mace enable

To apply the global Measurement, Aggregation, and Correlation Engine (MACE) policy on an interface, use the **mace enable** command in interface configuration mode. To disable the MACE policy on an interface, use the **no** form of this command.

mace enable

no mace enable

Syntax Description

This command has no arguments or keywords.

Command Default

No MACE policy is applied on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

Use the **mace enable** command to apply the global MACE policy on an interface. This command applies the global MACE policy in both directions, ingress and egress, of the interface. The MACE runs on the traffic coming over this interface. MACE policy is limited to those targets for which the Wide Area Application Services (WAAS) policy can be enabled. MACE supports all the interfaces that are supported by WAAS.

To enable MACE, you must first perform the following configurations:

- Flow record of type MACE
- Flow exporter
- Flow monitor of type MACE
- Class map of type WAAS
- Policy map of type MACE

When you configure a **mace enable** command, the metrics of the matching flows are collected and updated on every packet. When the export timer expires, these metrics are aggregated and exported to various collectors, according to the defined configuration. If the flow is optimized by WAAS, the metrics of both segments, pre-WAAS and post-WAAS, of the flow are exported.

Examples

The following example shows how to enable MACE on Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# mace enable
```

Related Commands

Command	Description
class-map type waas	Configures a WAAS Express class map.
flow exporter	Creates a Flexible NetFlow flow exporter.
flow monitor type mace	Configures a flow monitor for MACE.
flow record type mace	Configures a flow record for MACE.
policy-map type mace	Configures a MACE policy map.

mace monitor waas

To enable the Measurement, Aggregation, and Correlation Engine (MACE) monitoring on Wide Area Application Services (WAAS), use the **mace monitor waas** command in global configuration mode. To disable MACE monitoring, use the **no** form of this command.

mace monitor waas [**all** | **optimized**] [**name**] *monitor-name*

no mace monitor waas [**all** | **optimized**] [**name**] *monitor-name*

Syntax Description

all	(Optional) Enables MACE monitoring for all WAAS flows.
optimized	(Optional) Enables MACE monitoring for WAAS-optimized flows.
name	(Optional) Specifies the name of a flow monitor.
monitor-name	Name of the specific flow monitor that is configured using the **flow monitor type mace** command.

Command Default

No MACE is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

Use the **mace monitor waas** command to enable MACE for all WAAS instances that run on the router.

MACE monitors all the flows on which WAAS is active for optimization.

To enable MACE on WAAS, you must first configure the following:

- A flow record of type MACE
- A flow exporter
- A flow monitor of type MACE

When you use the **mace monitor waas** command along with the **optimized** keyword, MACE monitors all the flows on which WAAS is active for optimization.

When you use this command along with the **all** keyword, MACE monitors all the flows configured in a WAAS policy. This includes the flows that are subject to either WAAS optimization or pass-through actions.

When you use this command without the **all** or **optimized** keyword, MACE monitors all WAAS classes that have the **optimize** keyword configured in them. MACE also exports the flows that are tagged by WAAS as passthrough, even when they match the classes with optimize actions in them.

Note If you wish to choose a subset of WAAS classes, you must create a global MACE policy that includes the desired classes.

Examples

The following example shows how to configure MACE to monitor all the flows that are configured in a WAAS policy:

```
Router(config)# mace monitor waas all my-flow-monitor
```

Related Commands

Command	Description
flow exporter	Creates a Flexible NetFlow flow exporter.
flow monitor type mace	Configures a flow monitor for MACE.
flow record type mace	Configures a flow record for MACE.
mace enable	Applies the global MACE policy on an interface.

map-class frame-relay

To specify a map class to define quality of service (QoS) values for a virtual circuit (VC), use the **map-class frame-relay** command in global configuration mode. To remove a map class, use the **no** form of this command.

map-class frame-relay *map-class-name*

no map-class frame-relay *map-class-name*

Syntax Description

map-class-name	Name of map class.

Defaults

A map class is not specified.

Command Modes

Global configuration

Command History

Release	Modification
11.2	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

After you specify the named map class, you can specify the QoS parameters—such as incoming and outgoing committed information rate (CIR), committed burst rate, excess burst rate, and the idle timer—for the map class.

To specify the protocol-and-address combination to which the QoS parameters are to be applied, associate this map class with the static maps under a map list.

Examples

The following example specifies a map class “hawaii” and defines three QoS parameters for it. The “hawaii” map class is associated with a protocol-and-address static map defined under the **map-list** command.

```
map-list bermuda source-addr E164 123456 dest-addr E164 654321
 ip 10.108.177.100 class hawaii
 appletalk 1000.2 class hawaii

map-class frame-relay hawaii
 frame-relay cir in 2000000
 frame-relay cir out 56000
 frame-relay be out 9000
```

Related Commands

Command	Description
frame-relay bc	Specifies the incoming or outgoing Bc for a Frame Relay VC.
frame-relay be	Sets the incoming or outgoing Be for a Frame Relay VC.
frame-relay cir	Specifies the incoming or outgoing CIR for a Frame Relay VC.
frame-relay idle-timer	Specifies the idle timeout interval for an SVC.

map-group

To associate a map list with a specific interface, use the **map-group** command in interface configuration mode.

map-group *group-name*

Syntax Description

group-name	Name used in a **map-list** command.

Defaults

A map list is not associated with an interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	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

A map-group association with an interface is required for switched virtual circuit (SVC) operation. In addition, a map list must be configured.

The **map-group** command applies to the interface or subinterface on which it is configured. The associated E.164 or X.121 address is defined by the **map-list** command, and the associated protocol addresses are defined by using the **class** command under the **map-list** command.

Examples

The following example configures a physical interface, applies a map group to the physical interface, and then defines the map group:

```
interface serial 0
 ip address 172.10.8.6
 encapsulation frame-relay
 map-group bermuda
 frame-relay lmi-type q933a
 frame-relay svc

map-list bermuda source-addr E164 123456 dest-addr E164 654321
 ip 10.1.1.1 class hawaii
 appletalk 1000.2 class rainbow
```

Related Commands

Command	Description
class (map-list)	Associates a map class with a protocol-and-address combination.
map-list	Specifies a map group and link it to a local E.164 or X.121 source address and a remote E.164 or X.121 destination address for Frame Relay SVCs.

map-list

To specify a map group or map list and link it to a local E.164 or X.121 source address and a remote E.164 or X.121 destination address for Frame Relay switched virtual circuits (SVCs), use the **map-list** command in global configuration mode. To delete a previous map-group link, use the **no** form of this command.

map-list *map-group-name* **source-addr** {**e164** | **x121**} *source-address* **dest-addr** {**e164** | **x121**} *destination-address* **clps** *number* [**cdps** *number*]

no map-list *map-group-name* **source-addr** {**e164** | **x121**} *source-address* **dest-addr** {**e164** | **x121**} *destination-address* **clps** *number* [**cdps** *number*]

Syntax Description

map-group-name	Name of the map group or map list. This map group or list must be associated with a physical interface.
source-addr {**e164** | **x121**}	Specifies the type of source address.
source-address	Address of the type specified (E.164 or X.121).
dest-addr {**e164** | **x121**}	Specifies the type of destination address.
destination-address	Address of the type specified (E.164 or X.121).
clps *number*	Specifies the calling party subaddress. The subaddress range is from 1 to 9.
cdps *number*	(Optional) Specifies the called party subaddress. The subaddress range is from 1 to 9.

Defaults

A map group or map list is not linked to a source and destination address.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	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 in a release earlier than Cisco IOS Release 15.0(1)M. The **clps** *number* and **cdps** *number* keyword and argument pairs were added.

Usage Guidelines

Use the **map-class** command to define quality of service (QoS) parameters—such as incoming and outgoing committed information rate (CIR), committed burst rate, excess burst rate, and the idle timer—for the static maps defined under a map list or map group.

Each SVC needs to use a source and destination number, in much the same way that a public telephone network needs to use source and destination numbers. These numbers allow the network to route calls from a specific source to a specific destination. This specification is done through map lists or map groups.

Depending on switch configuration, addressing can take either of two forms: E.164 or X.121.

An X.121 address number is 14 digits long and has the following form:

```
Z CC P NNNNNNNNNN
```

Table 18 describes the codes in an X.121 address number form.

Table 18 X.121 Address Numbers

Code	Meaning	Value
Z	Zone code	3 for North America
C	Country code	10–16 for the United States
P	Public data network (PDN) code	Provided by the PDN
N	10-digit number	Set by the network for the specific destination

An E.164 number has a variable length; the maximum length is 15 digits. An E.164 number has the fields shown in Figure 1 and described in Table 19.

Figure 1 E.164 Address Format

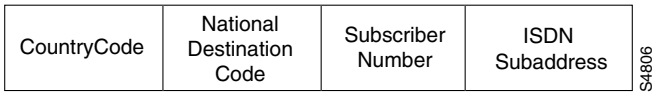

Table 19 E.164 Address Field Descriptions

Field	Description
Country code	Can be 1, 2, or 3 digits long. Some current values are the following: • Code 1—United States of America • Code 44—United Kingdom • Code 61—Australia
National destination code + subscriber number	Referred to as the National ISDN number; the maximum length is 12, 13, or 14 digits, based on the country code.
ISDN subaddress	Identifies one of many devices at the termination point. An ISDN subaddress is similar to an extension on a PBX.

Examples

In the following SVC example, if IP or AppleTalk triggers the call, the SVC is set up with the QoS parameters defined within the class “example”.

An SVC triggered by either protocol results in two SVC maps, one for IP and one for AppleTalk. Two maps are set up because these protocol-and-address combinations are heading for the same destination, as defined by the **dest-addr** keyword and the values following it in the **map-list** command.

```
map-list test source-addr e164 123456 dest-addr e164 654321 clps 2 cdps 4
 ip 10.1.1.1 class example
 appletalk 1000.2 class example
```

Related Commands

Command	Description
class (**map-list**)	Associates a map class with a protocol-and-address combination.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

match fr-de

To match packets on the basis of the Frame Relay discard eligibility (DE) bit setting, use the **match fr-de** command in class-map configuration mode. To remove the match criteria, use the **no** form of this command.

match fr-de

no match fr-de

Syntax Description

This command has no arguments or keywords.

Command Default

Packets are not matched on the basis of the Frame Relay DE bit setting.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.0(25)S	This command was introduced for the Cisco 7500 series router.
12.0(26)S	This command was implemented on the Cisco 7200 series router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(15)T2	This command was integrated into Cisco IOS Release 12.4(15)T2.
12.2(33)SB	This command was implemented on the Cisco 7300 series router.

Examples

The following example creates a class called match-fr-de and matches packets on the basis of the Frame Relay DE bit setting.

```
Router(config)# class-map match-fr-de
Router(config-cmap)# match fr-de
Router(config-cmap)# end
```

Related Commands

Command	Description
set fr-de	Changes the DE bit setting in the address field of a Frame Relay frame to 1 for all traffic leaving an interface.

match protocol (L2TPv3)

To configure protocol demultiplexing, use the **match protocol** command in xconnect configuration mode. To disable protocol demultiplexing, use the **no** form of this command.

match protocol ipv6

no match protocol ipv6

Syntax Description

ipv6	Specifies IPv6 as the protocol to demultiplex.

Command Default

IPv6 protocol demultiplexing is disabled by default.

Command Modes

Xconnect configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

Protocol demultiplexing is supported only for Ethernet and terminated data-link connection identifier (DLCI) Frame Relay traffic in Cisco IOS Release 12.0(29)S and later releases.

Protocol demultiplexing requires supporting the combination of an IP address and an **xconnect** command configuration on the IPv4 provider edge (PE) interface. This combination of configurations is not allowed without enabling protocol demultiplexing, with the exception of switched Frame Relay permanent virtual circuits (PVCs). If no IP address is configured, the protocol demultiplexing configuration is rejected. If an IP address is configured, the **xconnect** command configuration is rejected unless protocol demultiplexing is enabled in xconnect configuration mode before exiting that mode. If an IP address is configured with an **xconnect** command configuration and protocol demultiplexing enabled, the IP address cannot be removed. To change or remove the configured IP address, the **xconnect** command configuration must first be disabled.

Table 20 shows the valid combinations of configurations.

Table 20 Support for the ATM Cell Relay Features

Scenario	IP Address	xconnect Configuration	Protocol Demultiplexing Configuration
Routing	Yes	No	—
L2VPN	No	Yes	No
IPv6 Protocol Demultiplexing	Yes	Yes	Yes

Examples

The following example configures IPv6 protocol demultiplexing in an xconnect configuration:

```
xconnect 10.0.3.201 888 pw-class demux
 match protocol ipv6
```

Related Commands

Command	Description
xconnect	Binds an attachment circuit to a Layer 2 pseudowire and enters xconnect configuration mode

match tcp

To match WAAS Express TCP traffic based on the IP address or port options, use the **match tcp** command in QoS class-map configuration mode. To remove the match, use the **no** form of this command.

match tcp {**any** | **destination** | **source**} {**ip** *ip-address* [*inverse mask*] | **port** *start-port-number* [*end-port-number*]}

match tcp {**any** | **destination** | **source**} {**ip** *ip-address* [*inverse mask*] | **port** *start-port-number* [*end-port-number*]}

Syntax Description

any	Matches based on any of TCP traffic.
destination	Matches the traffic based on the destination IP address or port number.
source	Matches the TCP traffic based on the source IP address or port number.
ip *ip-address* [*inverse mask*]	(Optional) Matches the TCP traffic based on the source or destination IP address and inverse mask.
port	Matches the TCP traffic based on the port number.
start-port-number	The starting port number.
end-port-number	(Optional) The ending port number.

Command Default

Traffic is matched on all TCP traffic.

Command Modes

QoS class-map configuration (config-cmap)

Command History

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

Usage Guidelines

Use this command to match the TCP traffic based on the IP address or port number of the source or destination. If Network Address Translation (NAT) is used, the IP address refers to the inside local address and outside global address.

Note The class-map type of WAAS combines filters using the match-any logical operator. The match-all logical operator is not supported by the WAAS class map. This means that if one match criterion (filters) matches, the entire class map also matches.

Examples

The following example matches traffic having a destination TCP port number from 7000 to 7009:

```
Router(config)# class-map type waas waas_global
Router(config-cmap)# match tcp destination port 7000 7009
```

The following example matches traffic if the following conditions are matched:

- Destination IP address is in the range 209.165.200.225 and destination TCP port is 80.
- Destination IP address is in the range 209.165.200.225 and destination TCP port is 8080.

```
Router(config)# class-map type waas waas_global
Router(config-cmap)# match tcp destination ip 209.165.200.225 0.0.0.31 port 80 80
Router(config-cmap)# match tcp destination ip 209.165.200.225 0.0.0.31 port 8080 8080
```

Related Commands

Command	Description
class-map type waas	Defines a WAAS Express class map.

mls l2tpv3 reserve

To reserve a loopback interface to use as a source for the Layer 2 Tunnel Protocol version 3 (L2TPv3) tunnel for a specific line card and processor pair, use the **mls l2tpv3 reserve** command in interface configuration mode. To cancel the loopback interface reservation, use the **no** form of this command.

mls l2tpv3 reserve {**slot** *slot-num* | **interface** {**TenGigabitEthernet** *slot_num*/*slot_unit* | **GigabitEthernet** *slot_num*/*slot_unit* **GigabitEthernet** *slot_num*/*slot_unit*}}

no mls l2tpv3 reserve {**slot** *slot-num* | **interface** {**TenGigabitEthernet** *slot_num*/*slot_unit* | **GigabitEthernet** *slot_num*/*slot_unit* **GigabitEthernet** *slot_num*/*slot_unit*}}

Syntax Description

slot *slot_num*	Router slot number for a Cisco 7600 series SPA Interface Processor-400 (SIP-400) line card.
interface	Specifies that the interface is for a Cisco 7600 series ES Plus line card.
TenGigabitEthernet	Specifies a 2-Port 10 Gigabit Ethernet or a 4-Port 10 Gigabit Ethernet line card.
GigabitEthernet	Specifies 20-Port Gigabit Ethernet or 40-Port Gigabit Ethernet line cards.
slot_num/*slot_unit*	Slot number in which the line card is inserted and the slot unit (the line card port number). When using two Gigabit Ethernet interfaces, the slot numbers of the two interfaces must match and can either be 1, 11, 21, or 31. The slot unit of the second Gigabit Ethernet interface must be ten plus the slot number of the first Gigabit Ethernet interface.

Command Default

No loopback interface is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRC	This command was introduced on the Cisco 7600 series routers.
12.2(33)SRD	This command was modified to support the Cisco 7600 series ES Plus line cards.

Usage Guidelines

This command also prevents the reserved loopback interface from being used across multiple line cards.

Examples

The following example reserves a loopback interface to use as a source for the L2TPv3 tunnel for a SIP-400 line card:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface Loopback1
Router(config-if)# mls l2tpv3 reserve slot 4
Router(config-if)# end
```

```
Router#
*Sep 11 04:03:26.770: %SYS-5-CONFIG_I: Configured from console by console
Router# show running interface Loopback1
Building configuration...
Current configuration : 69 bytes
!
interface Loopback1
 no ip address
 mls l2tpv3 reserve slot 4
end
```

The following example reserves a loopback interface to use as a source for the L2TPv3 tunnel for two 40-Port Gigabit Ethernet line cards:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface Loopback1
Router(config-if)# mls l2tpv3 reserve interface GigabitEthernet 3/11 GigabitEthernet 3/20
Router(config-if)# end
Router#
*Sep 10 10:46:01.671: %SYS-5-CONFIG_I: Configured from console by console
Router# show running interface Loopback1
Building configuration...
Current configuration : 112 bytes
!
interface Loopback1
 no ip address
 mls l2tpv3 reserve interface GigabitEthernet3/11 GigabitEthernet3/20
end
```

The following example reserves a loopback interface to use as a source for the L2TPv3 tunnel for a 2-Port 10 Gigabit Ethernet line card:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface Loopback2
Router(config-if)# mls l2tpv3 reserve interface TenGigabitEthernet 9/1
Router(config-if)# end
Router#
*Sep 10 10:49:31.451: %SYS-5-CONFIG_I: Configured from console by console
Router# show running interface Loopback2
Building configuration...
Current configuration : 112 bytes
!
interface Loopback2
 no ip address
 mls l2tpv3 reserve interface Tengigether 9/1
end
```

Related Commands

Command	Description
show running interface	Verifies the configuration.

monitor l2tun counters tunnel l2tp

To enable or disable the collection of per-tunnel control message statistics for Layer 2 Tunnel Protocol (L2TP) tunnels, use the **monitor l2tun counters tunnel l2tp** command in privileged EXEC mode.

monitor l2tun counters tunnel l2tp id *local-id* {**start** | **stop**}

Syntax Description

id *local-id*	Specifies the local ID of an L2TP tunnel.
start	Specifies that per-tunnel control message statistics will be collected for the tunnel.
stop	Specifies that per-tunnel control message statistics will not be collected for the tunnel. **Note** Any existing per-tunnel statistics will be lost when the **stop** keyword is issued.

Command Default

Per-tunnel statistics are not collected for any tunnels.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use the **monitor l2tun counters tunnel l2tp** command to enable or disable the collection of per-tunnel control message statistics. Per-tunnel statistics must be enabled for each tunnel that you want to monitor.

Use the **show l2tun counters tunnel l2tp id** *local-id* command to display per-tunnel statistics for a specific tunnel. Use the **show l2tun counters tunnel l2tp all** command to display per-tunnel statistics for all tunnels that have per-tunnel statistics enabled.

Use the **clear l2tun counters tunnel l2tp id** *local-id* command to clear the per-tunnel statistics for a specific tunnel. Per-tunnel statistics are also cleared when the collection of per-tunnel statistics is disabled.

Examples

The following example enables the collection of per-tunnel control message statistics for the tunnel with the local tunnel ID 4230:

```
monitor l2tun counters tunnel l2tp id 4230 start
```

The following example disables the collection of per-tunnel control message statistics for the tunnel with the local tunnel ID 4230:

```
monitor l2tun counters tunnel l2tp id 4230 stop
```

Related Commands

Command	Description
clear l2tun counters tunnel l2tp	Clears global or per-tunnel control message statistics for L2TP tunnels.
show l2tun counters tunnel l2tp	Displays global or per-tunnel control message statistics for L2TP tunnels.

monitor peer bfd

To enable pseudowire fast-failure detection capability in a bidirectional forwarding detection (BFD) configuration, use the **monitor peer bfd** command in pseudowire class configuration mode. To disable pseudowire fast-failure detection, use the **no** form of this command.

monitor peer bfd [**local interface** *loopback-url*]

no monitor peer bfd

Syntax Description

local interface *loopback-url*	(Optional) Local interface for the source address to use when locating a BFD configuration.

Command Default

Pseudowire fast-failure detection is not enabled.

Command Modes

Pseudowire class (config-pw-class)

Command History

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

Examples

The following example shows how to enable pseudowire fast-failure detection capability:

```
Router# configure terminal
 interface Loopback0
  ip address 10.1.1.1 255.255.255.255
  !
  pseudowire-class mpls
  monitor peer bfd local interface Loopback0
```

Related Commands

Command	Description
bfd map	Configures a BFD map that associates timers and authentication with multihop templates.
bfd-template	Creates a BFD template and enters BFD configuration mode.
encapsulation (Any Transport over MPLS)	Configures the AAL encapsulation for AToM.
pseudowire-class	Specifies the name of a Layer 2 pseudowire class.

neighbor (L2VPN Pseudowire Switching)

To specify the routers that should form a point-to-point Layer 2 virtual forwarding interface (VFI) connection, use the **neighbor** command in L2 VFI point-to-point configuration mode. To disconnect the routers, use the **no** form of this command.

neighbor *ip-address vc-id* {**encapsulation mpls** |**pw-class** *pw-class-name*}

no neighbor *ip-address vc-id* {**encapsulation mpls** |**pw-class** *pw-class-name*}

Syntax Description

ip-address	IP address of the VFI neighbor.
vc-id	Virtual circuit (VC) identifier.
encapsulation mpls	Encapsulation type.
pw-class	Pseudowire type.
pw-class-name	Name of the pseudowire you created when you established the pseudowire class.

Command Default

Routers do not form a point-to-point Layer 2 VFI connection.

Command Modes

L2 VFI point-to-point configuration (config-vfi)

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

A maximum of two **neighbor** commands are allowed when you issue an **l2 vfi point-to-point** command.

Examples

The following example is a typical configuration of a Layer 2 VFI connection:

```
Router(config)# l2 vfi atom point-to-point
Router(config-vfi)# neighbor 10.10.10.10 1 encapsulation mpls
```

Related Commands

Command	Description
l2 vfi point-to-point	Establishes a point-to-point Layer 2 VFI between two separate networks.

neighbor (VPLS)

To specify the type of tunnel signaling and encapsulation mechanism for each Virtual Private LAN Service (VPLS) peer, use the **neighbor** command in L2 VFI manual configuration mode. To disable a split horizon, use the **no** form of this command.

neighbor *remote-router-id vc-id* {**encapsulation** *encapsulation-type* | **pw-class** *pw-name*} [**no-split-horizon**]

no neighbor *remote-router-id* [*vc-id*]

Syntax Description

remote-router-id	Remote peer router identifier. The remote router ID can be any IP address, as long as it is reachable.
vc-id	32-bit identifier of the virtual circuit between the routers.
encapsulation	Specifies tunnel encapsulation.
encapsulation-type	Specifies the tunnel encapsulation type; valid values are **l2tpv3** and **mpls**.
pw-class	Specifies the pseudowire class configuration from which the data encapsulation type is taken.
pw-name	Name of the pseudowire class.
no-split-horizon	(Optional) Disables the Layer 2 split horizon forwarding in the data path.

Defaults

Split horizon is enabled.

Command Modes

L2 VFI manual configuration (config-vfi)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. This command was updated so that the remote router ID need not be the LDP router ID of the peer.

Usage Guidelines

In a full-mesh VPLS network, keep split horizon enabled to avoid looping.

With the introduction of VPLS Autodiscovery, the remote router ID no longer needs to be the LDP router ID. The address that you specify can be any IP address on the peer, as long as it is reachable. When VPLS Autodiscovery discovers peer routers for the VPLS, the peer router addresses might be any routable address.

Examples

This example shows how to specify the tunnel encapsulation type:

```
Router(config-vfi)# l2 vfi vfi-1 manual
Router(config-vfi)# vpn 1
Router(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls
```

This example shows how to disable the Layer 2 split horizon in the data path:

```
Router(config-vfi)# l2 vfi vfi-1 manual
Router(config-vfi)# vpn 1
Router(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls no-split-horizon
```

Related Commands

Command	Description
l2 vfi manual	Creates a Layer 2 VFI.

oam-ac emulation-enable

To enable Operation, Administration, and Maintenance (OAM) cell emulation on ATM adaptation layer 5 (AAL5) over Multiprotocol Label Switching (MPLS) or Layer 2 Tunnel Protocol Version 3 (L2TPv3), use the **oam-ac emulation-enable command in the appropriate** configuration mode on both provider edge (PE) routers**.** To disable OAM cell emulation, use the **no** form of this command on both routers.

oam-ac emulation-enable [*seconds*]

no oam-ac emulation-enable [*seconds*]

Syntax Description

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

Command Default

OAM cell emulation is disabled.

Command Modes

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

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(30)S	This command was updated to enable OAM cell emulation as part of a virtual circuit (VC) class.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command is used with AAL5 over MPLS or L2TPv3 and is not supported with ATM cell relay over MPLS or L2TPv3.

Examples

The following example shows how to enable OAM cell emulation on an ATM permanent virtual circuit (PVC):

```
Router# interface ATM 1/0/0
Router(config-if)# pvc 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 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 10.13.13.13 100 encapsulation mpls
```

Related Commands

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

optimize

To apply WAAS Express optimization, use the **optimize** command in QoS policy-map configuration mode. To remove the optimization, use the **no** form of this command.

optimize tfo{**dre** | **lz**} **application** *application-name*

no optimize tfo{**dre** | **lz**} **application** *application-name*

Syntax Description

tfo	Applies Transport Flow Optimization (TFO) only.
dre	Applies Data Redundancy Elimination (DRE) and TFO.
lz	Applied Lempel-Ziv (LZ) and TFO.
application *application-name*	Class-map application name.

Command Default

The default optimization is pass-through.

Command Modes

QoS policy-map class configuration (config-pmap-c)

Command History

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

Usage Guidelines

Use this command to apply optimizations for WAN traffic.

Cisco WAAS Express uses a variety of TFO features to optimize TCP traffic intercepted by the WAAS devices. TFO protects communicating clients and servers from negative WAN conditions, such as bandwidth constraints, packet loss, congestion, and retransmission. Cisco WAAS Express uses the following optimization technologies based on the type of traffic it encounters:

- TFO—A collection of optimization technologies such as automatic windows scaling, increased buffering, and selective acknowledgment that optimize all TCP traffic over your network.
- DRE—A compression technology that reduces the size of transmitted data by removing redundant information before sending the shortened data stream over the WAN. DRE operates on significantly larger streams and maintains a much larger compression history than LZ compression.
- LZ—A compression technology that operates on smaller data streams and keeps limited compression history compared to RE.

Note If you do not use this command, pass-through optimization is applied on the WAN traffic.

Examples

This example creates a new policy with WAAS Express actions and application tagging:

```
Router(config)# policy-map type waas_global
```

```
Router(config-pmap)# class AFS
Router(config-pmap-c)# optimize tfo lz application Filesystem
Router(config-pmap-c)# exit
Router(config-pmap)# class Http
Router(config-pmap-c)# optimize tfo dre lz application Web
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

Related Commands

Command	Description
class	Associates a map class with a specified DLCI.
passthrough	Allows traffic without optimization.
policy-map type waas	Defines a WAAS Express policy map.
sequence-interval	Assigns sequential numbering to the class maps.

packet drop during-authorization

To specify that packets received from the user during authorization will be dropped, use the **packet drop during-authorization** command in transparent auto-logon configuration mode. To remove the configuration, use the **no** form of this command.

packet drop during-authorization

no packet drop during-authorization

Syntax Description

This command has no arguments or keywords.

Defaults

Packet drop during authorization is disabled, and packets from the authorizing user are forwarded.

Command Modes

Transparent auto-logon configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Use this command for configuring data traffic packet drop for users that are waiting for authorization (WA).

Examples

The following example specifies that packets received from the user during authorization will be dropped:

```
Router(config-login-transparent)# packet drop during-authorization
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

parameter-map type waas

To configure WAAS Express global parameters, use the **parameter-map type waas** command in global configuration mode. To remove global parameters, use the **no** form of this command.

parameter-map type waas *parameter-map-name*

no parameter-map type waas *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map. **Note** The only parameter-map type supported is **waas_global**.

Command Default

Global parameters are not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command extends the **parameter-map type** command and enters parameter-map configuration mode. The parameter map type of WAAS can be deleted only if WAAS Express is not enabled on any interface.

Examples

The following example shows how to configure global parameters for WAAS Express:

```
Router> enable
Router# configure terminal
Router(config)# parameter-map type waas waas_global
```

Related Commands

Command	Description
class-map type waas	Configures a WAAS Express class map.
cpu-threshold	Sets the CPU threshold limit.
lz entropy-check	Enables entropy checking to turn on LZ compression.
parameter-map type	Creates or modifies a parameter map.
policy-map type waas	Configures WAAS Express policy map.
tfo auto-discovery blacklist	Configures a blacklist with autodiscovery for WAAS Express.
tfo optimize	Configures compression for WAAS Express.
waas config	Restores or removes WAAS Express default configurations.

passthrough

To pass through match traffic and not apply the WAN optimization, use the **passthrough** command in QoS policy-map class configuration mode. To remove the default optimization, use the **no** form of this command.

passthrough application *application-name*

no passthrough application *application-name*

Syntax Description

application *application-name*	Specifies the class-map application name.

Command Default

The default optimization is pass-through.

Command Modes

QoS policy-map class configuration (config-pmap-c)

Command History

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

Usage Guidelines

Use this command if you do not want to specify any optimizations such as Transport Flow Optimization (TFO), Data Redundancy Elimination (DRE), and Lempel-Ziv (LZ) for WAN traffic.

Examples

The following example shows how to specify pass-through optimization for Instant-Messaging:

```
Router(config)# policy-map type waas waas_global
Router(config-pmap)# sequence-interval 111
Router(config-pmap-c)# optimize tfo dre lz application File-System
Router(config-pmap-c)# passthrough application Instant-Messaging
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
class	Associates a map class with a specified DLCI.
policy-map type waas	Defines a WAAS Express policy map.
optimize	Applies WAAS optimization.
sequence-interval	Assigns sequential numbering to class maps.

password

To configure the password used by a provider edge (PE) router for Challenge Handshake Authentication Protocol (CHAP) style Layer 2 Tunnel Protocol Version 3 (L2TPv3) authentication, use the **password** command in L2TP class configuration mode. To disable a configured password, use the **no** form of this command.

password [**0** | **7**] *password*

no password

Syntax Description

[0 | 7]	(Optional) Specifies the input format of the shared secret. • **0**—Specifies that a plain-text secret will be entered. • **7**—Specifies that an encrypted secret will be entered. The default value is **0**.
password	The password used for L2TPv3 authentication.

Defaults

If a password is not configured for the L2TP class with the **password** command, the password configured with the **username password** command in global configuration mode is used.
The default input format of the shared secret is **0**.

Command Modes

L2TP class configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The password hierarchy sequence used for a local and remote peer PE for L2TPv3 authentication is as follows:

- The L2TPv3 password (configured with the **password** command) is used first.
- If no L2TPv3 password exists, the globally configured password (configured with the **username password** command) for the router is used.

Note The use of a special character such as '\'(backslash) and a three or more digit number for the character setting like **password**, results in incorrect translation.

Examples

The following example sets the password named tunnel2 to be used to authenticate an L2TPv3 session between the local and remote peers in L2TPv3 pseudowires configured with the L2TP class configuration named l2tp class1:

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# authentication
Router(config-l2tp-class)# password tunnel2
```

Related Commands

Command	Description
authentication	Enables L2TPv3 CHAP-style authentication.
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.

password (L2TP)

To configure the password used by a provider edge (PE) router for Layer 2 authentication, use the **password** command in L2TP class configuration mode. To disable a configured password, use the **no** form of this command.

password [*encryption-type*] *password*

no password [*encryption-type*] *password*

Syntax Description

encryption-type	(Optional) Specifies the type of encryption to use. The valid values are from 0 to 7. Currently defined encryption types are 0 (no encryption) and 7 (text is encrypted using an algorithm defined by Cisco). The default encryption type is 0.
password	Specifies the password used for L2TPv3 authentication.

Command Default

If a password is not configured for the L2TP class with the **password** command, the password configured with the **username** command in global configuration mode is used.

Command Modes

L2TP class 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.
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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The password that you define with the **password** command is also used for attribute-value pair (AVP) hiding.

The password hierarchy sequence used for a local and remote peer PE for L2TPv3 authentication is as follows:

- The L2TPv3 password (configured with the **password** command) is used first.
- If no L2TPv3 password exists, the globally configured password (configured with the **username password** command) for the router is used.

Examples

The following example sets the password named "tunnel2" to be used to authenticate an L2TPv3 session between the local and remote peers in L2TPv3 pseudowires that has been configured with the L2TP class configuration named "l2tp-class1":

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# authentication
Router(config-l2tp-class)# password tunnel2
```

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.
username	Establishes a username-based authentication system.

platform trace runtime process forwarding-manager module mfr

To enable Forwarding Manager Route Processor and Embedded Service Processor trace messages for the multilink frame relay, use the **platform trace runtime process forwarding-manager module mfr** command in the global configuration mode. To disable the Forwarding Manager Route Processor and Embedded Service Processor debug messages, use the **no** form of this command.

platform trace runtime slot *slot* **bay** *bay* **process forwarding-manager module mfr level** {*level*}

no platform trace runtime slot *slot* **bay** *bay* **process forwarding-manager module mfr level** {*level*}

Syntax Description

slot	Shared Port Adapter (SPA) Interprocessor, Embedded Service Processor, or Route Processor slot. Valid options are: • F0—Embedded Service Processor slot 0 • R0—Route Processor slot 0 • F1—Embedded Service Processor slot 1 • R1—Route Processor slot 1
bay	Chassis bay to be configured. Valid options are: • 0 • 1
level *level*	Selects the trace level. The trace level determines the amount of information that should be stored about a module in the trace buffer or file. Valid options are: • **debug**—Provides debug-level output. • **emergency**—Provides information about an issue that makes the system unusable. • **error**—Provides information about a system error. • **info**—Provides informational messages. • **noise**—Provides all possible trace messages pertaining to the module. The noise level is always equal to the highest possible tracing level. • **notice**—Provides information regarding a significant issue, that does not, however, affect the normal functioning of the router. • **verbose**—Provides all possible tracing messages. • **warning**—Provides information about a system warning.

Command Default

The default tracing level for every module on the Cisco ASR 1000 Series Routers is notice.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines Trace-level settings are leveled, that is, every setting contains all the messages from the lower setting plus the messages from its own setting. For instance, setting the trace level to 3 (error) ensures that the trace file contains all the output for the 0 (emergencies), 1 (alerts), 2 (critical), and 3 (error) settings. Setting the trace level to 4 (warning) ensures that all the trace output for a specific module is included in that trace file.

All trace levels cannot be configured by users. Specifically, the alert, critical, and notice tracing levels cannot be set by users. To trace these messages, set the trace level to a higher level, which collects these messages.

When setting the trace levels, it is also important to remember that the setting is not done in a configuration mode. As a result of this, trace level settings are returned to their defaults after every router reload.

Caution Setting the tracing of a module to the debug level or higher can have a negative performance impact. Setting the tracing to the debug level or higher should be done with discretion.

Caution Setting a large number of modules to high tracing levels can severely degrade performance. If a high level of tracing is needed in a specific context, it is almost always preferable to set a single module on a higher tracing level rather than setting multiple modules to high tracing levels.

Examples In the following example, the trace level of the Forwarding Processor in the Forwarding Manager of the ESP processor in slot 0 is set to the informational tracing level (info):

```
Router(config)# platform trace runtime slot F0 bay 0 process forwarding-manager module mfr
level info
```

In the following example, the trace level for the Route Processor in the Forwarding Manager of the ESP processor in slot 0 is set to the informational tracing level (info):

```
Router(config)# platform trace runtime slot r0 bay 0 process forwarding-manager module mfr
level info
```

Related Commands

Command	Description
show platform software trace level	Displays the trace levels for specified modules.
show platform software trace message	Displays trace messages.

policy-map type mace

To configure a Measurement, Aggregation, and Correlation Engine (MACE) policy map and enter policy map configuration mode, use the **policy-map type mace** command in global configuration mode. To remove a MACE policy map, use the **no** form of this command.

policy-map type mace *name*

no policy-map type mace *name*

Syntax Description

name	Name of the MACE policy map. The only accepted value for this argument is **mace_global**.

Command Default

No MACE policy map is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

Use the **policy-map type mace** command to classify session traffic and run MACE on that traffic. Two types of class maps are supported in a MACE policy map:

- A quality of service (QoS) class map (default type class map)
- A Wide Area Application Services (WAAS) class map

The usage of QoS and WAAS class maps in the MACE policy is independent of QoS or WAAS policies being configured on the routers.

Inside a MACE policy map, you can configure a flow monitor name using only the **flow monitor** command. The name of the flow monitor is used to collect the corresponding flow metrics and to export these flow metrics when the cache timeout is updated.

Note Only one flow monitor can be configured in a class map.

Examples

The following example shows how to configure the MACE policy map, mace_global:

```
Router(config)# policy-map type mace mace_global
Router(config-pmap)# class class1
Router(config-pmap-c)# flow monitor name my-flow-monitor
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.
flow monitor	Creates or modifies a Flexible NetFlow flow monitor.
policy-map	Enters policy-map configuration mode, and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

policy-map type waas

To configure a WAAS Express policy map, use the **policy-map type waas** command in global configuration mode. To remove a WAAS Express policy-map, use the **no** form of this command.

policy-map type waas *policy-map-name*

no policy-map type waas *policy-map-name*

Syntax Description

policy-map-name	Name of the class map. **Note** The only policy-map type supported is **waas_global**.

Command Default

No WAAS Express policy maps are configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command extends the **policy-map** command and enters QoS policy-map configuration mode. The policy-map type of WAAS can be deleted only if WAAS Express is not enabled on any interface.

Examples

The following example shows how to configure a WAAS Express policy map:

```
Router> enable
Router# configure terminal
Router(config)# policy-map type waas waas_global
Router(config-pmap)# class waas_global
```

Related Commands

Command	Description
class	Associates a map class with a specified DLCI.
optimize	Applies optimization to WAN network traffic.
parameter-map type waas	Configures WAAS Express global parameters.
passthrough	Sends the network traffic without applying any optimization.
policy-map	Creates or modifies a policy map.
sequence-interval	Assigns sequential numbering to class maps.
waas config	Restores or removes WAAS Express default configurations.

precedence (Frame Relay VC-bundle-member)

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

precedence {*level* | **other**}

no precedence

Syntax Description

level	The precedence level or levels for the Frame Relay PVC bundle member. The range is from 0 to 7: • 0—routine • 1—priority • 2—immediate • 3—flash • 4—flash override • 5—critical • 6—internetwork control • 7—network control A PVC bundle member can be configured with a single precedence level, multiple individual precedence levels, a range of precedence levels, multiple ranges of precedence levels, or a combination of individual precedence levels and ranges. Examples are as follows: • 0 • 0,2,3 • 0-2,4-5 • 0,1,2-4,7
other	Specifies that this Frame Relay PVC bundle member will handle all of the remaining precedence levels that are not explicitly configured on any other bundle member PVCs.

Defaults

Precedence levels are not configured.

Command Modes

Frame Relay VC-bundle-member configuration

Command History

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

Usage Guidelines

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

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

This command is available only when the match type for the PVC bundle is set to precedence by using the **match precedence** command in Frame Relay VC-bundle configuration mode.

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

All precedence levels must be accounted for in the PVC bundle configuration, or the bundle will not come up. However, a PVC can be a bundle member without a precedence level associated with it. As long as all valid precedence levels are handled by other PVCs in the bundle, the bundle can come up, but the PVC that has no precedence level configured will not participate in it.

A precedence level can be configured on one PVC bundle member per bundle. If you configure the same precedence level on more than one PVC within a bundle, the following error appears on the console:

```
%Overlapping precedence levels
```

When you use the **mpls ip** command to enable multiprotocol label switching (MPLS) on the interface, MPLS and IP packets can flow across the interface, and PVC bundles that are configured for IP precedence mapping are converted to MPLS EXP mapping. The PVC bundle functionality remains the same with respect to priority levels, bumping, and so on, but the **match precedence** command is replaced by the **match exp** command, and each **precedence** command is replaced by the **exp** command. The result is that a bundle-member PVC previously configured to carry precedence level 1 IP traffic now carries EXP level 1 MPLS traffic.

When MPLS is disabled, the **match precedence** and **match dscp** commands are restored, and the **exp** commands are replaced by **precedence** commands.

When MPLS is enabled or disabled, PVC bundles configured for IP precedence mapping or MPLS EXP mapping will stay up, and traffic will be transmitted over the appropriate bundle-member PVCs.

Examples

The following example shows how to configure Frame Relay PVC bundle member 101 to carry traffic with IP precedence level 5:

```
frame-relay vc-bundle bundle1
 match precedence
 pvc 101
 precedence 5
```

Related Commands

Command	Description
bump	Configures the bumping rules for a specific PVC member of a bundle.
class	Associates a map class with a specified DLCI.
dscp (Frame Relay VC-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
exp	Configures MPLS EXP levels for a Frame Relay PVC bundle member.
match	Specifies which bits of the IP header to use for mapping packet service levels to Frame Relay PVC bundle members.
match dscp	Configures a specific IP differentiated service code point (DSCP) value as a match criterion.
match precedence	Configures IP precedence values as match criteria.
protect (Frame Relay VC-bundle-member)	Configures a Frame Relay PVC bundle member with protected group or protected PVC status.

protect (Frame Relay VC-bundle-member)

To configure a Frame Relay permanent virtual circuit (PVC) bundle member with protected group or protected PVC status, use the **protect** command in Frame Relay VC-bundle-member configuration mode. To remove the protected status from a PVC, use the **no** form of this command.

protect {**group** | **vc**}

no protect {**group** | **vc**}

Syntax Description

group	Configures the PVC bundle member as part of a collection of protected PVCs within the PVC bundle.
vc	Configures the PVC member as individually protected.

Command Default

The PVC is not in a protected group and is also not individually protected.

Command Modes

Frame Relay VC-bundle-member configuration

Command History

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

Usage Guidelines

When an individually-protected PVC goes down, it takes the bundle down. When all members of a protected group go down, the bundle goes down.

Despite any protection configurations, the PVC bundle will go down if a downed PVC has no PVC to which to bump its traffic or if the last PVC that is up in a PVC bundle goes down.

Examples

The following example configures Frame Relay PVC bundle member 101 as an individually protected PVC:

```
frame-relay vc-bundle new york
 pvc 101
  protect vc
```

Related Commands

Command	Description
bump	Configures the bumping rules for a specific PVC member of a bundle.
bundle	Creates a bundle or modifies an existing bundle to enter bundle configuration mode.
dscp (Frame Relay VC-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
exp	Configures MPLS EXP levels for a Frame Relay PVC bundle member.
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.

protocol (L2TP)

To specify the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session and to cause control plane configuration settings to be taken from a specified L2TP class, use the **protocol** command in pseudowire class configuration mode. To remove the signaling protocol (and the control plane configuration to be used) from a pseudowire class, use the **no** form of this command.

protocol {**l2tpv2** | **l2tpv3** | **none**} [*l2tp-class-name*]

no protocol {**l2tpv2** | **l2tpv3** | **none**} [*l2tp-class-name*]

Syntax Description

l2tpv2	Specifies that the Layer 2 Tunnel Protocol (L2TP) signaling protocol will be used.
l2tpv3	Specifies that the L2TPv3 signaling protocol will be used. This is the default.
none	Specifies that no signaling protocol will be used in L2TPv3 sessions.
l2tp-class-name	(Optional) The name of the L2TP class whose control plane configuration is to be used for pseudowires set up from a specified pseudowire class. If you do not enter a value for the *l2tp-class-name* argument, the default control plane configuration settings in the L2TP signaling protocol are used.

Command Default

The default protocol is **l2tpv3**.

Command Modes

Pseudowire class 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.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

Use the **protocol** (L2TP) command to configure the signaling protocol to use in sessions created from the specified pseudowire class. In addition, you can use this command to specify the L2TP class (see the "Configuring the Xconnect Attachment Circuit" section in the *Layer 2 Tunnel Protocol Version 3* feature document) from which the control plane configuration settings are to be taken.

Use the **protocol none** command to specify that no signaling will be used in L2TPv3 sessions created from the specified pseudowire class. This configuration is required for interoperability with a remote peer running the Universal Tunnel Interface (UTI).

Do not use this command if you want to configure a pseudowire class that will be used to create manual L2TPv3 sessions (see the "Static L2TPv3 Sessions" section in the *Layer 2 Tunnel Protocol Version 3* feature document).

Examples

The following example shows how to enter pseudowire class configuration mode and how to configure L2TPv3 as the signaling protocol. The control plane configuration used in the L2TP class named "class1" will be used to create dynamic L2TPv3 sessions for a VLAN xconnect interface.

```
Router(config)# pseudowire-class vlan-xconnect
Router(config-pw)# protocol l2tpv3 class1
```

Related Commands

Command	Description
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

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

peer-ip-address	The IP address of the remote peer.
vcid	The 32-bit identifier of the virtual circuit between the routers at each end of the Layer 2 control channel.
pw-class *pw-class-name*	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: • **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. To remove a pseudowire class configuration, use the **no** form of this command.

pseudowire-class [*pw-class-name*]

no pseudowire-class [*pw-class-name*]

Syntax Description

pw-class-name	(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 *pw-class-name* argument.

Command Default

No pseudowire classes are 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.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

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

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

The local interface name for each pseudowire class configured between a pair of PE routers can be the same or different.

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

Examples

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

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

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.

pvc (Frame Relay VC-bundle)

To create a permanent virtual circuit (PVC) that is a Frame Relay PVC bundle member, and to enter Frame Relay VC-bundle-member configuration mode, use the **pvc** command in Frame Relay VC-bundle configuration mode. To delete a PVC from the Frame Relay PVC bundle, use the **no** form of this command.

pvc *dlci* [*vc-name*]

no pvc *dlci* [*vc-name*]

Syntax Description

dlci	Data-link connection identifier (DLCI) number used to identify the PVC.
vc-name	(Optional) Alphanumeric name for the PVC.

Command Default

No PVC is defined.

Command Modes

Frame Relay VC-bundle configuration

Command History

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

Usage Guidelines

To use this command, you must first create a Frame Relay PVC bundle and enter Frame Relay VC-bundle configuration mode.

A PVC bundle must have at least one PVC for the bundle to come up. A PVC bundle cannot have more than eight PVCs. If you try to configure more than eight PVCs in a bundle, the following message appears on the console:

```
%FR vc-bundle contains 8 members. Cannot add another.
```

Dynamic PVCs can be specified as PVC bundle members; however, if a PVC has already been created by using another configuration command, you cannot add it to a PVC bundle. If you try to do so, the following message appears on the console:

```
%DLCI 200 is not a dynamic PVC. Cannot add to VC-Bundle.
```

If a PVC is already a member of a PVC bundle, any attempt to reuse that same PVC in a command that creates a PVC (for example, **frame-relay interface-dlci** or **frame-relay local-dlci**) causes the following error message:

```
%Command is inapplicable to vc-bundle PVCs.
```

Examples

The following example creates a PVC that has a DLCI number of 101 and that belongs to a Frame Relay PVC bundle named new_york:

```
frame-relay vc-bundle new_york
 pvc 101
```

Related Commands

Command	Description
dscp (frame-relay vc-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
exp	Configures MPLS EXP levels for a Frame Relay PVC bundle member.
frame-relay vc-bundle	Creates a Frame Relay PVC bundle and enters Frame Relay VC-bundle configuration mode.
match	Specifies which bits of the IP header to use for mapping packet service levels to Frame Relay PVC bundle members
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.

rd (VPLS)

To specify the route distinguisher (RD) to distribute endpoint information in a Virtual Private LAN Service (VPLS) configuration, use the **rd** command in L2 VFI configuration mode. To remove the manually configured RD and return to the automatically generated RD, use the **no** form of this command.

rd {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

no rd {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

Syntax Description

autonomous-system-number:nn	Specifies a 16-bit autonomous system number and 32-bit arbitrary number. The autonomous system number does not have to match the local autonomous system number.
ip-address:nn	Specifies a 32-bit IP address and a 16-bit arbitrary number. Only IPv4 addresses are supported.

Command Default

VPLS Autodiscovery automatically generates a route distinguisher using the Border Gateway Protocol (BGP) autonomous system number and the configured virtual forwarding instance (VFI) Virtual Private Network (VPN) ID.

Command Modes

L2 VFI configuration

Command History

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

Usage Guidelines

VPLS Autodiscovery automatically generates a route distinguisher using the BGP autonomous system number and the configured VFI VPN ID. You can use this command to change the automatically generated route distinguisher.

The same RD value cannot be configured in multiple VFIs.

There are two formats for configuring the route distinguisher argument. It can be configured in the *autonomous-system-number*:*network-number* format, or it can be configured in the *IP address*:*network-number* format.

An RD is either:

- autonomous system-related—Composed of an autonomous system number and an arbitrary number.
- IP address-related—Composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

16-bit-autonomous-system-number:*32-bit-number*
For example, 101:3.

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

Examples

The following example shows a configuration using VPLS Autodiscovery that sets the RD to an IP address of 10.4.4.4 and a network address of 70:

```
l2 vfi SP2 autodiscovery
 vpn id 200
 vpls-id 10.4.4.4:70
 rd 10.4.5.5:7
```

The following example shows a configuration using VPLS Autodiscovery that sets the RD to an autonomous system number of 2 and a network address of 3:

```
l2 vfi SP2 autodiscovery
 vpn id 200
 vpls-id 10.4.4.4:70
 rd 2:3
```

Related Commands

Command	Description
l2 vfi autodiscovery	Enable a VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.

receive-window

To configure the packet size of the receive window on the remote provider edge router at the other end of a Layer 2 control channel, use the **receive-window** command in L2TP class configuration mode. To disable the configured value, use the **no** form of this command.

receive-window *number*

no receive-window *number*

Syntax Description

number	The number of packets that can be received by the remote peer before backoff queueing occurs. The valid values range from 1 to the upper limit the peer has for receiving packets. The default value is the upper limit that the remote peer has for receiving packets.

Command Default

The default packet size of the receive window is the upper limit that the remote peer has for receiving packets.

Command Modes

L2TP class 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.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

To determine the upper limit for the *number* argument, refer to the platform-specific documentation for the peer router.

Examples

The following example sets a receive window of 30 packets to the remote peer in Layer 2 pseudowires that have been configured with the L2TP class named" l2tp-class1":

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# receive-window 30
```

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.

retransmit

To configure the retransmission settings of control packets, use the **retransmit** command in L2TP class configuration mode. To disable the configured values, use the **no** form of this command.

retransmit {**initial retries** *initial-retries* | **retries** *retries* | **timeout** {**max** | **min**} *seconds*}

no retransmit {**initial retries** *initial-retries* | **retries** *retries* | **timeout** {**max** | **min**} *seconds*}

Syntax Description

initial retries *initial-retries*	Specifies how many start control channel requests (SCCRQs) are re-sent before giving up on the session. Valid values for the *initial-retries* argument range from 1 to 1000. The default value is 2
retries *retries*	Specifies how many retransmission cycles occur before determining that the peer provider edge (PE) router does not respond. Valid values for the *retries* argument range from 1 to 1000. The default value is 15.
timeout {**max** | **min**} *seconds*	Specifies maximum and minimum retransmission intervals (in seconds) for resending control packets. Valid values for the *timeout* argument range from 1 to 8. The default maximum interval is 8; the default minimum interval is 1.

Command Default

The default values of the retransmission settings are used.

Command Modes

L2TP class 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.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

Use this command to configure the amount of time spent trying to establish or maintain a control channel.

Examples

The following example configures ten retries for sending tunneled packets to a remote peer in Layer 2 pseudowires that have been configured with the Layer 2 Tunnel Protocol (L2TP) class named "l2tp-class1":

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# retransmit retries 10
```

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.

rewrite ingress tag

To specify the encapsulation adjustment to be performed on a frame ingressing a service instance, use the **rewrite ingress tag** command in service instance configuration mode. To delete the encapsulation adjustment, use the **no** form of this command.

rewrite ingress tag {**pop** {**1** | **2**} [**symmetric**] | **push** {**dot1ad** *vlan-id* [**dot1q** *vlan-id*] [**symmetric**] | **dot1q** *vlan-id* [**second-dot1q** *vlan-id*] [**symmetric**]} | **translate** {**1-to-1** {**dot1ad** *vlan-id* | **dot1q** *vlan-id*} [**symmetric**] | **1-to-2** {**dot1ad** *vlan-id* **dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id*} [**symmetric**] | {**2-to-1** {**dot1ad** *vlan-id* | **dot1q** *vlan-id*} [**symmetric**] | **2-to-2** {**dot1ad** *vlan-id* **dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id*} [**symmetric**]}

no rewrite ingress tag

Syntax on the Cisco ASR 1000 Series Aggregation Router

rewrite ingress tag {**pop** {**1** | **2**} [**symmetric**] | **push** {**dot1ad** *vlan-id* [**dot1q** *vlan-id*] [**symmetric**] | **dot1q** *vlan-id* [**second-dot1q** *vlan-id*] [**symmetric**] | **vlan-type** {**0x88a8** | **0x9100** | **0x9200**} [**second-dot1q** *vlan-id*] [**symmetric**]} | **translate** {**1-to-1** {**dot1ad** *vlan-id* | **dot1q** *vlan-id* [**vlan-type** {**0x88a8** | **0x9100** | **0x9200**}] [**symmetric**]} | **1-to-2** {**dot1ad** *vlan-id* **dot1q** *vlan-id* | **dot1q** *vlan-id* {**second-dot1q** *vlan-id* | **vlan-type** {**0x88a8** | **0x9100** | **0x9200**} **second-dot1q** *vlan-id*}} [**symmetric**] | **2-to-1** {**dot1ad** *vlan-id* [**symmetric**] | **dot1q** *vlan-id* [**vlan-type** {**0x88a8** | **0x9100** | **0x9200**}] [**symmetric**]} | **2-to-2** {**dot1ad** *vlan-id* **dot1q** *vlan-id* [**symmetric**] | **dot1q** *vlan-id* {**second-dot1q** *vlan-id* | **vlan-type** {**0x88a8** | **0x9100** | **0x9200**} **second-dot1q** *vlan-id*} [**symmetric**]}}

no rewrite ingress tag

Syntax Description

pop	Removes a tag from a packet.
{**1** | **2**}	Specifies either the outermost tag or the two outermost tags for removal from a packet.
symmetric	(Optional) Indicates a reciprocal adjustment to be done in the egress direction. For example, if the ingress pops a tag, the egress pushes a tag and if the ingress pushes a tag, the egress pops a tag.
push	Adds a tag.
dot1ad	Specifies an IEEE 802.1ad tag.
vlan-id	Integer in the range 1 to 4094 that identifies the VLAN.
dot1q	Specifies an IEEE 802.1Q tag.
second-dot1q	Specifies a different 802.1Q tag at the ingress service instance.
vlan-type	Specifies the type of VLAN protocol.
0x88a8	Specifies the protocol type 0x88a8.
0x9100	Specifies the protocol type 0x9100.
0x9200	Specifies the protocol type 0x9200.
translate	Translates, by VLAN ID, a tag or a pair of tags defined in the **encapsulation** command.

1-to-1	Translates a single tag defined by the **encapsulation** command to a single tag defined in the **rewrite ingress tag** command.
1-to-2	Translates a single tag defined by the **encapsulation** command to a pair of tags defined in the **rewrite ingress tag** command.
2-to-1	Translates, by VLAN ID, a pair of tags defined by the **encapsulation** command to a single tag defined in the **rewrite ingress tag** command.
2-to-2	Translates, by VLAN ID, a pair of tags defined by the **encapsulation** command to a pair of tags defined in the **rewrite ingress tag** command.

Command Default

The frame is left intact on ingress (the service instance is equivalent to a trunk port).

Command Modes

Service instance configuration (config-if-srv)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The **symmetric** keyword is accepted for all rewrite operations only when a single VLAN is configured in encapsulation. If a list of VLANs or a range of VLANs is configured in encapsulation, the **symmetric** keyword is accepted only for push rewrite operations.

The **pop** keyword assumes the elements being popped are defined by the encapsulation type. The exception case should be drop the packet.

The **translate** keyword assumes the tags being translated from are defined by the encapsulation type. In the 2-to-1 option, the "2" means 2 tags of a type defined by the **encapsulation** command. The translation operation requires at least one "from" tag in the original packet. If the original packet contains more tags than the ones defined in the "from," the operation should be done beginning on the outer tag. Exception cases should be dropped.

Examples

The following example shows how to specify the encapsulation adjustment to be performed on the frame ingressing the service instance:

```
Router> enable
Router# configure terminal
Router(config) interface gigabitethernet 2/0/0
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# rewrite ingress tag push dot1q 200
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by an interface.

route-target (VPLS)

To specify a route target (RT) for a Virtual Private LAN Service (VPLS) virtual forwarding instance (VFI), use the **route-target** command in L2 VFI configuration mode. To revert to the automatically-generated route target, use the **no** form of this command.

route-target [**import** | **export** | **both**] {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

no route-target {**import** | **export** | **both**} {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

Syntax Description

import	(Optional) Imports routing information from the target virtual private network (VPN) extended community.
export	(Optional) Exports routing information to the target VPN extended community.
both	(Optional) Imports both import and export routing information to the target VPN extended community.
autonomous-system-number:*nn*	The autonomous system number and a 32-bit number.
ip-address:*nn*	The IP address and a 16-bit number.

Defaults

VPLS Autodiscovery automatically generates a route target using the lower six bytes of the route distinguisher (RD) and VPLS ID.

Command Modes

L2 VFI configuration

Command History

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

Usage Guidelines

The same route target cannot be configured in multiple VFIs.

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

16-bit-autonomous-system-number:*32-bit-number*
For example, 101:3.

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

Examples

The following example shows a VPLS Autodiscovery configuration that configures route-target extended community attributes for VFI SP1:

```
l2 vfi SP1 autodiscovery
 vpn id 100
 vpls-id 5:300
 rd 4:4
 route-target 10.1.1.1:29
```

Related Commands

Command	Description
auto-route-target	Automatically generates the route target in a VFI.
l2 vfi autodiscovery	Enable a VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.

rtcp-regenerate

To generate and terminate the RTCP packets on the SPA-DSP, use the **rtcp-regenerate** command in the SBC configuration mode (config-sbc) for the Unified Model, and from the SBC DBE configuration mode (config-sbc-dbe) for the Distributed Model.

rtcp-regenerate

no rtcp-regenerate

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

SBC configuration (config-sbc) for the Unified Model

SBC DBE configuration (config-sbc-dbe) for the Distributed Model

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

Use this command to generate and terminate the RTCP packets on the SPA-DSP on a Cisco ASR 1000 Series Router.

Examples

The following example shows how to generate and terminate the RTCP packets on the SPA-DSP on the Cisco Unified Border Element: Unified Model:

```
Router> enable
Router# config terminal
Router(config)# sbc mySBC
Router(config-sbc)# rtcp-regenerate
```

The following example shows how to generate and terminate the RTCP packets on the SPA-DSP on the Cisco Unified Border Element: Distributed Model:

```
Router> enable
Router# config terminal
Router(config)# sbc mySBC dbe
```