This command is used to enable VRF selection by policy routing packets through a route map. The route map is attached to the incoming interface. Match criteria is defined in an IP access list or in an IP prefix list. Match criteria can also be defined based on packet length with the **match length** route map command. The VRF must be defined prior to the configuration of this command, and the **ip policy route-map** interface configuration command must be configured to enable policy routing under the interface or subinterface. If the VRF is not defined or if policy routing is not enabled, an error message will be printed in the console when you attempt to configure the **set vrf** command.



Note

The **set vrf** command cannot be configured with the **set default interface**, **set interface**, **set ip default next-hop**, and **set ip next-hop** policy routing commands because a packet cannot be set to an interface and the next hop cannot be changed when the VRF is specified. This is designed behavior. An error message will be printed in the console if you attempt to configure the **set vrf** command with any of the four above set clauses

Examples

The following example shows a route-map sequence that selects and sets a VRF based on match criteria defined in three different access lists. (The access list configuration is not shown in this example.) If the route map falls through and a match does not occur, the packet will be dropped if the destination is local.

```
route-map PBR-VRF-Selection permit 10
match ip address 40
set vrf VRF_1
```

```

!
route-map PBR-VRF-Selection permit 20
match ip address 50
set vrf VRF_2
!
route-map PBR-VRF-Selection permit 30
match ip address 60
set vrf VRF_3

```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
debug ip policy	Displays IP policy routing packet activity.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ip vrf	Configures a VRF routing table.
ip vrf receive	Inserts the IP address of an interface as a connected route entry in a VRF routing table.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or performs policy routing on packets.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

show connection

To display the status of interworking connections, use the **show connection** command in EXEC mode.

show connection [*all* | *element* | *id ID* | *name name* | *port port*]

Syntax Description	all	(Optional) Displays information about all interworking connections.
	<i>element</i>	(Optional) Displays information about the specified connection element.
	<i>id ID</i>	(Optional) Displays information about the specified connection identifier.
	<i>name name</i>	(Optional) Displays information about the specified connection name.
	<i>port port</i>	(Optional) Displays information about all connections on an interface.

Defaults Default state is **show connection all**.

Command Modes EXEC

Command History	Release	Modification
	12.1(2)T	This command was introduced as show connect (FR-ATM).
	12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S and updated to show all interworking connections.
	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.

Examples The following example shows the local interworking connections on a router:

```
Router# show connection

ID   Name           Segment 1           Segment 2           State
-----
1    conn1          ATM 1/0/0 AAL5 0/100  ATM 2/0/0 AAL5 0/100  UP
2    conn2          ATM 2/0/0 AAL5 0/300  Serial0/1 16          UP
3    conn3          ATM 2/0/0 AAL5 0/400  FA 0/0.1 10          UP
4    conn4          ATM 1/0/0 CELL 0/500  ATM 2/0/0 CELL 0/500  UP
5    conn5          ATM 1/0/0 CELL 100    ATM 2/0/0 CELL 100    UP
```

[Table 1](#) describes the significant fields shown in the display.

Table 1 *show connection Field Descriptions*

Display	Description
ID	Arbitrary connection identifier assigned by the operating system.
Name	Name of the connection.

Table 1 *show connection Field Descriptions (continued)*

Display	Description
Segment 1 Segment 2	Information about the interworking segments, including: <ul style="list-style-type: none"> • Interface name and number • The type of encapsulation (if any) assigned to the interface • The PVC assigned to the ATM interface, DLCI assigned to the serial interface, or VLAN ID assigned to the Ethernet interface.
State or Status	Status of the connection, including the following states: UP, DOWN, OPER DOWN, ADMIN DOWN, COMING UP.

Related Commands

Command	Description
show atm pvc	Displays the status of ATM PVCs and SVCs.
show frame-relay pvc	Displays the status of Frame Relay interfaces.

show controllers vsi control-interface

To display information about an ATM interface configured with the **tag-control-protocol vsi** command to control an external switch (or if an interface is not specified, to display information about all Virtual Switch Interface [VSI] control interfaces), use the **show controllers vsi control-interface** command in user EXEC or privileged EXEC mode.

```
show controllers vsi control-interface [interface]
```

Syntax Description

<i>interface</i>	(Optional) Specifies the interface number.
------------------	--

Command Modes

User EXEC
Privileged EXEC

Command History

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

Examples

The following is sample output from the **show controllers vsi control-interface** command:

```
Router# show controllers vsi control-interface
```

```
Interface:          ATM2/0          Connections:          14
```

The display shows the number of cross-connects currently on the switch that were established by the MPLS LSC through the VSI over the control interface.

Related Commands

Command	Description
tag-control-protocol vsi	Configures the use of VSI on a control port.

show controllers vsi descriptor

To display information about a switch interface discovered by the Multiprotocol Label Switching (MPLS) Label Switch Controller (LSC) through a Virtual Switch Interface (VSI), or if no descriptor is specified, about all such discovered interfaces, use the **show controllers vsi descriptor** command in user EXEC or privileged EXEC mode.

show controllers vsi descriptor [*descriptor*]

Syntax Description	<i>descriptor</i>	(Optional) Physical descriptor. For the Cisco BPX switch, the physical descriptor has the following form: <i>slot.port.0</i>
---------------------------	-------------------	--

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

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

Usage Guidelines Specify an interface by its (switch-supplied) physical descriptor.

Per-interface information includes the following:

- Interface name
- Physical descriptor
- Interface status
- Physical interface state (supplied by the switch)
- Acceptable VPI and VCI ranges
- Maximum cell rate
- Available cell rate (forward/backward)
- Available channels

Similar information is displayed when you enter the **show controllers xtagatm** privileged EXEC command. However, you must specify a Cisco IOS interface name instead of a physical descriptor.

Examples The following is sample output from the **show controllers vsi descriptor** command:

```
Router# show controllers vsi descriptor 12.2.0

Phys desc: 12.2.0
Log intf:  0x000C0200 (0.12.2.0)
Interface: XTagATM0
IF status: up                               IFC state: ACTIVE
Min VPI:   1                               Maximum cell rate: 10000
Max VPI:   259                             Available channels: 2000
```

```

Min VCI:      32                Available cell rate (forward): 10000
Max VCI:     65535             Available cell rate (backward): 10000
    
```

Table 2 describes the significant fields shown in the display.

Table 2 *show controllers vsi descriptor Field Descriptions*

Field	Description
Phys desc	Physical descriptor. A string learned from the switch that identifies the interface.
Log intf	Logical interface ID. This 32-bit entity, learned from the switch, uniquely identifies the interface.
Interface	The (Cisco IOS) interface name.
IF status	Overall interface status. Can be “up,” “down,” or “administratively down.”
Min VPI	Minimum virtual path identifier. Indicates the low end of the VPI range configured on the switch.
Max VPI	Maximum virtual path identifier. Indicates the high end of the VPI range configured on the switch.
Min VCI	Minimum virtual channel identifier. Indicates the high end of the VCI range configured on the switch.
Max VCI	Maximum virtual channel identifier. Indicates the high end of the VCI range configured on, or determined by, the switch.
IFC state	Operational state of the interface, according to the switch. Can be one of the following: <ul style="list-style-type: none"> • FAILED_EXT (that is, an external alarm) • FAILED_INT (indicates the inability of the MPLS LSC to communicate with the VSI slave controlling the interface, or another internal failure) • REMOVED (administratively removed from the switch)
Maximum cell rate	Maximum cell rate for the interface, which has been configured on the switch (in cells per second).
Available channels	Indicates the number of channels (endpoints) that are currently free to be used for cross-connects.
Available cell rate (forward)	Cell rate that is currently available in the forward (that is, ingress) direction for new cross-connects on the interface.
Available cell rate (backward)	Cell rate that is currently available in the backward (that is, egress) direction for new cross-connects on the interface.

Related Commands

Command	Description
show controllers xtagatm	Displays information about an extended MPLS ATM interface.

show controllers vsi session

To display information about all sessions with Virtual Switch Interface (VSI) slaves, use the **show controllers vsi session** command in user EXEC or privileged EXEC mode.

show controllers vsi session [*session-number* [**interface** *interface*]]



Note

A session consists of an exchange of VSI messages between the VSI master (the LSC) and a VSI slave (an entity on the switch). There can be multiple VSI slaves for a switch. On the BPX, each port or trunk card assumes the role of a VSI slave.

Syntax Description

<i>session-number</i>	(Optional) Specifies the session number.
interface <i>interface</i>	(Optional) Specifies the VSI control interface.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

If a session number and an interface are specified, detailed information on the individual session is presented. If the session number is specified, but the interface is omitted, detailed information on all sessions with that number is presented. (Only one session can contain a given number, because multiple control interfaces are not supported.)

Examples

The following is sample output from the **show controllers vsi session** command:

```
Router# show controllers vsi session
```

Interface	Session	VCD	VPI/VCI	Switch/Slave Ids	Session State
ATM0/0	0	1	0/40	0/1	ESTABLISHED
ATM0/0	1	2	0/41	0/2	ESTABLISHED
ATM0/0	2	3	0/42	0/3	DISCOVERY
ATM0/0	3	4	0/43	0/4	RESYNC-STARTING
ATM0/0	4	5	0/44	0/5	RESYNC-STOPPING
ATM0/0	5	6	0/45	0/6	RESYNC-UNDERWAY
ATM0/0	6	7	0/46	0/7	UNKNOWN
ATM0/0	7	8	0/47	0/8	UNKNOWN
ATM0/0	8	9	0/48	0/9	CLOSING
ATM0/0	9	10	0/49	0/10	ESTABLISHED
ATM0/0	10	11	0/50	0/11	ESTABLISHED
ATM0/0	11	12	0/51	0/12	ESTABLISHED

Table 3 describes the significant fields shown in the display.

Table 3 show controllers vsi session Field Descriptions

Field	Description
Interface	Control interface name.
Session	Session number (from 0 to <n-1>), where n is the number of sessions on the control interface.
VCD	Virtual circuit descriptor (virtual circuit number). Identifies the VC carrying the VSI protocol between the master and the slave for this session.
VPI/VCI	Virtual path identifier or virtual channel identifier (for the VC used for this session).
Switch/Slave Ids	Switch and slave identifiers supplied by the switch.
Session State	Indicates the status of the session between the master and the slave. <ul style="list-style-type: none"> • ESTABLISHED is the fully operational steady state. • UNKNOWN indicates that the slave is not responding. Other possible states include the following: <ul style="list-style-type: none"> • CONFIGURING • RESYNC-STARTING • RESYNC-UNDERWAY • RESYNC-ENDING • DISCOVERY • SHUTDOWN-STARTING • SHUTDOWN-ENDING • INACTIVE

In the following example, session number 9 is specified with the **show controllers vsi session** command:

```
Router# show controllers vsi session 9

Interface:          ATM1/0      Session number:      9
VCD:               10          VPI/VCI:             0/49
Switch type:       BPX          Switch id:            0
Controller id:     1            Slave id:             10
Keepalive timer:   15           Powerup session id:  0x0000000A
Cfg/act retry timer: 8/8       Active session id:   0x0000000A
Max retries:       10           Ctrl port log intf:  0x000A0100
Trap window:       50           Max/actual cmd wndw: 21/21
Trap filter:       all          Max checksums:       19
Current VSI version: 1          Min/max VSI version: 1/1
Messages sent:     2502          Inter-slave timer:   4.000
Messages received: 2502          Messages outstanding: 0
```

Table 4 describes the significant fields shown in the display.

Table 4 show controllers vsi session Field Descriptions

Field	Description
Interface	Name of the control interface on which this session is configured.
Session number	A number from 0 to <n-1>, where <i>n</i> is the number of slaves. Configured on the MPLS LSC with the <i>slaves</i> option of the tag-control-protocol vsi command.
VCD	Virtual circuit descriptor (virtual circuit number). Identifies the VC that carries VSI protocol messages for this session.
VPI/VCI	Virtual path identifier or virtual channel identifier for the VC used for this session.
Switch type	Switch device (for example, the BPX).
Switch id	Switch identifier (supplied by the switch).
Controller id	Controller identifier. Configured on the LSC, and on the switch, with the id option of the tag-control-protocol vsi command.
Slave id	Slave identifier (supplied by the switch).
Keepalive timer	VSI master keepalive timeout period (in seconds). Configured on the MPLS LSC through the keepalive option of the tag-control-protocol-vsi command. If no valid message is received by the MPLS LSC within this time period, it sends a keepalive message to the slave.
Powerup session id	Session ID (supplied by the slave) used at powerup time.
Cfg/act retry timer	Configured and actual message retry timeout period (in seconds). If no response is received for a command sent by the master within the actual retry timeout period, the message is re-sent. This applies to most message transmissions. The configured retry timeout value is specified through the retry option of the tag-control-protocol vsi command. The actual retry timeout value is the larger of the configured value and the minimum retry timeout value permitted by the switch.
Active session id	Session ID (supplied by the slave) for the currently active session.
Max retries	Maximum number of times that a particular command transmission will be retried by the master. That is, a message may be sent up to <max_retries+1> times. Configured on the MPLS LSC through the retry option of the tag-control-protocol vsi command.
Ctrl port log intf	Logical interface identifier for the control port, as supplied by the switch.
Trap window	Maximum number of outstanding trap messages permitted by the master. This is advertised, but not enforced, by the LSC.
Max/actual cmd wndw	Maximum command window is the maximum number of outstanding (that is, unacknowledged) commands that may be sent by the master before waiting for acknowledgments. This number is communicated to the master by the slave. The command window is the maximum number of outstanding commands that are permitted by the master, before it waits for acknowledgments. This is always less than the maximum command window.
Trap filter	This is always "all" for the LSC, indicating that it wants to receive all traps from the slave. This is communicated to the slave by the master.

Table 4 *show controllers vsi session Field Descriptions (continued)*

Field	Description
Max checksums	Maximum number of checksum blocks supported by the slave.
Current VSI version	VSI protocol version currently in use by the master for this session.
Min/max VSI version	Minimum and maximum VSI versions supported by the slave, as last reported by the slave. If both are zero, the slave has not yet responded to the master.
Messages sent	Number of commands sent to the slave.
Inter-slave timer	Timeout value associated by the slave for messages it sends to other slaves. On a VSI-controlled switch with a distributed slave implementation (such as the BPX), VSI messages may be sent between slaves to complete their processing. For the MPLS LSC VSI implementation to function properly, the value of its retry timer is forced to be at least two times the value of the interslave timer. (See “Cfg/act retry timer” in this table.)
Messages received	Number of responses and traps received by the master from the slave for this session.
Messages outstanding	Current number of outstanding messages (that is, commands sent by the master for which responses have not yet been received).

Related Commands

Command	Description
tag-control-protocol vsi	Configures the use of VSI on a control port.

show controllers vsi status

To display a one-line summary of each Virtual Switch Interface (VSI)-controlled interface, use the **show controllers vsi status** command in user EXEC or privileged EXEC mode.

show controllers vsi status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

If an interface is discovered by the LSC, but no extended Multiprotocol Label Switching (MPLS) ATM interface is associated with it through the **extended-port** command, then the interface name is marked <unknown>, and interface status is marked n/a.

Examples

The following is sample output from the **show controllers vsi status** command:

```
Router# show controllers vsi status
```

```
Interface Name           IF Status   IFC State   Physical Descriptor
switch control port     n/a        ACTIVE      12.1.0
XTagATM0                 up         ACTIVE      12.2.0
XTagATM1                 up         ACTIVE      12.3.0
<unknown>                n/a       FAILED-EXT  12.4.0
```

[Table 5](#) describes the significant fields shown in the display.

Table 5 *show controllers vsi status Field Descriptions*

Field	Description
Interface Name	The (Cisco IOS) interface name.
IF Status	Overall interface status. Can be “up,” “down,” or “administratively down.”
IFC State	The operational state of the interface, according to the switch. Can be one of the following: <ul style="list-style-type: none"> FAILED-EXT (that is, an external alarm) FAILED-INT (indicates the inability of the MPLS LSC to communicate with the VSI slave controlling the interface, or another internal failure) REMOVED (administratively removed from the switch)
Physical Descriptor	A string learned from the switch that identifies the interface.

show controllers vsi traffic

To display traffic information about Virtual Switch Interface (VSI)-controlled interfaces, VSI sessions, or virtual circuits (VCs) on VSI-controlled interfaces, use the **show controllers vsi traffic** command in user EXEC or privileged EXEC mode.

```
show controllers vsi traffic { descriptor descriptor | session session-number | vc [descriptor
descriptor [vpi vci]] }
```

Syntax Description

descriptor <i>descriptor</i>	Displays traffic statistics for the specified descriptor.
session <i>session-number</i>	Displays traffic statistics for the specified session.
vc	Displays traffic statistics for the specified VC.
descriptor [descriptor <i>descriptor</i>]	Specifies the name of the physical descriptor.
<i>vpi</i>	Virtual path identifier (0 to 4095).
<i>vci</i>	Virtual circuit identifier (0 to 65535).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	The VPI range of values was extended to 4095.

Usage Guidelines

If none of the keywords is specified, traffic for all interfaces is displayed. You can specify a single interface by its (switch-supplied) physical descriptor. For the BPX switch, the physical descriptor has the form

slot.port. 0

If a session number is specified, the output displays VSI protocol traffic by message type. The VC traffic display is also displayed by the **show xmplsatm vc cross-connect traffic descriptor** command.

Examples

The following is sample output from the **show controllers vsi traffic** command:

```
Router# show controllers vsi traffic

Phys desc: 10.1.0
Interface: switch control port
IF status: n/a
Rx cells: 304250           Rx cells discarded: 0
Tx cells: 361186           Tx cells discarded: 0
Rx header errors: 4294967254 Rx invalid addresses (per card): 80360
Last invalid address: 0/53

Phys desc: 10.2.0
```

```

Interface: XTagATM0
IF status: up
Rx cells: 202637          Rx cells discarded: 0
Tx cells: 194979          Tx cells discarded: 0
Rx header errors: 4294967258 Rx invalid addresses (per card): 80385
Last invalid address: 0/32

Phys desc: 10.3.0
Interface: XTagATM1
IF status: up
Rx cells: 182295          Rx cells discarded: 0
Tx cells: 136369          Tx cells discarded: 0
Rx header errors: 4294967262 Rx invalid addresses (per card): 80372
Last invalid address: 0/32
    
```

Table 6 describes the significant fields shown in the display.

Table 6 show controllers vsi traffic Field Descriptions

Field	Description
Phys desc	Physical descriptor of the interface.
Interface	The Cisco (IOS) interface name.
Rx cells	Number of cells received on the interface.
Tx cells	Number of cells transmitted on the interface.
Rx cells discarded	Number of cells received on the interface that were discarded due to traffic management.
Tx cells discarded	Number of cells that could not be transmitted on the interface due to traffic management and which were therefore discarded.
Rx header errors	Number of cells that were discarded due to ATM header errors.
Rx invalid addresses	Number of cells received with an invalid address (that is, an unexpected VPI/VCI combination). With the Cisco BPX switch, this count is of all such cells received on all interfaces in the port group of this interface.
Last invalid address	Number of cells received on this interface with ATM cell header errors.

The following sample output is displayed when you enter the **show controllers vsi traffic session 9** command:

```

Router# show controllers vsi traffic session 9
          Sent                               Received
Sw Get Cnfg Cmd:      3656      Sw Get Cnfg Rsp:      3656
Sw Cnfg Trap Rsp:      0          Sw Cnfg Trap:          0
Sw Set Cnfg Cmd:      1          Sw Set Cnfg Rsp:      1
Sw Start Resync Cmd:  1          Sw Start Resync Rsp:  1
Sw End Resync Cmd:    1          Sw End Resync Rsp:    1
Ifc Getmore Cnfg Cmd: 1          Ifc Getmore Cnfg Rsp: 1
Ifc Cnfg Trap Rsp:    4          Ifc Cnfg Trap:        4
Ifc Get Stats Cmd:    8          Ifc Get Stats Rsp:    8
Conn Cmt Cmd:         73          Conn Cmt Rsp:         73
Conn Del Cmd:         50          Conn Del Rsp:         0
Conn Get Stats Cmd:   0          Conn Get Stats Rsp:   0
Conn Cnfg Trap Rsp:   0          Conn Cnfg Trap:       0
Conn Bulk Clr Stats Cmd: 0      Conn Bulk Clr Stats Rsp: 0
Gen Err Rsp:          0          Gen Err Rsp:          0
unused:               0          unused:               0
unknown:              0          unknown:              0
    
```

TOTAL: 3795 TOTAL: 3795

Table 7 describes the significant fields shown in the display.

Table 7 *show controllers vsi traffic session Field Descriptions*

Field	Description
Sw Get Cnfg Cmd	Number of VSI “get switch configuration command” messages sent.
Sw Cnfg Trap Rsp	Number of VSI “switch configuration asynchronous trap response” messages sent.
Sw Set Cnfg Cmd	Number of VSI “set switch configuration command” messages sent.
Sw Start Resync Cmd	Number of VSI “set resynchronization start command” messages sent.
Sw End Resync Cmd	Number of VSI “set resynchronization end command” messages sent.
Ifc Getmore Cnfg Cmd	Number of VSI “get more interfaces configuration command” messages sent.
Ifc Cnfg Trap Rsp	Number of VSI “interface configuration asynchronous trap response” messages sent.
Ifc Get Stats Cmd	Number of VSI “get interface statistics command” messages sent.
Conn Cmt Cmd	Number of VSI “set connection committed command” messages sent.
Conn Del Cmd	Number of VSI “delete connection command” messages sent.
Conn Get Stats Cmd	Number of VSI “get connection statistics command” messages sent.
Conn Cnfg Trap Rsp	Number of VSI “connection configuration asynchronous trap response” messages sent.
Conn Bulk Clr Stats Cmd	Number of VSI “bulk clear connection statistics command” messages sent.
Gen Err Rsp	Number of VSI “generic error response” messages sent or received.
Sw Get Cnfg Rsp	Number of VSI “get connection configuration command response” messages received.
Sw Cnfg Trap	Number of VSI “switch configuration asynchronous trap” messages received.
Sw Set Cnfg Rsp	Number of VSI “set switch configuration response” messages received.
Sw Start Resync Rsp	Number of VSI “set resynchronization start response” messages received.
Sw End Resync Rsp	Number of VSI “set resynchronization end response” messages received.
Ifc Getmore Cnfg Rsp	Number of VSI “get more interfaces configuration response” messages received.
Ifc Cnfg Trap	Number of VSI “interface configuration asynchronous trap” messages received.
Ifc Get Stats Rsp	Number of VSI “get interface statistics response” messages received.
Conn Cmt Rsp	Number of VSI “set connection committed response” messages received.
Conn Del Rsp	Number of VSI “delete connection response” messages received.
Conn Get Stats Rsp	Number of VSI “get connection statistics response” messages received.
Conn Cnfg Trap	Number of VSI “connection configuration asynchronous trap” messages received.

Table 7 *show controllers vsi traffic session Field Descriptions (continued)*

Field	Description
Conn Bulk Clr Stats Rsp	Number of VSI “bulk clear connection statistics response” messages received.
unused, unknown	“Unused” messages are those whose function codes are recognized as being part of the VSI protocol, but which are not used by the MPLS LSC and, consequently, are not expected to be received or sent. “Unknown” messages have function codes that the MPLS LSC does not recognize as part of the VSI protocol.
TOTAL	Total number of VSI messages sent or received.

show controllers xtagatm

To display information about an extended Multiprotocol Label Switching (MPLS) ATM interface controlled through the Virtual Switch Interface (VSI) protocol (or, if an interface is not specified, to display information about all extended MPLS ATM interfaces controlled through the VSI protocol), use the **show controllers xtagatm** command in user EXEC or privileged EXEC mode.

show controllers xtagatm *if-number*

Syntax Description	<i>if-number</i>	Specifies the interface number.
Command Modes	User EXEC Privileged EXEC	
Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Per-interface information includes the following:

- Interface name
- Physical descriptor
- Interface status
- Physical interface state (supplied by the switch)
- Acceptable VPI and VCI ranges
- Maximum cell rate
- Available cell rate (forward/backward)
- Available channels

Similar information appears if you enter the **show controllers vsi descriptor** command. However, you must specify an interface by its (switch-supplied) physical descriptor, instead of its Cisco IOS interface name. For the Cisco BPX switch, the physical descriptor has the form *slot.port.0*.

Examples In this example, the sample output is from the **show controllers xtagatm** command specifying interface 0:

```
Router# show controllers xtagatm 0

Interface XTagATM0 is up
Hardware is Tag-Controlled ATM Port (on BPX switch BPX-VSI1)
Control interface ATM1/0 is up
Physical descriptor is 10.2.0
Logical interface 0x000A0200 (0.10.2.0)
Oper state ACTIVE, admin state UP
VPI range 1-255, VCI range 32-65535
VPI is not translated at end of link
```

```

Tag control VC need not be strictly in VPI/VCI range
Available channels: ingress 30, egress 30
Maximum cell rate: ingress 300000, egress 300000
Available cell rate: ingress 300000, egress 300000
Endpoints in use: ingress 7, egress 8, ingress/egress 1
Rx cells 134747
rx cells discarded 0, rx header errors 0
rx invalid addresses (per card): 52994
last invalid address 0/32
Tx cells 132564
tx cells discarded: 0
    
```

Table 8 describes the significant fields shown in the display.

Table 8 show controllers xtagatm Field Descriptions

Field	Description
Interface XTagATM0 is up	Indicates the overall status of the interface. May be “up,” “down,” or “administratively down.”
Hardware is Tag-Controlled ATM Port	<p>Indicates the hardware type.</p> <p>If the XTagATM was successfully associated with a switch port, a description of the form (on <switch_type> switch <name>) follows this field, where <switch_type> indicates the type of switch (for example, BPX), and the name is an identifying string learned from the switch.</p> <p>If the XTagATM interface was not bound to a switch interface (with the extended-port interface configuration command), then the label “Not bound to a control interface and switch port” appears.</p> <p>If the interface has been bound, but the target switch interface has not been discovered by the LSC, then the label “Bound to undiscovered switch port (id <number>)” appears, where <number> is the logical interface ID in hexadecimal notation.</p>
Control interface ATM1/0 is up	Indicates that the XTagATM interface was bound (with the extended-port interface configuration command) to the VSI master whose control interface is ATM1/0 and that this control interface is up.
Physical descriptor is...	A string identifying the interface that was learned from the switch.
Logical interface	This 32-bit entity, learned from the switch, uniquely identifies the interface. It appears in both hexadecimal and dotted quad notation.
Oper state	<p>Operational state of the interface, according to the switch. Can be one of the following:</p> <ul style="list-style-type: none"> • ACTIVE • FAILED_EXT (that is, an external alarm) • FAILED_INT (indicates the inability of the MPLS LSC to communicate with the VSI slave controlling the interface, or another internal failure) • REMOVED (administratively removed from the switch)
admin state	Administrative state of the interface, according to the switch—either “Up” or “Down.”
VPI range 1 to 255	Indicates the allowable VPI range for the interface that was configured on the switch.

Table 8 *show controllers xtagatm Field Descriptions (continued)*

Field	Description
VCI range 32 to 65535	Indicates the allowable VCI range for the interface that was configured on, or determined by, the switch.
LSC control VC need not be strictly in VPI or VCI range	Indicates that the label control VC does not need to be within the range specified by VPI range, but may be on VPI 0 instead.
Available channels	Indicates the number of channels (endpoints) that are currently free to be used for cross-connects.
Maximum cell rate	Maximum cell rate for the interface, which was configured on the switch.
Available cell rate	Cell rate that is currently available for new cross-connects on the interface.
Endpoints in use	Number of endpoints (channels) in use on the interface, broken down by anticipated traffic flow, as follows: <ul style="list-style-type: none"> • Ingress—Endpoints carry traffic into the switch • Egress—Endpoints carry traffic away from the switch • Ingress/egress—Endpoints carry traffic in both directions
Rx cells	Number of cells received on the interface.
rx cells discarded	Number of cells received on the interface that were discarded due to traffic management actions (rx header errors).
rx header errors	Number of cells received on the interface with cell header errors.
rx invalid addresses (per card)	Number of cells received with invalid addresses (that is, unexpected VPI or VCI). On the BPX, this counter is maintained per port group (not per interface).
last invalid address	Address of the last cell received on the interface with an invalid address (for example, 0/32).
Tx cells	Number of cells sent from the interface.
tx cells discarded	Number of cells intended for transmission from the interface that were discarded due to traffic management actions.

Related Commands

Command	Description
show controllers vsi descriptor	Displays information about a switch interface discovered by the MPLS LSC through the VSI.