CHAPTER 2

CLI Command Reference

Revised: January 28, 2014, OL-31200-01

This chapter contains an alphabetical listing of commands for the Cisco ASR 901S Series Aggregation Services Router.

> **Note** For a general reference for Cisco IOS, see the documentation for Cisco IOS Software Releases 15.1S. The Cisco ASR 901S does not necessarily support all of the commands listed in the 15.1S documentation.

- asr901-ecmp-hash-config global-type
- asr901-ecmp-hash-config ipv4-type
- asr901-ecmp-hash-config ipv6-type
- asr901-ecmp-hash-config mpls-to-ip
- asr901-multicast source
- asr901-platf-frr enable
- asr901-platf-multicast enable
- asr901-platf-multi-nni-cfm
- bfd all-interfaces
- bfd interval
- channel-group (interface)
- channel-protocol (interface)
- class (policy-map)
- clear platform ptp stats
- clear platform ptp stats
- clock-port
- clock-destination
- clock source (interface)
- debug platform tcam error
- debug platform tcam error
- debug platform tcam error

- show policy-map interface
- show ptp port running detail
- show rep topology
- show table-map
- show xconnect
- snmp mib rep trap-rate
- speed
- synce state master
- synce state slave
- synchronous mode
- table-map
- termination
- transport ipv4
- tune-buffer port
- xconnect logging redundancy

asr901-ecmp-hash-config global-type

To specify the equal-cost multi-path routing (ECMP) hashing algorithm at the global level, use the **asr901-ecmp-hash-config global-type** command in global configuration mode. To remove this configuration, use the **no** form of this command.

asr901-ecmp-hash-config global-type {**hash-crc16-mode** | **hash-seed** *seed-value* | **hash-xor1-mode** | **hash-xor2-mode** | **hash-xor4-mode** | **hash-xor8-mode** | **tunnel-mode**} **add**

no asr901-ecmp-hash-config global-type {**hash-crc16-mode** | **hash-seed** *seed-value* | **hash-xor1-mode** | **hash-xor2-mode** | **hash-xor4-mode** | **hash-xor8-mode** | **tunnel-mode**} **add**

Syntax Description

hash-crc16-mode	Enables hash CRC-16 modes.
hash-seed	Enables hash seed value for hash computation.
seed-value	Hash seed value.
hash-xor1-mode	Enables hash XOR1 mode.
hash-xor2-mode	Enables hash XOR2 mode.
hash-xor4-mode	Enables hash XOR4 mode.
hash-xor8-mode	Enables hash XOR8 mode.
tunnel-mode	Enables tunnel mode to look into the inner header for tunneled packets.
add	Adds hash mode.

Command Default

The hash-crc16-mode algorithm is enabled by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.3(2)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Usage Guidelines

This command is used to configure the ECMP hash configurations for improved load distribution of IP traffic. The **hash-crc16-mode algorithm** is enabled by default for ECMP.

Examples

The following example shows how to configure the ECMP hash configuration on a Cisco ASR 901 router:

```
Router# configure terminal
Router(config)# asr901-ecmp-hash-config global-type hash-xor1-mode
Router(config)# asr901-ecmp-hash-config global-type hash-xor1-mode add
```

Related Commands

Command	Description
asr901-ecmp-hash-config ipv4-type	Enables the ipv4-type of ECMP hash configurations.
asr901-ecmp-hash-config ipv6-type	Enables the ipv6-type of ECMP hash configurations.
asr901-ecmp-hash-config mpls-to-ip	Enables the mpls-to-ip type of ECMP hash configurations.

asr901-ecmp-hash-config ipv4-type

To specify equal-cost multi-path routing (ECMP) hashing algorithm for IPv4 configuration, use the **asr901-ecmp-hash-config ipv4-type** command in global configuration mode. To remove this configuration, use the **no** form of this command.

asr901-ecmp-hash-config ipv4-type {**dest-addrs** | **dest-l4-port** | **l3-proto-id** | **outer-vlan** | **src-addrs** | **src-intf** | **src-l4-port**} **add**

no asr901-ecmp-hash-config ipv4-type {**dest-addrs** | **dest-l4-port** | **l3-proto-id** | **outer-vlan** | **src-addrs** | **src-intf** | **src-l4-port**} **add**

Syntax Description

dest-addrs	Specifies the destination IPv4 address.
dest-l4-port	Specifies the destination Layer 4 port.
l3-proto-id	Specifies the Layer 3 protocol identifier.
outer-vlan	Specifies the outer virtual local area network (VLAN).
src-addrs	Specifies the source IPv4 address.
src-intf	Specifies the source or the incoming interface.
src-l4-port	Specifies the source Layer 4 port.
add	Adds IPv4 ECMP hash configuration.

Command Default

The ECMP parameters, such as **dest-l4-port**, **src-intf**, and **src-l4-port**, are disabled by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.3(2)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Usage Guidelines

This command is used to configure IPv4 type ECMP hash configurations for improved load distribution of IP traffic. All the ECMP parameters are enabled by default except **dest-l4-port**, **src-intf**, and **src-l4-port**. You should configure the **asr901-ecmp-hash-config ipv4-type** command to enable them.

Examples

The following example shows how to configure IPv4 type ECMP hash configuration on a Cisco ASR 901 router:

```
Router# configure terminal
Router(config)# asr901-ecmp-hash-config ipv4-type dest-addrs
Router(config)# asr901-ecmp-hash-config ipv4-type dest-addrs add
```

Related Commands

Command	Description
asr901-ecmp-hash-config global-type	Enables the global-type of ECMP hash configurations.
asr901-ecmp-hash-config ipv6-type	Enables the ipv6-type of ECMP hash configurations.
asr901-ecmp-hash-config mpls-to-ip	Enables the mpls-to-ip type of ECMP hash configurations.

asr901-ecmp-hash-config ipv6-type

To specify equal-cost multi-path routing (ECMP) hashing algorithm for IPv6 configuration, use the **asr901-ecmp-hash-config ipv6-type** command in global configuration mode. To remove this configuration, use the **no** form of this command.

asr901-ecmp-hash-config ipv4-type {**dest-addrs** | **dest-l4-port** | **ipv6-next-header** | **outer-vlan** | **src-addrs** | **src-intf** | **src-l4-port**} **add**

no asr901-ecmp-hash-config ipv4-type {**dest-addrs** | **dest-l4-port** | **ipv6-next-header** | **outer-vlan** | **src-addrs** | **src-intf** | **src-l4-port**} **add**

Syntax Description

dest-addrs	Specifies the destination IPv6 address.
dest-l4-port	Specifies the destination Layer 4 port.
ipv6-next-header	Specifies the source or the incoming interface.
outer-vlan	Specifies the outer virtual local area network (VLAN).
src-addrs	Specifies the source IPv4 address.
src-intf	Specifies the source or the incoming interface.
src-l4-port	Specifies the source Layer 4 port.
add	Adds IPv6 ECMP hash configuration.

Command Default

The ECMP parameters, such as **dest-l4-port**, **src-intf**, and **src-l4-port**, are disabled by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.3(2)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Usage Guidelines

This command is used to configure IPv6-type ECMP hash configurations for improved load distribution of IP traffic. All the ECMP parameters are enabled by default except **dest-l4-port**, **src-intf**, and **src-l4-port**. You should configure the **asr901-ecmp-hash-config ipv6-type** command to enable them.

Examples

The following example shows how to configure IPv6-type ECMP hash configuration on a Cisco ASR 901 router:

```
Router# configure terminal
Router(config)# asr901-ecmp-hash-config ipv6-type dest-addrs
Router(config)# asr901-ecmp-hash-config ipv6-type dest-addrs add
```

Related Commands

Command	Description
asr901-ecmp-hash-config global-type	Enables the global-type of ECMP hash configurations.
asr901-ecmp-hash-config ipv4-type	Enables the IPv4-type of ECMP hash configurations.
asr901-ecmp-hash-config mpls-to-ip	Enables the mpls-to-ip type of ECMP hash configurations.

asr901-ecmp-hash-config mpls-to-ip

To specify equal-cost multi-path routing (ECMP) hashing algorithm for Multiprotocol Label Switching (MPLS) to IP configuration, use the **asr901-ecmp-hash-config mpls-to-ip** command in global configuration mode. To remove this configuration, use the **no** form of this command.

asr901-ecmp-hash-config mpls-to-ip {**dest-addrs** | **dest-l4-port** | **l3-proto-id** | **outer-vlan** | **src-addrs** | **src-intf** | **src-l4-port**} **add**

no asr901-ecmp-hash-config mpls-to-ip {**dest-addrs** | **dest-l4-port** | **l3-proto-id** | **outer-vlan** | **src-addrs** | **src-intf** | **src-l4-port**} **add**

Syntax Description

dest-addrs	Specifies the destination IPv4 address.
dest-l4-port	Specifies the destination Layer 4 port.
l3-proto-id	Specifies the Layer 3 protocol ID.
outer-vlan	Specifies the outer virtual local area network (VLAN).
src-addrs	Specifies the source IPv4 address.
src-intf	Specifies the source or the incoming interface.
src-l4-port	Specifies the source Layer 4 port.
add	Adds ECMP hash configuration.

Command Default

The ECMP parameters, such as **dest-l4-port**, **src-intf**, and **src-l4-port**, are disabled by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.3(2)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Usage Guidelines

This command is used to configure MPLS to IP-type ECMP hash configurations. All the ECMP parameters are enabled by default except **dest-l4-port**, **src-intf**, and **src-l4-port**. You should configure the **asr901-ecmp-hash-config mpls-to-ip** command to enable them.

Examples

The following example shows how to configure MPLS to IP-type ECMP hash configuration on a Cisco ASR 901 router:

```
Router# configure terminal
Router(config)# asr901-ecmp-hash-config mpls-to-ip dest-addrs
Router(config)# asr901-ecmp-hash-config mpls-to-ip dest-addrs add
```

Related Commands

Command	Description
asr901-ecmp-hash-config global-type	Enables the global-type of ECMP hash configurations.
asr901-ecmp-hash-config ipv4-type	Enables the IPv4-type of ECMP hash configurations.
asr901-ecmp-hash-config ipv6-type	Enables the IPv6-type of ECMP hash configurations.

asr901-multicast source

To send the multicast packets to the CPU enabling it to transmit register packets to Rendezvous Point (RP), use the **asr901-multicast source** command on the interface configuration mode. Use the **no** form of the command to disable transmission of multicast packets.

asr901-multicast source

no asr901-multicast source

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Interface configuration (config-if)#

Command History

Release	Modification
15.4(1)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Usage Guidelines

This command should be enabled on the SVI interface that is connected to the traffic source. After the configuration, normal Protocol Independent Multicast sparse mode (PIM-SM) register process begins.

Examples

This example shows how to enable multicast on a Cisco ASR 901 series router:

```
Router# configure terminal
Router(config)# interface type number
Router(config-if)# asr901-multicast source
```

asr901-platf-frr enable

To enable traffic engineering (TE) Fast Reroute (FRR) link protection on the Cisco ASR 901S router, use the **asr901-platf-frr** command in global configuration mode. To delete this configuration, use the **no** form of this command.

asr901-platf-frr enable

no asr901-platf-frr enable

Syntax Description

This command has no arguments or keywords.

Command Default

The TE-FRR functionality is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)SNG	This command was introduced.

Examples

The following example shows how to enable TE-FRR on the Cisco ASR 901S router:

```
Router# configure terminal
Router#(config) asr901-platf-frr enable
```

asr901-platf-multicast enable

To enable multicast on the Cisco ASR 901S series routers, use the **asr901-platf-multicast enable** command. Use the **no** form of the command to disable multicast.

asr901-platf-multicast enable

no asr901-platf-multicast enable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.4(1)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Usage Guidelines

This command is used to enable platform multicast on a Cisco ASR 901 series router.

Examples

This example shows how to enable multicast on a Cisco ASR 901 series router:

```
Router# configure terminal
Router(config)# ip multicast-routing
Router(config)# asr901-platf-multicast enable
```

Related Commands

Command	Description
show asr901 multicast-support	Displays the platform support for IPv4 or IPv6 multicast on the Cisco ASR 901S series routers.

asr901-platf-multi-nni-cfm

To enable the multi-Network-to-Network Interface Connectivity Fault Management (multi-NNI CFM) configuration, use the **asr901-platf-multi-nni-cfm** command. Use the **no** form of the command to enable the Synthetic Loss Measurement (SLM) over cross connect EVC configuration.

asr901-platf-multi-nni-cfm

no asr901-platf-multi-nni-cfm

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.3(3)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Usage Guidelines

This command is used to enable multi-NNI CFM configuration or SLM over cross connect EVC configuration on a Cisco ASR 901 router. You can configure by enabling or disabling the command. By default, the multi-NNI CFM configuration is enabled. When you run the required command , a syslog is generated so that you can save the configuration and reload the router. You should reload the router after using the **asr901-multi-nni-cfm** command or **no** form of the command.

Examples

This example shows how to enable multi-NNI CFM over cross connect EVC configuration on a Cisco ASR 901 router:

```
Router# configure terminal
Router(config)# asr901-platf-multi-nni-cfm
```

This example shows how to enable SLM over cross connect EVC configuration on a Cisco ASR 901 router:

```
Router# configure terminal
Router(config)# no asr901-platf-multi-nni-cfm
```

bfd all-interfaces

To enable Bidirectional Forwarding Detection (BFD) for all interfaces participating in the routing process, use the **bfd all-interfaces** command in router configuration mode. To disable BFD for all interfaces, use the **no** form of this command.

bfd all-interfaces

no bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is not enabled on the interfaces participating in the routing process.

Command Modes

Router configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

There are two methods to configure routing protocols to use BFD for failure detection. To enable BFD for all neighbors of a routing protocol, enter the **bfd all-interfaces** command in router configuration mode. If you do not want to enable BFD on all interfaces, enter the **bfd interface** command in router configuration mode.

Examples

The following example shows BFD enabled for all Intermediate System-to-Intermediate System (IS-IS) neighbors:

```
Router> enable
Router# configure terminal
Router(config)# router isis tag1
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

The following example shows BFD enabled for all Open Shortest Path First (OSPF) neighbors:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 123
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
bfd interface	Enables BFD on a per-interface basis for a BFD peer.

bfd interval

To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the **bfd** command in interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command.

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

Syntax Description

interval *milliseconds*	Specifies the rate at which BFD control packets will be sent to BFD peers. The configurable time period for the *milliseconds* argument is from 50 to 999 milliseconds (ms).
min_rx *milliseconds*	Specifies the rate at which BFD control packets will be expected to be received from BFD peers. The configurable time period for the *milliseconds* argument is from 1 to 999 milliseconds (ms).
multiplier *multiplier-value*	Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The configurable value range for the *multiplier-value* argument is from 3 to 50.

Command Default

No baseline BFD session parameters are set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Examples

The following example shows the BFD session parameters set for Fast Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config)# interface vlan1
Router(config-if)# bfd interval 50 min_rx 3 multiplier 3
Router(config-if)# end
```

Related Commands

Command	Description
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.
bfd interface	Enables BFD on a per-interface basis for a BFD peer.
ip ospf bfd	Enables BFD on a specific interface configured for OSPF.

channel-group (interface)

To assign and configure an EtherChannel interface to an EtherChannel group, use the channel-group command in interface configuration mode. To remove the channel-group configuration from the interface, use the no form of this command.

channel-group *number* **mode {active | on | passive}**

no channel-group *number*

Syntax Description

number	Integer that identifies the channel-group. Valid values are from 1 to 256; the maximum number of integers that can be used is 64. For Fast EtherChannel groups, the number is an integer from 1 to 4. This number is the one previously assigned to the port-channel interface.
mode	Specifies the EtherChannel mode of the interface.
active	Enables Link Aggregation Control Protocol (LACP) unconditionally.
on	Enables EtherChannel only.
passive	Enables LACP only when an LACP device is detected. This is the default state.

Command Default

No channel groups are assigned.

Command Modes

Interface configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The on Keyword

When you use the **on** keyword, a usable EtherChannel exists only when a port group in on mode is connected to another port group in the on mode.

You can change the **mode** for an interface only if it is the only interface that is designated to the specified channel group.

The **on** keyword forces the bundling of the interface on the channel without any negotiation.

With the **on** mode, a usable EtherChannel exists only when a port group in on mode is connected to another port group in on mode.

If you enter the **channel-group** command on an interface that is added to a channel with a different protocol than the protocol you are entering, the command is rejected.

If the interface belongs to a channel, the **no** form of this command is rejected.

All ports in the same channel group must use the same protocol; you cannot run two protocols on one channel group.

You can change the protocol at any time, but this change causes all existing EtherChannels to reset to the default channel mode for the new protocol.

Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode).

All ports in a channel must be on the same DFC-equipped module. You cannot configure any of the ports to be on other modules.

On systems that are configured with nonfabric-enabled modules and fabric-enabled modules, you can bundle ports across all modules, but those bundles cannot include a DFC-equipped module port.

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

You do not have to disable the IP address that is assigned to a physical interface that is part of a channel group, but it is highly recommended.

You can create both Layer 2 and Layer 3 port channels by entering the interface port-channel command or when the channel group gets its first physical interface assignment. The port channels are not created at runtime or dynamically.

Any configuration or attribute changes that you make to the port-channel interface are propagated to all interfaces within the same channel group as the port channel (for example, configuration changes are also propagated to the physical interfaces that are not part of the port channel but are part of the channel group).

When configuring Layer 2 EtherChannels, you cannot put Layer 2 LAN ports into manually created port-channel logical interfaces.

Caution Caution Do not enable Layer 3 addresses on the physical EtherChannel interfaces. Assigning bridge groups on the physical EtherChannel interfaces causes loops in your network.

Examples

This example shows how to add EtherChannel interface 1/0 to the EtherChannel group that is specified by port-channel 1:

```
Router(config-if)# channel-group 1 mode on
Router(config-if)#
```

Related Commands

Command	Description
interface	Creates a port-channel virtual interface and puts the CLI in interface configuration mode when the port-channel keyword is used.
ip address	Sets a primary or secondary IP address on an interface.
show etherchannel	Displays the EtherChannel information for a channel.
show interfaces port-channel	Displays traffic that is seen by a specific port channel.

channel-protocol (interface)

To enable Link Aggregation Control Protocol (LACP) on an interface to manage channeling, use the **channel-protocol** command in interface configuration mode. Use the **no** form of this command to deselect the protocol.

channel-protocol {lacp}

no channel-protocol

Syntax Description

lacp	Specifies LACP to manage channeling.

Command Modes

Interface configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

This command is valid on multiple interfaces (for example, Fast Ethernet) and routers and switches.

Examples

The following example shows how to set the lacp.

```
(config-if)# channel-protocol lacp
```

class (policy-map)

To specify the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class** command in policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

class {*class-name* | **class-default**}

no class {*class-name* | **class-default**}

Syntax Description

class-name	Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.
class-default	Specifies the default class so that you can configure or modify its policy.

Command Default

No class is specified.

Command Modes

Policy-map configuration (config-pmap)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Policy Map Configuration Mode

Within a policy map, the **class** (policy-map) command can be used to specify the name of the class whose policy you want to create or change. First, the policy map must be identified.

To identify the policy map (and enter the required policy-map configuration mode), use the **policy-map** command before you use the **class** (policy-map) command. After you specify a policy map, you can configure policy for new classes or modify the policy for any existing classes in that policy map.

Class Characteristics

The class name that you specify in the policy map ties the characteristics for that class—that is, its policy—to the class map and its match criteria, as configured using the **class-map** command.

When you configure policy for a class and specify its bandwidth and attach the policy map to an interface, class-based weighted fair queueing (CBWFQ) determines if the bandwidth requirement of the class can be satisfied. If so, CBWFQ allocates a queue for the bandwidth requirement.

When a class is removed, available bandwidth for the interface is incremented by the amount previously allocated to the class.

The maximum number of classes that you can configure for a router—and, therefore, within a policy map—is 64.

Predefined Default Class

The **class-default** keyword is used to specify the predefined default class called class-default. The class-default class is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

Examples

The following example configures a class policy included in the policy map called policy1. Class2 specifies policy for traffic with a CoS value of 2.

```
! The following commands create class-maps class1 and class2
! and define their match criteria:

class-map class2
 match cos 2

! The following commands create the policy map, which is defined to contain policy
! specification for class2:
policy-map policy1

Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect
Router(config-pmap-c)#
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class-map	Creates a class map to be used for matching packets to a specified class.
fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
queue-limit	Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.

clear platform ptp stats

To clear the statistics of ptp protocol on the Cisco ASR 901S router, use the **clear platform ptp stats** command.

clear platform ptp stats

Syntax Description

This command has no arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Examples

The following example shows sample output for `clear platform ptp stats` command:

```
Router# clear platform ptp stats

PTP counters cleared
```

Related Commands

Command	Description
show platform ptp stats	Displays statistics about the ptp protocol on the Cisco ASR 901S router.

clock-port

Specifies the mode of a PTP clock port.

clock-port *port-name port-role*

no clock-port *port-name port-role*

Syntax Description

name	Specifies a name for the clock port.
port-role	Specifies the role of the clock port, which can be slave or master. • slave—Sets the clock port to PTP slave mode; the port exchanges timing packets with a PTP master device. • master—Sets the clock port to PTP master mode; the port exchanges timing packets with PTP slave devices.

Defaults

This command is disabled by default.

Command Modes

PTP clock configuration mode

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Examples

The following example shows how to configure a PTP clock port.

```
Router# config terminal
Router(config)# ptp clock ordinary domain 0
Router(config-ptp-clk)# clock-port SLAVE slave
Router(config-ptp-port)# transport ipv4 unicast interface loopback
Router(config-ptp-clk)# clock-source 8.8.8.1
```

Related Commands

Command	Description
ptp clock	Creates a PTP clock instance.

clock-destination

Specifies the IP address of a clock destination. This command applies only when the router is in PTP master unicast mode.

ptp clock-destination *clock-ip-address*

no ptp clock-destination *clock-ip-address*

Syntax Description

clock-ip-address	The IP address of the clock destination.

Defaults

There is no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

If the router is set to ptp master unicast, you can only configure a single destination. If the router is set to ptp master unicast negotiation, you do not need to use this command as the router uses negotiation to determine the IP address of PTP slave devices.

Examples

The following example shows how to configure a PTP announcement:

```
Router(config-ptp-clk)# clock-port MASTER Master
Router(config-ptp-port)# transport ipv4 unicast interface loopback
Router(config-ptp-port)#clock destination 8.8.8.2
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
ptp enable	Enables PTP mode on an interface.
ptp master	Sets an interface in master clock mode for PTP clocking
ptp mode	Specifies the PTP mode.
ptp clock-source	Specifies a PTP clock source.

clock source (interface)

To set the clock source on the interface, use the **clock source** command in interface configuration mode. To restore the default clock source, use the **no** form of this command.

clock source *clock-ip-address*

no clock source *clock-ip-address*

Syntax Description

clock-ip-address	The IP address of the clock source.

Defaults

There is no default setting.

Command Modes

Interface configuration mode.

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

By default, the clock source on the interface is set to internal.

Related Commands

Command	Description
ptp slave	Sets an interface in slave clock mode for PTP clocking
ptp mode	Specifies the PTP mode.
ptp clock-destination	Specifies a PTP clock destination.

debug platform tcam error

To enable Ternary Content Addressable Memory (TCAM) error printing, use the **debug platform tcam error** command in the privileged EXEC mode. To disable TCAM error printing, use the **no debug platform tcam error** command.

debug platform tcam error

no debug platform tcam error

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Examples

The following is sample output from the **debug platform tcam error** command:

```
Router# debug platform tcam error
TCAM Error printing turned ON
```

debug platform tcam info

To enable TCAM info printing, use the **debug platform tcam info** command in the privileged EXEC mode. To disable TCAM info printing, use the **no debug platform tcam info** command.

debug platform tcam info

no debug platform tcam info

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Examples

The following is sample output from the **debug platform tcam info** command:

```
Router# debug platform tcam info
TCAM Info printing turned ON
```

dmm responder hardware timestamp

To configure hardware-based timestamping, use the **dmm responder hardware timestamp** command in Maintenance End Point (MEP) configuration mode. To disable hardware-based time stamping, use the **no** form of this command.

dmm responder hardware timestamp

no dmm responder hardware timestamp

Syntax Description

This command has no arguments or keywords.

Command Default

Hardware-based timestamping is disabled on the receiver MEP.

Command Modes

MEP configuration (config-if-srv-ecfm-mep)

Command History

Release	Modification
15.3(2)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Router.

Examples

The following example shows how to configure hardware-based timestamping on the receiver MEP:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0
Router(config-if)# service instance 1310 ethernet ssvc1310
Router(config-if-srv)# encapsulation dot1q 1310
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 1310
Router(config-if-srv)# cfm mep domain sdmm mpid 1310
Router(config-if-srv-ecfm-mep)# dmm responder hardware timestamp
```

Related Commands

Command	Description
bridge-domain (service instance)	Binds a service instance or a MAC tunnel to a bridge domain instance.
cfm mep domain	Configures MEP for a domain.
encapsulation dot1q (service instance)	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance
rewrite ingress tag	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance.
service instance ethernet	Configures an Ethernet service instance on an interface.

duplex

To configure duplex operation on an interface, use the **duplex** command in interface configuration mode. Use the **no** form of this command to return to the default value.

duplex [**full** | **half**]

no duplex

Syntax Description

full	Specifies full-duplex operation.
half	Specifies half-duplex operation.

Defaults

Full-duplex mode

Command Modes

Interface configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Duplex Options and Interfaces

Table 2-1 lists the supported command options by interface.

Table 2-1 Supported duplex Command Options

Interface Type	Supported Syntax	Default Setting
Gigabit Ethernet Interfaces	**duplex full**	**full**
10 Mbps ports	**duplex** [**half** | **full**]	**half**
100 Mbps ports	**duplex** [**half** | **full**]	**half**

If the transmission speed on a 16-port RJ-45 Gigabit Ethernet port is set to 1000, the duplex mode is set to full. If the transmission speed is changed to 10 or 100, the duplex mode stays at half duplex. You must configure the correct duplex mode when the transmission speed is changed to 10 or 100 from 1000.

Gigabit Ethernet is full duplex only. You cannot change the duplex mode on Gigabit Ethernet ports or on a 10/100/1000-Mbps port that is configured for Gigabit Ethernet.

When manually configuring the interface speed to either 10 or 100 Mbps, you should also configure the duplex mode on the interface.

Caution Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

Table 2-2 describes the interface behavior for different combinations of the **duplex** and **speed** command settings. The specified **duplex** command configured with the specified **speed** command produces the resulting system action.

Note If you need to force an interface port to operate with certain settings and therefore disable autonegotiation, you must be sure that the remote link is configured with compatible link settings for proper transmission. This includes support of flow control on the link.

Table 2-2 Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex half	**speed 10**	Forces 10-Mbps and half-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 10**	Forces 10-Mbps and full-duplex operation, and disables autonegotiation on the interface.
duplex half	**speed 100**	Forces 100-Mbps and half-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 100**	Forces 100-Mbps and full-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 1000**	Forces 1000-Mbps and full-duplex operation, and disables autonegotiation on the interface (Gigabit Ethernet only).

Examples

The following example shows how to configure duplex half operation:

```
Router(config)# interface gigabitethernet0/0
Router(config-if)# duplex half
```

Related Commands

Command	Description
interface	Selects an interface to configure and enters interface configuration mode.
interface gigabitethernet	Selects a particular Gigabit Ethernet interface for configuration.
show interfaces	Displays traffic that is seen by a specific interface.
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.
speed	Sets the port speed for a Fast Ethernet interface.

encapsulation dot1q (service instance)

To define the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance, use the **encapsulation dot1q** command in the service instance mode. To delete the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance, use the **no** form of this command.

encapsulation dot1q *vlan-id*[,*vlan-id*[-*vlain-id*]] [**native**]

no encapsulation dot1q *vlan-id*[,*vlan-id*[-*vlain-id*]] [**native**]

.

Syntax Description

vlan-id	VLAN ID, integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. Optional) Comma must be entered to separate each VLAN ID range from the next range.
native	(Optional) Sets the VLAN ID value of the port to the value specified by the *vlan-id* argument.

Command Default

No matching criteria are defined.

Command Modes

Service instance

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The criteria for this command are: single VLAN, range of VLANs, and lists of the previous two.

A single 802.1Q service instance, allows one VLAN, multiple VLANs, or a range of VLANs. The native keyword can only be set if a single VLAN tag has been specified.

Only a single service instance per port is allowed to have the **native** keyword.

Only one encapsulation command may be configured per service instance.

Examples

The following example shows how to map 802.1Q frames ingress on an interface to the appropriate service instance:

```
Router(config-if-srv)# encapsulation dot1q 10
```

Related Commands

Command	Description
encapsulation dot1q second-dot1q	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation untagged	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

encapsulation dot1ad

To define the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance, use the encapsulation dot1ad command in the service instance mode. To delete the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance, use the no form of this command.

encapsulation dot1ad {*vlan-id[,vlan-id[-vlain-id]]* | **any**}

no encapsulation dot1ad

Syntax Description

vlan-id	VLAN ID, integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. (Optional) Comma must be entered to separate each VLAN ID range from the next range.
any	Matches any packet with one or more VLANs.

Command Default

No matching criteria are defined.

Command Modes

Service instance

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

An interface with encapsulation dot1ad causes the router to categorize the interface as an 802.1ad interface. This causes special processing for certain protocols and other features:

- MSTP uses the IEEE 802.1ad MAC STP address instead of the STP MAC address.
- Certain QoS functions may use the Drop Eligibility (DE) bit of the IEEE 802.1ad tag.

The **encapsulation dot1ad** command requires the interface to be of dot1ad nni (network-network interface) port.

Related Commands

Command	Description
encapsulation dot1q	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.

Command	Description
encapsulation dot1q second dot1q	Double-tagged 802.1Q encapsulation. Matching criteria to be used to map QinQ frames ingress on an interface to the appropriate EFP. The outer tag is unique and the inner tag can be a single VLAN, a range of VLANs or lists of VLANs or VLAN ranges.
encapsulation untagged	Matching criteria to be used to map untagged (native) Ethernet frames entering an interface to the appropriate EFP.

esmc mode

To enable or disable ESMC process on the interface, use the **esmc mode** command in interface configuration mode. Use the **no** form of this command to disable the configuration

esmc mode <*tx* | *rx* >

no esmc mode

SyntaxDescription

tx	Transmission mode
rx	Receiving mode

Command Default

Enabled for synchronous mode and disabled for asynchronous mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

If the interface is configured as line source but does not receive ESMC message from peer node on the interface, then the interface is removed from selectable clock source list. By default this is enabled for synchronous mode and disabled for asynchronous mode.

Note This command is not supported for non-synchronous ethernet interfaces.

Examples

The following example shows how to enable ESMC process:

```
Router(config-if)#esmc mode tx
```

Related Commands

Command	Description
esmc process	Enables the ESMC process in a router.
show esmc	Displays the enabled ESMCs in a router.
show interfaces accounting	Displays the number of packets of each protocol type that have been sent through all configured interfaces.

ethernet loopback

To start or stop an ethernet loopback function on an interface, use the **ethernet loopback** privileged EXEC command.

ethernet loopback start local interface *type number* [**service instance** *instance-number*] {**external** | **internal**} **source mac-address** *source-address* [**destination mac-address** *destination-address*] **timeout** {*time-in-seconds* | **none**}

or

ethernet loopback stop local interface *type number* **id** *session id*

Syntax Description

start	Starts the Ethernet loopback operation configured on the interface.
stop	Stops the Ethernet loopback operation configured on the interface.
local interface *type number*	Specifies the interface on which to start or stop the loopback operation.
service-instance *instance-number*	Specifies the service instance ID. This is an optional field.
external | internal source mac-address *source-address*	Specifies the external or internal source MAC address for the loopback operation.
destination mac-address *destination-address*	Specifies the destination MAC address for the loopback operation. This is an optional field.
timeout {*time-in-seconds* | **none**}	Specifies the timeout interval in seconds. The range is from 0 to 90000 seconds. The default is 300 seconds. Specify **timeout none** to set the loopback to no time out.
id *session id*	Specifies the data plane loopback session ID. The range is from 1 to 3.
all	Stop all Ethernet loopback operations on the switch. This keyword is available only after the **stop** keyword.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
15.2(2)SNG	This command was introduced on the Cisco ASR 901S router.

Usage Guidelines

You cannot start terminal loopback. You can configure ethernet loopback and use the **ethernet loopback start** or **ethernet loopback stop** command only for physical ports and not for VLANs.

Examples

The following example shows how to start a facility port loopback process, verify it, and then to stop it:

```
Router(config)# interface gigabitEthernet0/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop1
Router(config-if-srv)# bridge domain 10
Router(config-if-srv)# end
Router# ethernet loopback start local interface gigabitEthernet 0/1 service instance 10 
internal source mac-address 0123.4567.89ab destination mac-address 255.255.255 timeout 
9000
Router# ethernet loopback stop local interface gigabitEthernet 0/1 id 3
```

Related Commands

Command	Description
show ethernet loopback	Shows information about the per port Ethernet loopbacks configured on a router or an interface.

ethernet oam remote-failure action

To enable Ethernet Operations, Administration, and Maintenance (OAM) remote failure actions, use the **ethernet oam remote-failure action** command in interface configuration mode. To turn off remote failure actions, use the **no** form of this command.

ethernet oam remote-failure {**critical-event** | **dying-gasp** | **link-fault**} **action** {**error-block-interface** | **error-disable-interface**}

no ethernet oam remote-failure {**critical-event** | **dying-gasp** | **link-fault**} **action**

Syntax Description

critical-event	Specifies remote critical event failures.
dying-gasp	Specifies remote dying-gasp failures.
link-fault	Specifies remote link-fault failures.
error-block-interface	Sets the interface to the blocking state when an error occurs.
error-disable-interface	Disables the interface when an error occurs.

Command Default

Actions in response to Ethernet OAM remote failures do not occur.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Use this command to configure an interface to take specific actions when Ethernet OAM remote-failure events occur.

Release 15.1(2)SNG does not support sending critical-event messages but can receive all three message types.

Examples

The following example shows how to configure the action that the Ethernet 1/1 interface takes when a critical event occurs:

```
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet oam remote-failure critical-event action
error-disable-interface
```

hw-module alarm

To enable alarms individually and set a trigger when the alarm pin transitions from high to low or low to high, use the **hw-module alarm** command in global configuration mode. To disable the alarm and trigger, use the **no** form of this command.

hw-module alarm *alarm type* **enable** *trigger type*

no hw-module alarm *alarm type* **enable** *trigger type*

Syntax Description

alarm type	Alarm type. The available options are 1, 2, 3, and 4.
trigger type	Alarm trigger type. The available options are: 0—Triggers when the alarm pin transitions from high to low. 1—Triggers when the alarm pin transitions from low to high.

Command Default

The alarm port functionality is disabled by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.4(1)S	This command was introduced on the Cisco ASR 901SS Series Aggregation Services Routers.

Usage Guidelines

This command is used to poll the alarm status every second to check if there are any changes in the alarm state based on the user configuration. The alarms can be enabled individually and set to trigger when the alarm pin transitions from high to low or vice versa..

Examples

The following example shows how to enable an alarm and set the trigger type on a Cisco ASR 901S router:

```
Router# configure terminal
Router(config)# hw-module alarm 1 enable 1
```

hw-module led disable

To disable the LED on the ASR 901S router, use the **hw-module led disable** command in global configuration mode. To enable the LED, use the **no** form of this command.

hw-module led disable

no hw-module led disable

Syntax Description

This command has no arguments or keywords.

Command Default

The LED is enabled by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.4(1)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Usage Guidelines

This command is used to disable or enable the System, Management, and Network LEDs on the Cisco ASR 901S router.

Examples

The following example shows how to disable the LED on the Cisco ASR 901 router:

```
Router# configure terminal
Router(config)# hw-module led disable
```

interface vlan

To create a dynamic Switch Virtual Interface (SVI), use the **interface vlan** command in global configuration mode.

interface vlan *vlanid*

no interface vlan ***vlanid***

Syntax Description

vlanid	Unique VLAN ID number (1 to 4094) used to create or access a VLAN.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

SVIs are created the first time that you enter the **interface vlan** *vlanid* command for a particular VLAN. The vlanid value corresponds to the VLAN tag that is associated with the data frames on an Inter-Switch Link (ISL), the 802.1Q-encapsulated trunk, or the VLAN ID that is configured for an access port. A message displays whenever you create a new VLAN interface, so that you can check if you entered the correct VLAN number.

If you delete an SVI by entering the **no interface vlan** *vlanid* command, the associated initial domain part (IDP) pair is forced into an administrative down state and is marked as deleted. The deleted interface will not be visible in the show interface command.

You can reinstate a deleted SVI by entering the **interface vlan** *vlanid* command for the deleted interface. The interface comes back up, but much of the previous configuration is gone.

Examples

The following example shows the output when you enter the interface vlan vlanid command for a new VLAN number:

```
Router(config)# interface vlan 23
% Creating new VLAN interface.
```

interface port-channel

To create an EtherChannel interface, use the **interface port-channel** command in global configuration mode. To remove this EtherChannel port from the Cisco CMTS, use the **no** form of this command.

interface port-channel *number*

no interface port-channel *number*

Syntax Description

number	Identifying port channel number for this interface (EtherChannel port). The range is 1 to 8.

Command Default

By default, EtherChannel groups and ports are not defined, and they are disabled (off mode) configured.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The first EtherChannel interface configured becomes the bundle master for all EtherChannel interfaces in the group. That is, the MAC address of the first EtherChannel interface is the MAC address for all EtherChannel interfaces in the group. If the first EtherChannel interface is later removed, the second EtherChannel interface to be configured becomes the bundled master by default.

Repeat this configuration on every EtherChannel port to be bundled into a FastEtherChannel (FEC) or GigabitEtherChannel (GEC) group. This configuration must be present on all EtherChannel interfaces before the EtherChannel group can be configured.

Examples

The following example configures the port to have an EtherChannel port number of 1 within its EtherChannel group. The EtherChannel group is defined with the channel-group command.

```
Router(config)# interface port-channel 1
```

Related Commands

Command	Description
channel-group	Assigns an EtherChannel port to an EtherChannel group.
show interface port-channel	Displays the EtherChannel interfaces and channel identifiers, with their mode and operational status.

interface range

To execute commands on multiple subinterfaces at the same time, use the **interface range** command in global configuration mode.

interface range {*type number* [**-** *interface-number*] [**,**] . . .*type number* | **macro** *word*}

no interface range *type number*

Syntax Description

type number	Interface type and interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function. • You can enter any number of interface type and numbers.
- *interface-number*	(Optional) Ending interface number.
,	Allows you to configure more interface types.
macro	Specifies a macro keyword.
word	Previously defined keyword, up to 32 characters long.

Command Default

No interface range is set.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Configuration Changes

All configuration changes made to a range of subinterfaces are saved to NVRAM, but the range itself does not get saved to NVRAM. Use the **define interface range** command to create and save a range.

You can enter the range in two ways:

- Specifying up to five interface ranges
- Specifying a previously defined macro

You can specify either the interfaces or the name of a range macro. A range must consist of the same interface type, and the interfaces within a range cannot span slots.

You cannot specify both the **interface range** and **macro** keywords in the same command. After creating a macro, the command does not allow you to enter additional ranges. Likewise, if you have already specified an interface range, the command does not allow you to enter a macro.

VLANs

When you define a VLAN, valid values are from 1 to 4094. The last VLAN number cannot exceed 4094.

You cannot use the **interface range** command to create switch virtual interfaces (SVIs) in that particular range. You can use the **interface range** command only to configure existing VLAN SVIs within the range. To display VLAN SVIs, enter the **show running-config** command. VLANs not displayed cannot be used in the **interface range** command.

The commands entered under the **interface range** command are applied to all existing VLAN SVIs within the range.

You can enter the command **interface range create vlan** *x* **-** *y* to create all VLANs in the specified range that do not already exist. If you are using discontiguous VLANs, you can use the **interface range vlan** command to configure multiple SVIs without creating unneeded SVIs and wasting interface descriptor blocks (IDBs).

After specifying a VLAN range, you can continue using the **interface range** command to specify another interface (Fast Ethernet, Gigabit Ethernet, loopback, port-channel, or tunnel).

Note VLANs 4093, 4094, and 4095 are reserved and cannot be configured by the user.

Examples

interface range Gigabit Ethernet Example

The following example shows how to set a Gigabit Ethernet range:

```
Router(config)# interface range gigabitethernet 0/1 - 3
```

Related Commands

Command	Description
define interface range	Defines an interface range macro.
encapsulation dot1q	Applies a unique VLAN ID to each subinterface within the range.

ip tos

To configure the Type of Service (ToS) level for IP traffic, use the ip tos command in pseudowire class configuration mode. To disable a configured ToS value, use the **no** form of this command.

ip tos value *value_number*

no ip tos value *value_number*

.

Syntax Description

value *value_number*	Specifies the type of service (ToS) level for IP traffic in the pseudowire.

Defaults

The default ToS value is 0.

Command Modes

Pseudowire class configuration

Command History

Release	Modification
15.1(2)SNI	Support for this command was introduced on the Cisco ASR 901S router.

Examples

```
Router(config) # pseudowire-class ether-pw
Router(config-pw)# ip tos value 1
```

Related Commands

Command	Description
pseudowire-class	Specifies the name of a Layer 2 pseudowire-class and enters pseudowire-class configuration mode.

l3-over-l2 flush buffers

To enable l3-over-l2 flush buffers for layer 3 over layer 2 deployments, use the **l3-over-l2 flush buffers** command in global configuration mode. To remove this configuration, use the **no** form of this command.

l3-over-l2 flush buffers

no l3-over-l2 flush buffers

Syntax Description

flush	Configures flushing of layer 3 buffers.
buffers	Enables flushing of layer 3 buffers for layer 3 over layer 2 support.

Command Default

This command is enabled by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.2(2)SNG	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Usage Guidelines

This command is required only when layer 3 is deployed over layer 2. When this command is enabled, ARP flushing is done whenever there is a MAC table flush.

You should use the **no** form of this command before configuring Layer 3 FRR features.

Examples

The following example shows how to enable l3-over-l2 flush buffers for layer 3 over layer 2 deployments on a Cisco ASR 901 router:

```
Router# configure terminal
Router(config)# l3-over-l2 flush buffers
```

l2proto-forward

To configure the forwarding of tagged Layer 2 Control Packets and dropping of untagged layer 2 control packets, use the **l2proto-forward** command in interface configuration mode. To delete this configuration, use the **no** form of this command.

l2proto-forward tagged {cdp | dtp | lacp | lldp | stp | udld | vtp}

no l2proto-forward tagged {cdp | dtp | lacp | lldp | stp | udld | vtp}

Syntax Description

cdp	Enables Cisco Discovery Protocol (CDP) tunneling.
dtp	Enables Dynamic Trunking Protocol (DTP) tunneling.
lacp	Enables Link Aggregration Control Protocol (LACP) tunneling.
lldp	Enables Link Layer Discovery Protocol (LLDP) tunneling.
stp	Enables Spanning Tree Protocol tunneling (STP).
udld	Enables UniDirectional Link Detection (UDLD) protocol tunneling.
vtp	Enables Vlan Trunking Protocol (VTP) tunneling.

Defaults

The default behavior is to peer the untagged layer 2 control packets and drop tagged layer 2 control packets.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(2)SNG	This command was introduced.

Usage Guidelines

Use this command to forward tagged and drop untagged layer 2 control protocol packets.

Examples

The following example shows how to configure the forwarding of tagged Layer 2 Control Packets and dropping of untagged layer 2 control packets using the **l2proto-forward** command.

```
Router# configure terminal
Router#(config) interface gigabitethernet 0/1
Router(config-if)# l2proto-forward tagged cdp
```

load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interva**l interface configuration command. Use the **no** form of this command to revert to the default setting.

load-interval *seconds*

no load-interval *seconds*

Syntax Description

seconds	Length of time for which data is used to compute load statistics. Specify a value that is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so forth).

Defaults

The default is 300 seconds (5 minutes).

Command Modes

Interface configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

If you want load computations to be more reactive to short bursts of traffic, rather than averaged over 5-minute periods, you can shorten the length of time over which load averages are computed.

If the load interval is set to 30 seconds, new data is used for load calculations over a 30-second period. This data is used to compute load statistics, including input rate in bits and packets per second, output rate in bits and packets per second, load, and reliability.

Load data is gathered every 5 seconds. This data is used for a weighted average calculation in which more-recent load data has more weight in the computation than older load data. If the load interval is set to 30 seconds, the average is computed for the last 30 seconds of load data.

The **load-interval** command allows you to change the default interval of 5 minutes to a shorter or longer period of time. if you change it to a shorter period of time, the input and output statistics that are displayed when you use the **show interface** command will be more current, and based on more instantaneous data, rather than reflecting a more average load over a longer period of time.

This command is often used for dial backup purposes, to increase or decrease the likelihood of a backup interface being implemented, but it can be used on any interface.

Examples

In the following example, the default 5-minute average is set to a 30-second average.

```
Router(config)# interface GigabitEthernet0/5
Router(config-if)# load-interval 30
```

Related Commands

Command	Description
show interfaces	Displays ALC information.

mac-flap-ctrl

To identify MAC flaps occurring in the router and to take preventive action, use the **mac-flap-ctrl on per-mac** command. To remove MAC flap control, use the **no** form of the command.

mac-flap-ctrl on per-mac <*mac-movement*> <*time-interval*>

no mac-flap-ctrl on per-mac <*mac-movement*> <*time-interval*>

Syntax Description

mac-movement	Maximum number of MAC movements that are allowed in the specified time.
time-interval	Time interval that can elapse before the MAC movements are tagged as flapping.

Command Default

The default values for the counters are five and ten; that is five movements in ten seconds.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNI	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Configure the maximum number of MAC movements that are allowed in a specified time interval, beyond which the MAC movement is termed as flapping. As preventive action, err-disabling is done in one of the ports that has MAC flapping.

Once the port is err-disabled, it can be administratively brought up using the **shut** and **no shut** commands.

Examples

The following example sets the maximum number of mac movements to 20 in 10 seconds, before a MAC flap is detected in the router.

```
Router(config)# mac-flap-ctrl on per-mac 20 10
```

Related Commands

Command	Description
None	None

match ip dscp

To identify a specific IP differentiated service code point (DSCP) value as a match criterion, use the **match ip dscp** class-map configuration command. To remove a specific IP DSCP value from a class map, use the **no** form of this command.

match ip dscp *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

no match ip dscp *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

Syntax Description

ip-dscp-value	Specifies the exact value from 0 to 63 used to identify an IP DSCP value.

Command Modes

Class-map configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Up to eight IP DSCP values can be matched in one match statement. For example, if you wanted the IP DSCP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values), enter the **match ip dscp 0 1 2 3 4 5 6 7** command.

This command is used by the class map to identify a specific IP DSCP value marking on a packet. The *ip-dscp-value* arguments are used as markings only. The IP DSCP values have no mathematical significance. For instance, the *ip-dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with an *ip-dscp-value* of 2 is different from a packet marked with an *ip-dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

Examples

The following example shows how to configure the service policy called priority55 and attach service policy priority55 to an interface. In this example, the class map called ipdscp15 evaluates all packets entering interface Fast Ethernet 0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet is treated with a priority level of 55.

```
Router(config)# class-map ip dscp15
Router(config-cmap)# match ip dscp 15
Router(config-cmap)# exit
Router(config)# policy-map priority55
Router(config-pmap)# class ip dscp 15
Router(config-pmap-c)# priority55
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet0/0
Router(config-if)# service-policy input priority55
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set ip dscp	Marks the IP DSCP value for packets within a traffic class.
show class-map	Displays all class maps and their matching criteria.

match vlan

To match and classify traffic on the basis of the virtual local-area network (VLAN) identification number, use the **match vlan** command in class-map configuration mode. To remove a previously specified VLAN identification number as a match criterion, use the **no** form of this command.

match vlan *vlan-id-number*

no match vlan *vlan-id-number*

Syntax Description

vlan-id-number	VLAN identification number, numbers, or range of numbers. Valid VLAN identification numbers must be in the range of 1 to 4095.

Command Default

Traffic is not matched on the basis of the VLAN identification number.

Command Modes

Class-map configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Specifying VLAN Identification Numbers

You can specify a single VLAN identification number, multiple VLAN identification numbers separated by spaces (for example, 2 5 7), or a range of VLAN identification numbers separated by a hyphen (for example, 25-35).

Support Restrictions

The following restrictions apply to the **match vlan** command:

- The **match vlan** command is supported for IEEE 802.1q and Inter-Switch Link (ISL) VLAN encapsulations only.

Examples

In the following sample configuration, the **match vlan** command is enabled to classify and match traffic on the basis of a range of VLAN identification numbers. Packets with VLAN identification numbers in the range of 25 to 50 are placed in the class called class1.

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match vlan 25-50
Router(config-cmap)# end
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specify or modifies the bandwidth allocated for a class belonging to a policy map.
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces.
service-policy	Attached a policy map to an interface.

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode, connect configuration mode, or xconnect subinterface configuration mode. To restore the MTU value to its original default value, use the **no** form of this command.

mtu *bytes*

no mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

Table 2-3 lists default MTU values according to media type.

Table 2-3 Default Media MTU Values

Media Type	Default MTU (Bytes)
Ethernet	9216
Serial	1500

Command Modes

Interface configuration (config-if)
Connect configuration (xconnect-conn-config)
xconnect subinterface configuration (config-if-xconn)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type.

Note The connect configuration mode is used only for Frame Relay Layer 2 interworking.

Changing the MTU Size

Changing the MTU size is not supported on a loopback interface.

Protocol-Specific Versions of the mtu Command

Changing the MTU value with the **mtu** interface configuration command can affect values for the protocol-specific versions of the command (the **ip mtu** command, for example). If the value specified with the **ip mtu** interface configuration command is the same as the value specified with the **mtu** interface configuration command, and you change the value for the **mtu** interface configuration command, the **ip mtu** value automatically matches the new **mtu** interface configuration command value. However, changing the values for the **ip mtu** configuration commands has no effect on the value for the **mtu** interface configuration command.

Examples

The following example shows how to specify an MTU of 1000 bytes:

```
Router# configure terminal
Router(config)# vlan 20
Router(config-vlan)# name test20
Router(config-if)# mtu 1000
```

Related Commands

Command	Description
ip mtu	Sets the MTU size of IP packets sent on an interface.

name

To specify the name of a iSCSI target in the target profile on the GGSN, use the **name** command in iSCSI interface configuration mode. To remove the IP address configuration, use the **no** form of the command.

name *target_name*

no name *target_name*

Syntax Description

target_name	Name of the SCSI target.

Command Default

No default behavior or values.

Command Modes

iSCSI interface configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Use the **name** command to specify the name of the SCSI target in an iSCSI target interface profile on the GGSN.

Examples

This example shows how to create Ethernet VLAN 20, name it test20, and add it to the VLAN database:

```
Router# configure terminal
Router(config)# vlan 20
Router(config-vlan)# name test20
Router(config-vlan)# end
```

Related Commands

Command	Description
gprs iscsi	Configures the GGSN to use the specified iSCSI profile for record storage.
ip	Specifies the IP address of the target on the SAN.
ip iscsi target-profile	Creates an iSCSI interface profile for an SCSI target (or modifies an existing one), and enters iSCSI interface configuration mode.
port	Specifies the number of the TCP port on which to listen for iSCSI traffic.

negotiation

To enable advertisement of speed, duplex mode, and flow control on a Gigabit Ethernet interface, use the **negotiation** command in interface configuration mode. To disable automatic negotiation, use the **no negotiation auto** command.

negotiation {**auto**}

no negotiation auto

Syntax Description

auto	Enables the autonegotiation protocol to configure the speed, duplex, and automatic flow control of the Gigabit Ethernet interface. This is the default.

Command Default

Autonegotiation is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The **negotiation auto** command is used instead of the **duplex** and **speed** commands (which are used on Ethernet to automatically configure the duplex and speed settings of the interfaces.

The **no negotiation auto** command is used to disable the autonegotiation. If the speed is set to 1000 Mbps and full-duplex is set for the Gigabit Ethernet interface in small form-factor pluggable (SFP) mode, then the autonegotiation is disabled (forced mode) using the **no negotiation auto** command.

Related Commands

Command	Description
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

network-clock eec

To configure the clocking system hardware with the desired parameters, use the **network-clock eec** command. Use the **no** form of the command to disable the clocking system hardware.

network-clock eec {*1* | *2*}

no network-clock eec {*1* | *2*}

Syntax Description

1	For option 1, the default value is EEC-Option 1 (2048).
2	For option 2, the default value is EEC-Option 2 (1544).

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **network-clock eec** command configures the clocking system hardware with the desired parameters.

Examples

The following example configures the clocking system hardware with EEC option 1:

```
Router(config)# network-clock eec 1
```

Related Commands

Command	Description
network-clock synchronization ssm option	Configures the router to work in a synchronized network mode as described in G.781

network-clock external hold-off

To override hold-off timer value for external interface, use the **network-clock external hold-off** command. Use the **no** form of the command to disable the configuration.

network-clock external <*slot/card/port*> **hold-off** {*0* | <*50-10000*>}

no network-clock external <*slot/card/port*> **hold-off** {*0* | <*50-10000*>}

Syntax Description

slot/port/card	Specifies the slot, card, or port of the interface used for timing.
hold-off	Specifies the hold-off timer value.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The ASR 901S router displays a warning message for values above 1800 ms, as waiting longer causes the clock to go into the holdover mode.

Examples

This example specifies the hold-off timer value for the external interface.

```
Router(config)#network-clock external 3/1/1 hold-off 300
```

Related Commands

Command	Description
network-clock hold-off	Configures general hold-off timer in milliseconds.

network-clock hold-off global

To configure general hold-off timer in milliseconds, use the **network-clock hold-off** command. Use the **no** form of the command to remove the configuration.

network-clock hold-off {*0* | *<50-10000>*} **global**

no network-clock hold-off {*0* | *<50-10000>*} **global**

SyntaxDescription

global	Configures the hold-off timer globally.

Command Default

The default value is 300 milliseconds.

Command Modes

Interface configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Displays a warning message for values below 300 ms and above 1800 ms.

Examples

This example configures the hold-off timer:

```
Router(config-if)#network-clock hold-off 75 global
```

Related Commands

Command	Description
network-clock synchronization ssm option	Configures the router to work in a synchronized network mode as described in G.781.

network-clock hold-off

To configure general hold-off timer in milliseconds, use the **network-clock hold-off** command in the interface configuration mode. Use the **no** form of the command to remove the configuration.

network-clock hold-off {*0* | *<50-10000>*}

no network-clock hold-off {*0* | *<50-10000>*}

SyntaxDescription

<50-10000>	Sets the hold-off timer. The default value is 300 milliseconds.

Command Default

The default value is 300 milliseconds.

Command Modes

Interface configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Displays a warning message for values below 300 ms and above 1800 ms.

Examples

This example configures the hold-off timer:

```
Router(config-if)#network-clock hold-off 1000
```

Related Commands

Command	Description
network-clock synchronization ssm option	Configures the router to work in a synchronized network mode as described in G.781.

network-clock input-source

To configure a clock source line interface, an external timing input interface, a GPS interface, or a packet-based timing recovered clock as the input clock for the system, use the **network-clock input-source** command. Use the **no** form of the command to disable the configuration.

network-clock input-source <*priority*> {**interface** *interface-name slot/port* | **top** *slot/port*}}

no network-clock input-source

Syntax Description

priority	Selection priority for the clock source (1 is the highest priority). When the higher-priority clock source fails, the next-higher-priority clock source is selected. Priority is a number between 1 and 250.
interface-name	Specifies the interface name.
slot/port	Specifies the slot/port name.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The **no** version of the command reverses the command configuration, implying that the priority has changed to undefined and the state machine is informed.

Note This command is not supported on the Cisco ASR 901S router.

Examples

This example configures the priority of the interface to 23.

```
Router(config)# network-clock input-source 23 interface top 0/12
```

Related Commands

Command	Description
network-clock wait-to-restore	Sets the value for the wait-to-restore timer globally.

network-clock hold-off global

To configure general hold-off timer in milliseconds, use the **network-clock hold-off** command. Use the **no** form of the command to remove the configuration.

network-clock hold-off {*0* | <*50-10000*>} **global**

no network-clock hold-off {*0* | <*50-10000*>} **global**

Syntax Description

global	Configures the hold-off timer globally.

Command Default

The default value is 300 milliseconds.

Command Modes

Interface configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S r

Usage Guidelines

Displays a warning message for values below 300 ms and above 1800 ms.

Examples

This example configures the hold-off timer:

```
Router(config-if)#network-clock hold-off 75 global
```

Related Commands

Command	Description
network-clock synchronization ssm option	Configures the router to work in a synchronized network mode as de in G.781.

network-clock revertive

To configure the clock-source as revertive, use the **network-clock revertive** command. Use the **no** form of the command to remove the configuration.

network-clock revertive

no network-clock revertive

Command Default

The default value is non-revertive.

Command Modes

Global configuration

Command History

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

Usage Guidelines

T he **network-clock revertive** command specifies whether or not the clock source is revertive. Clock sources with the same priority are always non-revertive. The default value is non-revertive.

In non-revertive switching, a switch to an alternate reference is maintained even after the original reference recovers from the failure that caused the switch. In revertive switching, the clock switches back to the original reference after that reference recovers from the failure, independent of the condition of the alternate reference.

Examples

This example shows how to make the clock-source revertive:

```
Router(config)#[no] network-clock revertive
```

Related Commands

Command	Description
network-clock input-source	Configures a clock source line interface, an external timing input interface, GPS interface, or a packet-based timing recovered clock as the input clock for the system.

network-clock wait-to-restore

Specifies the amount of time in seconds that the Cisco ASR 901S waits before considering a new clock source. Specify the **network-clock wait-to-restore-timeout** command in the interface configuration mode.

network-clock wait-to-restore *<0-86400>*

no network-clock wait-to-restore *<0-86400>*

Syntax Description

<0-86400>	The wait to restore time is configurable in the range of 0 to 86400 seconds. The default value is 300 seconds.

Defaults

The default setting is **network-clock-select wait-to-restore 300**.

Command Modes

Global configuration (config),

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The wait to restore time is configurable in the range of 0 to 86400 seconds. The default value is 300 seconds.

⚠ **Caution** Ensure that you set the wait-to-restore values above 50 seconds to avoid a timing flap.

Examples

The following example shows how to use the **network-clock wait-to-restore** command:

```
Router# config t
Router(config-if)# network-clock wait-to-restore 1000 global
Router(config-if)# exit
```

Related Commands

Command	Description
set network-clocks force-reselect	Forces the router to re-select the network clock.

network-clock wait-to-restore global

Specifies the amount of time in seconds that the Cisco ASR 901S waits before considering a new clock source.

network-clock wait-to-restore *<0-86400>* **global**

no network-clock wait-to-restore *<0-86400>* **global**

Syntax Description

<0-86400>	The wait to restore time is configurable in the range of 0 to 86400 seconds. The default value is 300 seconds.
global	Sets the value for the wait-to-restore timer globally.

Defaults

The default setting is **network-clock-select wait-to-restore 300**.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The wait to restore time is configurable in the range of 0 to 86400 seconds. The default value is 300 seconds.

Caution Ensure that you set the wait-to-restore values above 50 seconds to avoid a timing flap.

Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t
Router(config)# network-clock wait-to-restore 360 global
Router(config)# exit
```

Related Commands

Command	Description
set network-clocks force-reselect	Forces the router to re-select the network clock.

network-clock synchronization automatic

To enable G.781 based automatic clock selection process, use the **network-clock synchronization automatic** command. Use the **no** form of the command to disable the G.781 based automatic clock selection process.

network-clock synchronization automatic

no network-clock synchronization automatic

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The **network-clock synchronization automatic** command enables the G.781 based automatic clock selection process. G.781 is the ITU-T Recommendation that specifies the synchronization layer functions.

Examples

The following example shows how to enable the G.781 based automatic clock selection process.

```
Router(config)# network-clock synchronization automatic
```

Related Commands

Command	Description
network-clock eec	Configures the clocking system hardware with the desired parameters
network-clock synchronization ssm option	Configures the router to work in a synchronized network mode as described in G.781

network-clock synchronization ssm option

To configure the router to work in a synchronized network mode as described in G.781, use the **network-clock synchronization ssm option** command. Use the **no** form of the command to remove the configuration.

network-clock synchronization ssm option {*1*| *2* {*GEN1* | *GEN2*}}

no network-clock synchronization ssm option

Syntax Description

1	(Default) Refers to synchronization networks designed for Europe (E1 framings are compatible with this option)
2	Refers to synchronization networks designed for the US (T1 framings are compatible with this option).
GEN1	Specifies the first generation message.
GEN2	Specifies the second generation message.

Command Default

Option 1

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Network-clock configurations that are not common between options need to be configured again.

The default option is 1 and while choosing option 2, you need to specify the second generation message (GEN2) or first generation message (GEN1).

Examples

This example show how to configure the router to work in a synchronized network mode:

```
Router(config)#network-clock synchronization ssm option 2 GEN1
```

Related Commands

Command	Description
network-clock eec	Configures the clocking system hardware with the desired parameters

police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** command in policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

police cir percent *percentage* [*burst-in-msec*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percentage*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

no police cir percent *percentage* [*burst-in-msec*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percentage*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

Syntax Description

cir	Committed information rate. Indicates that the CIR will be used for policing traffic.
percent	Specifies that a percentage of bandwidth will be used for calculating the CIR.
percentage	Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
burst-in-msec	(Optional) Burst in milliseconds. Valid range is a number from 1 to 2000.
bc	(Optional) Conform burst (bc) size used by the first token bucket for policing traffic.
conform-burst-in-msec	(Optional) Specifies the bc value in milliseconds. Valid range is a number from 1 to 2000.
ms	(Optional) Indicates that the burst value is specified in milliseconds.
be	(Optional) Peak burst (be) size used by the second token bucket for policing traffic.
peak-burst-in-msec	(Optional) Specifies the be size in milliseconds. Valid range is a number from 1 to 2000.
pir	(Optional) Peak information rate. Indicates that the PIR will be used for policing traffic.
percent	(Optional) Specifies that a percentage of bandwidth will be used for calculating the PIR.
conform-action	(Optional) Action to take on packets whose rate is less than the conform burst. You must specify a value for peak-burst-in-msec before you specify the **conform-action**.
exceed-action	(Optional) Action to take on packets whose rate is within the conform and conform plus exceed burst.
violate-action	(Optional) Action to take on packets whose rate exceeds the conform plus exceed burst. You must specify the **exceed-action** before you specify the **violate-action**.

action	(Optional) Action to take on packets. Specify one of the following keywords: **All Supported Platforms** • **drop**—Drops the packet. • **set-dscp-transmit** *new-dscp*—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting. • **set-frde-transmit**—Sets the Frame Relay discard eligible (DE) bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1. • **set-prec-transmit** *new-prec*—Sets the IP precedence and sends the packet with the new IP precedence value setting. • **transmit**—Sends the packet with no alteration. • **policed-dscp-transmit**—(Exceed and violate action only). Changes the DSCP value per the policed DSCP map and sends the packet. • **set-cos-inner-transmit** *value*—Sets the inner class of service field as a policing action for a bridged frame on the Enhanced FlexWAN module, and when using bridging features on SPAs. • **set-cos-transmit** value—Sets the packet cost of service (CoS) value and sends the packet. • **set-mpls-exposition-transmit**—Sets the Multiprotocol Label Switching (MPLS) experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting. • **set-mpls-topmost-transmit**—Sets the MPLS experimental bits on the topmost label and sends the packet.

Command Default

All Supported Platforms

The default bc and be values are 4 ms.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

This command calculates the cir and pir on the basis of a percentage of the maximum amount of bandwidth available on the interface. When a policy map is attached to the interface, the equivalent cir and pir values in bits per second (bps) are calculated on the basis of the interface bandwidth and the percent value entered with this command. The **show policy-map interface** command can then be used to verify the bps rate calculated.

The calculated cir and pir bps rates must be in the range of 8000 and 2000000000 bps. If the rates are outside this range, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the bps values of the cir and the pir are recalculated on the basis of the revised amount of bandwidth. If the cir and pir percentages are changed after the policy map is attached to the interface, the bps values of the cir and pir are recalculated.

Conform Burst and Peak Burst Sizes in Milliseconds

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

Hierarchical Policy Maps

Policy maps can be configured in two-level (nested) hierarchies; a top (or “parent”) level and a secondary (or “child”) level. The **police** (percent) command can be configured for use in either a parent or child policy map.

Bandwidth and Hierarchical Policy Maps

The **police** (percent) command uses the maximum rate of bandwidth available as the reference point for calculating the bandwidth percentage. When the **police** (percent) command is configured in a child policy map, the **police** (percent) command uses the bandwidth amount specified in the next higher-level policy (in this case, the parent policy map). If the parent policy map does not specify the maximum bandwidth rate available, the **police** (percent) command uses the maximum bandwidth rate available on the next higher level (in this case, the physical interface, the highest point in the hierarchy) as the reference point. The **police** (percent) command always looks to the next higher level for the bandwidth reference point. The following sample configuration illustrates this point:

```
Policymap parent_policy
 class parent
  shape average 512000
  service-policy child_policy

Policymap child_policy
 class normal_type
  police cir percent 30
```

In this sample configuration, there are two hierarchical policies: one called parent_policy and one called child_policy. In the policy map called child_policy, the police command has been configured in the class called normal_type. In this class, the percentage specified by for the **police** (percent) command is 30 percent. The command will use 512 kbps, the peak rate, as the bandwidth reference point for class parent in the parent_policy. The **police** (percent) command will use 512 kbps as the basis for calculating the cir rate (512 kbps * 30 percent).

```
interface serial 4/0
 service-policy output parent_policy

Policymap parent_policy
 class parent
  bandwidth 512
  service-policy child_policy
```

In the above example, there is one policy map called parent_policy. In this policy map, a peak rate has not been specified. The **bandwidth** command has been used, but this command does not represent the maximum rate of bandwidth available. Therefore, the **police** (percent) command will look to the next higher level (in this case serial interface 4/0) to get the bandwidth reference point. Assuming the bandwidth of serial interface 4/0 is 1.5 Mbps, the **police** (percent) command will use 1.5 Mbps as the basis for calculating the cir rate (1500000 * 30 percent).

How Bandwidth Is Calculated

The **police** (percent) command is often used in conjunction with the **bandwidth** and **priority** commands. The **bandwidth** and **priority** commands can be used to calculate the total amount of bandwidth available on an entity (for example, a physical interface). When the **bandwidth** and **priority** commands calculate the total amount of bandwidth available on an entity, the following guideline is invoked:

- If the entity is a physical interface, the total bandwidth is the bandwidth on the physical interface.

For more information on bandwidth allocation, refer to the “Congestion Management Overview” chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example shows how to configure traffic policing using a CIR and a PIR on the basis of a percentage of bandwidth. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40
Router(config-pmap-c-police)# exit
```

After the policy map and class maps are configured, the policy map is attached to an interface as shown in the following example:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy input policy1
Router(config-if)# exit
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Gives priority to a traffic class in a policy map.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
shape (percent)	Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface.

Command	Description
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

police (two rates)

To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the **police** command in policy-map class configuration mode. To remove two-rate traffic policing from the configuration, use the **no** form of this command.

police cir *cir* [**bc** *conform-burst*] [**pir** *pir*] [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

no police cir

Syntax Description

cir	Committed information rate (CIR) at which the first token bucket is updated.
cir	Specifies the CIR value in bits per second. The value is a number from 8000 to 200000000.
bc	(Optional) Conform burst (bc) size used by the first token bucket for policing.
conform-burst	(Optional) Specifies the bc value in bytes. The value is a number from 1000 to 51200000.
pir	(Optional) Peak information rate (PIR) at which the second token bucket is updated.
pir	(Optional) Specifies the PIR value in bits per second. The value is a number from 8000 to 200000000.
be	(Optional) Peak burst (be) size used by the second token bucket for policing.
peak-burst	(Optional) Specifies the peak burst (be) size in bytes. The size varies according to the interface and platform in use.
conform-action	(Optional) Action to take on packets that conform to the CIR and PIR.
exceed-action	(Optional) Action to take on packets that conform to the PIR but not the CIR.

violate-action	(Optional) Action to take on packets exceed the PIR.
action	(Optional) Action to take on packets. Specify one of the following keywords: • **drop**—Drops the packet. • **set-dscp-transmit** *new-dscp*—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting. • **set-dscp-tunnel-transmit** *value*—Sets the DSCP value (0 to 63) in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking and transmits the packet with the new value. • **set-frde-transmit**—Sets the Frame Relay discard eligible (DE) bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1. • **set-mpls-exp-transmit**—Sets the Multiprotocol Label Switching (MPLS) experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting. • **set-prec-transmit** *new-prec*—Sets the IP precedence and sends the packet with the new IP precedence value setting. • **set-prec-tunnel-transmit** *value*—Sets the precedence value (0 to 7) in the tunnel header of an L2TPv3 or GRE tunneled packet for tunnel marking and transmits the packet with the new value. • **set-qos-transmit** *new-qos*—Sets the quality of service (QoS) group value and sends the packet with the new QoS group value setting. • **transmit**—Sends the packet with no alteration.

Command Default

Traffic policing using two rates is disabled.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Configuring Priority with an Explicit Policing Rate

When you configure a priority class with an explicit policing rate, traffic is limited to the policer rate regardless of congestion conditions. In other words, even if bandwidth is available, the priority traffic cannot exceed the rate specified with the explicit policer.

Token Buckets

Two-rate traffic policing uses two token buckets—Tc and Tp—for policing traffic at two independent rates. Note the following points about the two token buckets:

- The Tc token bucket is updated at the CIR value each time a packet arrives at the two-rate policer. The Tc token bucket can contain up to the confirm burst (Bc) value.
- The Tp token bucket is updated at the PIR value each time a packet arrives at the two-rate policer. The Tp token bucket can contain up to the peak burst (Be) value.

Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

A packet of B bytes arrives at time t. The last packet arrived at time t1. The CIR and the PIR token buckets at time t are represented by Tc(t) and Tp(t), respectively. Using these values and in this scenario, the token buckets are updated as follows:

$$Tc(t) = \min(CIR * (t-t1) + Tc(t1), Bc)$$

$$Tp(t) = \min(PIR * (t-t1) + Tp(t1), Be)$$

Marking Traffic

The two-rate policer marks packets as either conforming, exceeding, or violating a specified rate. The following points (using a packet of B bytes) illustrate how a packet is marked:

- If B > Tp(t), the packet is marked as violating the specified rate.
- If B > Tc(t), the packet is marked as exceeding the specified rate, and the Tp(t) token bucket is updated as Tp(t) = Tp(t) – B.

Otherwise, the packet is marked as conforming to the specified rate, and both token buckets—Tc(t) and Tp(t)—are updated as follows:

$$Tp(t) = Tp(t) - B$$

$$Tc(t) = Tc(t) - B$$

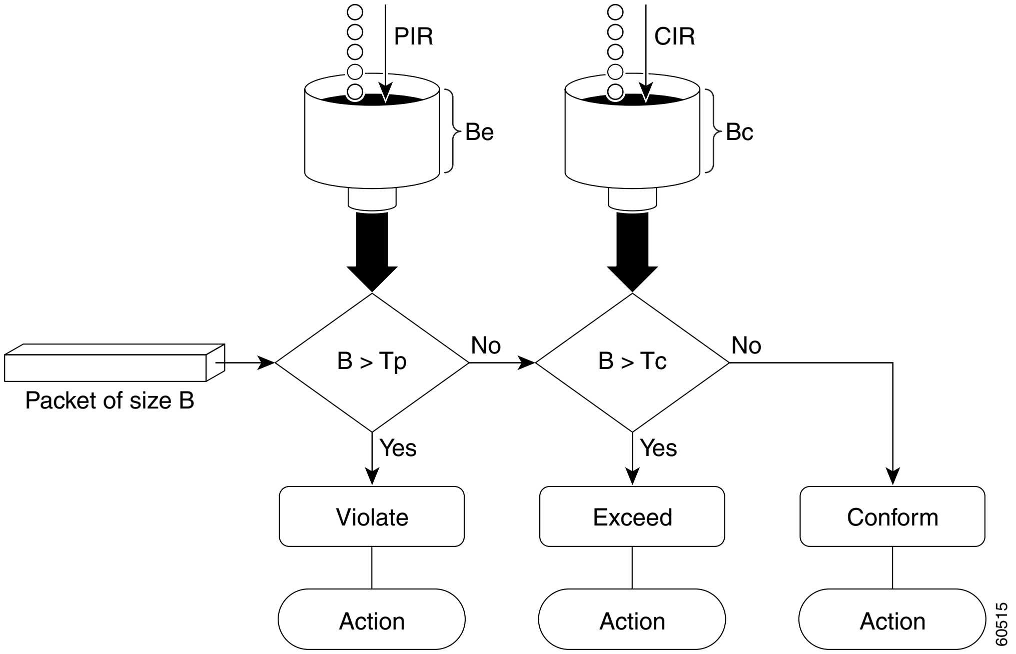
For example, if the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives at the two-rate policer, the packet would be marked as follows:

- 100 kbps would be marked as conforming to the rate.
- 100 kbps would be marked as exceeding the rate.
- 50 kbps would be marked as violating the rate.

Marking Packets and Assigning Actions Flowchart

The flowchart in Figure 2-1 illustrates how the two-rate policer marks packets and assigns a corresponding action (that is, violate, exceed, or conform) to the packet.

Figure 2-1 Marking Packets and Assigning Actions with the Two-Rate Policer



Examples

Setting Priority with an Explicit Policing Rate

In the following example, priority traffic is limited to a committed rate of 1000 kbps regardless of congestion conditions in the network:

```
Router(config)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# police cir 1000000 conform-action transmit exceed-action drop
```

Two-Rate Policing

In the following example, two-rate traffic policing is configured on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps:

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1

  Policy Map policy1
   Class police
    police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
```

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic marked as exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

Related Commands

Command	Description
police	Configures traffic policing.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or an output interface to be used as the service policy for that interface.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map** command in global configuration mode. To delete a policy map, use the **no** form of this command.

policy-map [**type** {**control** | **service**}] *policy-map-name*

no policy-map [**type** {**control** | **traffic**}] *policy-map-name*

Syntax Description

type	Specifies the policy-map type.
control	(Optional) Creates a control policy map.
service	(Optional) Creates a service policy map.
policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.

Command Default

The policy map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added to, or modified before you configure policies for classes whose match criteria are defined in a class map. The **policy-map** command enters policy-map configuration mode, in which you can configure or modify the class policies for a policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. Use the **class-map** and **match** commands to configure the match criteria for a class. Because you can configure a maximum of 64 class maps, a policy map cannot contain more than 64 class policies.

A single policy map can be attached to more than one interface concurrently. Except as noted, when you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by class policies that make up the policy map. In this case, if the policy map is already attached to other interfaces, it is removed from them.

Whenever you modify class policy in an attached policy map, class-based weighted fair queueing (CBWFQ) is notified and the new classes are installed as part of the policy map in the CBWFQ system.

Note Policy-map installation via subscriber-profile is not supported. If you configure an unsupported policy map and there are a large number of sessions, then an equally large number of messages print on the console. For example, if there are 32,000 sessions, then 32,000 messages print on the console at 9,600 baud.

Examples

The following example creates a policy map called “in-gold-policy”:

```
Router(config)# policy-map in-gold-policy
Router(config-pmap)# class in-class1
```

pseudowire-class

To specify the name of a Layer 2 pseudowire-class and enter pseudowire-class configuration mode, use the **pseudowire-class** command in global configuration mode. To remove a pseudowire class configuration, use the **no** form of this command.

pseudowire-class *pw-class-name*

no pseudowire-class *pw-class-name*

Syntax Description

pw-class-name	The name of a Layer 2 pseudowire-class.If you want to configure more than one pseudowire class, define a class name using the *pw-class-name* parameter.

Defaults

No pseudowire-class is defined.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The **pseudowire-class** command configures 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
- 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 entering the **pseudowire-class** command, the router switches to pseudowire-class configuration mode where PW settings can be configured.

Examples

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

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# exit
```

Related Commands

Command	Description
pseudowire	Binds an attachment circuit to a Layer 2 PW for an xconnect service.
xconnect	Binds an attachment circuit to an Layer 2 PW for an xconnect service and then enters xconnect configuration mode.

ql-enabled rep segment

Specifies the REP segment used for synchronous Ethernet clock selection.

ql-enabled rep segment *segment-id*

no ql-enabled rep segment *segment-id*

Syntax Description

segment	Specifies a REP segment.
segment-id	The REP segment ID of the REP segment

Defaults

There is no default setting.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

This command requires that you specify a synchronous Ethernet clock source.

Examples

The following example shows how to use the `ql-enabled` command:

```
Router# config t
Router(config)# ql-enabled rep segment 5
Router(config)# exit
```

Related Commands

Command	Description
rep segment	Enables Resilient Ethernet Protocol (REP) on an interface assigns a segment ID.

rep block port

Use the **rep block port** interface configuration command on the REP primary edge port to configure Resilient Ethernet Protocol (REP) VLAN load balancing. Use the **no** form of this command to return to the default configuration.

rep block port {id *port-id* | *neighbor_offset* | **preferred**} **vlan** {***vlan-list*** | **all**}

no rep block port {**id** *port-id* | *neighbor_offset* | **preferred**}

Syntax Description

id *port-id*	Identify the VLAN blocking alternate port by entering the unique port ID that is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can view the port ID for an interface by entering the **show interface** *interface-id* **rep detail** command.
neighbor_offset	Identify the VLAN blocking alternate port by entering the offset number of a neighbor. The range is –256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. **Note** Because you enter this command at the primary edge port (offset number 1), you would never enter an offset value of 1 to identify an alternate port.
preferred	Identify the VLAN blocking alternate port as the segment port on which you entered the **rep segment** *segment-id* **preferred** interface configuration command. **Note** Entering the **preferred** keyword does not ensure that the preferred port is the alternate port; it gives it preference over other similar ports.
vlan	Identify the VLANs to be blocked.
vlan-list	Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) of VLANs to be blocked.
all	Enter to block all VLANs.

Defaults

The default behavior after you enter the **rep preempt segment** privileged EXEC command (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the **rep block port** command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

Command Modes

Interface configuration

Command History

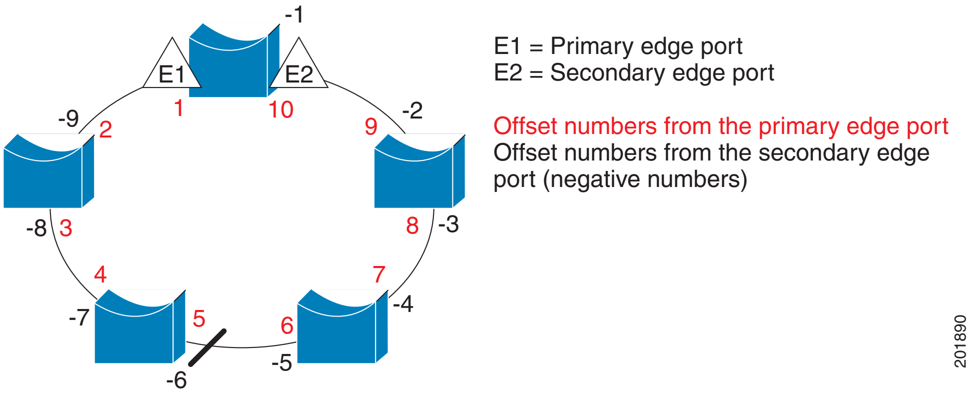
Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. See Neighbor Offset Numbers in a REP SegmentFigure 2-2.

Figure 2-2 Neighbor Offset Numbers in a REP Segment


-1
E1
E2
1
10
-9
2
9
-2
-8
3
8
-3
4
7
-7
5
6
-4
-5
-6
E1 = Primary edge port
E2 = Secondary edge port
Offset numbers from the primary edge port
Offset numbers from the secondary edge port (negative numbers)
201890

Note You would never enter an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **rep preempt delay** *seconds* interface configuration command and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing configuration blocks the configured VLANs and unblocks all other segment ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port in a segment has a unique port ID. The port ID format is similar to the one used by the spanning tree algorithm: a port number (unique on the bridge) associated to a MAC address (unique in the network). To determine the port ID of a port, enter the **show interface** *interface-id* **rep detail** privileged EXEC command.

Examples

This example shows how to configure REP VLAN load balancing on the Switch B primary edge port (Gigabit Ethernet port 0/1) and to configure Gigabit Ethernet port 0/2 of Switch A as the alternate port to block VLANs 1 to 100. The alternate port is identified by its port ID, shown in bold in the output of the **show interface rep detail** command for the Switch A port.

```
Switch A# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB17800EEE
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 1
```

```
Preempt Delay Timer: 35 sec
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to:
PDU/TLV statistics:
LSL PDU rx: 107122, tx: 192493

Router# config t
Router (config)# interface gigabitethernet0/1
Router (config-if)# rep block port id 0080001647FB1780 vlan 1-100
Router (config-if)# exit
```

This example shows how to configure VLAN load balancing by using a neighbor offset number and how to verify the configuration by entering the **show interfaces rep detail** privileged EXEC command:

```
Router# config t
Router (config)# interface gigabitethernet0/2
Router (config-if)# rep block port 6 vlan 1-110
Router (config-if)# end

Router# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB178009C3
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 3
Preempt Delay Timer: 35 sec
Load-balancing block port: 6
Load-balancing block vlan: 1-110
STCN Propagate to: none
LSL PDU rx: 1466780, tx: 3056637
HFL PDU rx: 2, tx: 0
BPA TLV rx: 1, tx: 2119695
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 757406, tx: 757400
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 178326, tx: 178323
```

Related Commands

Command	Description
rep preemt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
rep preempt segment	Manually starts REP VLAN load balancing on a segment.
show interface rep detail	Displays REP detailed configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep platform vlb segment

To configure the VLAN list which forms VLAN load balancing group use the **rep platform vlb segment** command. For more information on VLAN Load Balancing, see the Cisco ASR 901S Configuration Guide.

rep platform vlb segment *segment-id* **vlan** {*vlan-list* | **all**}

no rep platform vlb

Syntax Description

segment-id	ID of the REP segment. The range is from 1 to 1024.
vlan *vlan-list*	Enter vlan vlan-list to block a single VLAN or a range of VLANs,
all	Enter vlan all to block all VLANs. This is the default configuration.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

The **rep platform vlb segment** command should be issued on all Cisco ASR 901S routers participating in VLB for a particular segment and should have a matching VLAN list. This vlan list should also match with the **rep block** command issued on primary edge port.

Examples

The example shows how to configure the VLAN Load Balancing group:

```
Router(config)# rep platform vlb segment 1 vlan 100-200
```

Related Commands

Command	Description
rep block	Configures VLAN load balancing on the primary edge port, identifies the REP alternate port in one of three ways, and configures the VLANs to be blocked on the alternate port.

rep segment

Use the **rep segment** interface configuration command to enable Resilient Ethernet Protocol (REP) on the interface and to assign a segment ID to it. Use the **no** form of this command to disable REP on the interface.

rep segment *segment-id* [**edge [no-neighbor]** [**primary**]] [**preferred**]

no rep segment

Syntax Description

segment-id	Assign a segment ID to the interface. The range is from 1 to 1024.
edge	(Optional) Identify the interface as one of the two REP edge ports. Entering the **edge** keyword without the **primary** keyword configures the port as the secondary edge port. Each segment has only two edge ports. **Note** You must configure two edge ports, including one primary edge port for each segment.
no-neighbor	(Optional) Enter no-neighbor to configure a port with no external REP neighbors as an edge port. The port inherits all properties of edge ports, and you can configure them the same as any edge port.
primary	(Optional) On an edge port, specify that the port is the primary edge port. A segment has only one primary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port. You can identify the primary edge port for a segment by entering the **show rep topology** privileged EXEC command.
preferred	(Optional) Specify that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

Defaults

REP is disabled on the interface.

When REP is enabled on an interface, the default is for the port to be a regular segment port.

Command Modes

Interface configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

REP ports must be Layer 2 trunk ports.

A non-ES REP port can be either an IEEE 802.1Q trunk port or an ISL trunk port.

REP ports should not be configured as one of these port types:

- SPAN destination port
- Private VLAN port
- Tunnel port
- Access port
- REP ports must be network node interfaces (NNIs). REP ports cannot be user-network interfaces (UNIs) or enhanced network interfaces (ENIs).

You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the configuration is allowed, but the REP selects one of them to serve as the segment primary edge port.

- REP ports follow these rules:
  - There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
  - If only one port on a switch is configured in a segment, the port should be an edge port.
  - If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.

Note Release 12.2(33)MRA does not support the **no-neighbor** keyword.

  - If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port. Enter the **show rep topology** privileged EXEC command on a port in the segment to verify which port is the segment primary edge port.

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.

You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

Examples

This example shows how to enable REP on a regular (nonedge) segment port:

```
Router (config)# interface gigabitethernet 0/1
Router (config-if)# rep segment 100
```

This example shows how to enable REP on a port and to identify the port as the REP primary edge port:

```
Router (config)# interface gigabitethernet 0/2
Router (config-if)# rep segment 100 edge primary
```

This example shows how to enable REP on a port and to identify the port as the REP secondary edge port:

```
Router (config)# interface gigabitethernet 0/2
Router (config-if)# rep segment 100 edge
```

You can verify your settings by entering the **show interfaces rep** privileged EXEC command. To verify which port in the segment is the primary edge port, enter the **show rep topology** privileged EXEC command.

Related Commands

Command	Description
show interfaces rep [**detail**]	Displays REP configuration and status for all interfaces or the specified interface.
show rep topology [**detail**]	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

router isis

To enable the Intermediate System-to-Intermediate System (IS-IS) routing protocol and to specify an IS-IS process, use the **router isis** command in global configuration mode. To disable IS-IS routing, use the **no** form of this command.

router isis *area-tag*

no router isis *area-tag*

Syntax Description

area-tag	Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

This command is used to enable routing for an area. An appropriate network entity title (NET) must be configured to specify the area address of the area and system ID of the router. Routing must be enabled on one or more interfaces before adjacencies may be established and dynamic routing is possible.

If you have IS-IS running and at least one International Standards Organization Interior Gateway Routing Protocol (ISO-IGRP) process, the IS-IS process and the ISO-IGRP process cannot both be configured without an area tag. The null tag can be used by only one process. If you run ISO-IGRP and IS-IS, a null tag can be used for IS-IS, but not for ISO-IGRP at the same time. However, each area in an IS-IS multiarea configuration should have a nonnull area tag to facilitate identification of the area.

You can configure only one IS-IS routing process to perform Level 2 (interarea) routing. You can configure this process to perform Level 1 (intra-area) routing at the same time. You can configure up to 29 additional processes as Level 1-only processes. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1.

An interface cannot be part of more than one area, except in the case where the associated routing process is performing both Level 1 and Level 2 routing. On media such as WAN media where subinterfaces are supported, different subinterfaces could be configured for different areas.

If Level 2 routing is not desired for a given area, use the **is-type** command to remove Level 2. Level 2 routing can then be enabled on some other router instance.

Explicit redistribution between IS-IS instances is prohibited (prevented by the parser). In other words, you cannot issue a **redistribute isis** *area-tag* command in the context of another IS-IS router instance (**router isis** *area-tag*). Redistribution from any other routing protocol into a particular area is possible, and is configured per router instance, as in Cisco IOS software Release 12.0, using the **redistribute** and **route map** commands. By default, redistribution is into Level 2.

If multiple Level 1 areas are defined, the Target Address Resolution Protocol (TARP) behaves in the following way:

- The locally assigned target identifier gets the network service access point (NSAP) of the Level 2 area, if present.
- If only Level 1 areas are configured, the router uses the NSAP of the first active Level 1 area as shown in the configuration at the time of TARP configuration ("tarp run"). (Level 1 areas are sorted alphanumerically by tag name, with capital letters coming before lowercase letters. For example, AREA-1 precedes AREA-2, which precedes area-1.) Note that the target identifier NSAP could change following a reload if a new Level 1 area is added to the configuration after TARP is running.
- The router continues to process all Type 1 and 2 protocol data units (PDUs) that are for this router. Type 1 PDUs are processed locally if the specified target identifier is in the local target identifier cache. If not, they are "propagated" (routed) to all interfaces in the *same* Level 1 area. (The same area is defined as the area configured on the input interface.)
- Type 2 PDUs are processed locally if the specified target identifier is in the local target identifier cache. If not, they are propagated via all interfaces (all Level 1 or Level 2 areas) with TARP enabled. If the source of the PDU is from a different area, the information is also added to the local target identifier cache. Type 2 PDUs are propagated via all static adjacencies.
- Type 4 PDUs (for changes originated locally) are propagated to all Level 1 and Level 2 areas (because internally they are treated as "Level 1-2").
- Type 3 and 5 PDUs continue to be routed.
- Type 1 PDUs are propagated only via Level 1 static adjacencies if the static NSAP is in one of the Level 1 areas in this router.

After you enter the **router isis** command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

Examples

The following example starts IS-IS routing with the optional *area-tag* argument, where CISCO is the value for the *area-tag* argument:

```
router isis CISCO
```

The following example specifies IS-IS as an IP routing protocol for a process named Finance, and specifies that the Finance process will be routed on Ethernet interface 0 and serial interface 0:

```
router isis Finance
 net 49.0001.aaaa.aaaa.aaaa.00
interface Ethernet 0
 ip router isis Finance
interface serial 0
 ip router isis Finance
```

The following example shows usage of the **maximum-paths** option:

```
router isis
maximum-paths?
20
```

Related Commands

Command	Description
clns router isis	Enables IS-IS routing for ISO CLNS on an interface and attaches an area designator to the routing process.
ip router isis	Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.
net	Configures an IS-IS NET for the routing process.
redistribute (IP)	Redistribute routes from one routing domain into another routing domain.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.

service instance

To configure an Ethernet service instance, use the service instance command in Layer 2 VPN configuration mode. To disable this configuration, use the no form of this command.

service instance *id service-type*

no service instance *id service-type*

Syntax Description

id	Service instance ID. Integer from 1 to 4294967295.
service-type	Service type for the instance.

Command Default

None

Command Modes

Layer 2 VPN configuration (config-l2vpn)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

You must provision a Multiprotocol Label Switching (MPLS) pseudowire before configuring an Ethernet service instance in Layer 2 VPN configuration mode.

Examples

The following example shows how to configure an Ethernet service instance on a Cisco uBR10012 router:

```
Router(config-l2vpn) # service instance 4095 ethernet
```

service-policy (policy-map class)

To use a service policy as a QoS policy within a policy map (called a hierarchical service policy), use the **service-policy** command in policy-map class configuration mode. To disable a particular service policy as a QoS policy within a policy map, use the **no** form of this command.

service-policy *policy-map-name*

no service-policy *policy-map-name*

Syntax Description

policy-map-name	Specifies the name of the predefined policy map to be used as a QoS policy. The name can be a maximum of 40 alphanumeric characters.

Command Default

No service policies are used.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

This command is used to create hierarchical service policies in policy-map class configuration mode.

This command is different from the **service-policy** [**input** | **output**] *policy-map-name* command used in interface configuration mode. The purpose of the **service-policy** [**input** | **output**] *policy-map-name* is to attach service policies to interfaces.

The child policy is the previously defined service policy that is being associated with the new service policy through the use of the **service-policy** command. The new service policy using the preexisting service policy is the parent policy.

This command has the following restrictions:

- The **set** command is not supported on the child policy.
- The **priority** command can be used in either the parent or the child policy, but not *both* policies simultaneously.
- The **shape** command can be used in either the parent or the child policy, but not *both* polices simultaneously on a subinterface.
- The **fair-queue** command cannot be defined in the parent policy.
- If the **bandwidth** command is used in the child policy, the **bandwidth** command must also be used in the parent policy. The one exception is for policies using the default class.

Examples

The following example creates a hierarchical service policy in the service policy called parent:

```
Router(config)# policy-map child
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 500
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# service-policy child
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
fair-queue	Specifies the number of queues to be reserved for use by a traffic class.
policy-map	Specifies the name of the service policy to configure.
priority	Gives priority to a class of traffic belonging to a policy map.
service-policy	Specifies the name of the service policy to be attached to the interface.
shape	Specifies average or peak rate traffic shaping.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

set cos

To set the Layer 2 class of service (CoS) value of an outgoing packet, use the **set cos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

set cos {*cos-value*}

no set cos {*cos-value*}

Syntax Description

cos-value	Specific IEEE 802.1Q CoS value from 0 to 7.

Command Default

No CoS value is set for the outgoing packet.

Command Modes

Policy-map class configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

CoS packet marking is supported only in the Cisco Express Forwarding switching path.

The **set cos** command should be used by a router if a user wants to mark a packet that is being sent to a switch. Switches can leverage Layer 2 header information, including a CoS value marking.

The **set cos** command can be used only in service policies that are attached in the output direction of an interface. Packets entering an interface cannot be set with a CoS value.

The **match cos** and **set cos** commands can be used together to allow routers and switches to interoperate and provide quality of service (QoS) based on the CoS markings.

Layer 2 to Layer 3 mapping can be configured by matching on the CoS value because switches already can match and set CoS values. If a packet that needs to be marked to differentiate user-defined QoS services is leaving a router and entering a switch, the router should set the CoS value of the packet because the switch can process the Layer 2 header.

Using This Command with the Enhanced Packet Marking Feature

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

- Precedence
- Differentiated services code point (DSCP)

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

You can do the same for the DSCP marking category. That is, you can configure the **set cos dscp** command, and the DSCP value will be copied and used as the CoS value.

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

Examples

In the following example, the policy map called "cos-set" is created to assign different CoS values for different types of traffic. This example assumes that the class maps called "voice" and "video-data" have already been created.

```
Router(config)# policy-map cos-set
Router(config-pmap)# class voice
Router(config-pmap-c)# set cos 1
Router(config-pmap-c)# exit
Router(config-pmap)# class video-data
Router(config-pmap-c)# set cos 2
Router(config-pmap-c)# end
```

Enhanced Packet Marking Example

In the following example, the policy map called "policy-cos" is created to use the values defined in a table map called "table-map1". The table map called "table-map1" was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

In this example, the setting of the CoS value is based on the precedence value defined in "table-map1":

```
Router(config)# policy-map policy-cos
Router(config-pmap)# class class-default
Router(config-pmap-c)# set cos precedence table table-map1
Router(config-pmap-c)# end
```

Related Commands

Command	Description
match cos	Matches a packet on the basis of Layer 2 CoS marking.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
set precedence	Sets the precedence value in the packet header.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

set dscp

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set dscp** command in policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

set [**ip**] **dscp** {*dscp-value*}

no set [**ip**] **dscp** {*dscp-value*}

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets.
dscp-value	A number from 0 to 63 that sets the DSCP value. The following reserved keywords can be specified instead of numeric values: • **EF** (expedited forwarding) • **AF11** (assured forwarding class AF11) • **AF12** (assured forwarding class AF12)

Command Default

Disabled

Command Modes

Policy-map class configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

DSCP and Precedence Values Are Mutually Exclusive

The **set dscp** command cannot be used with the **set precedence** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Precedence Value and Queueing

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Use of the "from-field" Packet-marking Category

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 DSCP value. The "from-field" packet-marking categories are as follows:

- Class of service (CoS)
- QoS group

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-nam*e argument, the default action will be to copy the value associated with the "from-field" category as the DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value will be copied and used as the DSCP value.

Note The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the **set dscp cos** command, only the three bits of the CoS field will be used.

If you configure the **set dscp qos-group** command, the QoS group value will be copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set dscp qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value will not be copied and the packet will not be marked. No action is taken.

Set DSCP Values in IPv6 Environments

When this command is used in IPv6 environments, the default match occurs on both IP and IPv6 packets. However, the actual packets set by this function are only those which meet the match criteria of the class-map containing this function.

Set DSCP Values for IPv6 Packets Only

To set DSCP values for IPv6 values only, the **match protocol ipv6** command must also be used. Without that command, the precedence match defaults to match both IPv4 and IPv6 packets.

Set DSCP Values for IPv4 Packets Only

To set DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword, the match occurs on both IPv4 and IPv6 packets.

Examples

Packet-marking Values and Table Map

In the following example, the policy map called "policy1" is created to use the packet-marking values defined in a table map called "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.

In this example, the DSCP value will be set according to the CoS value defined in the table map called "table-map1".

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set dscp cos table table-map1
Router(config-pmap-c)# end
```

The **set dscp** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface. For information on attaching a service policy to an interface, refer to the "Modular Quality of Service Command-Line Interface" section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Related Commands

Command	Description
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
set precedence	Sets the precedence value in the packet header.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
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 ip dscp

The **set ip dscp** command is replaced by the set dscp command. See the set dscp command for more information.

set ip precedence (policy-map)

The **set ip precedence** (policy-map) command is replaced by the **set precedence** command. See the set precedence command for more information.

set ip precedence (route-map)

To set the precedence value (and an optional IP number or IP name) in the IP header, use the **set ip precedence** command in route-map configuration mode. To leave the precedence value unchanged, use the **no** form of this command.

set ip precedence [*number* | *name*]

no set ip precedence

Syntax Description

number | *name*	(Optional) A number or name that sets the precedence bits in the IP header. The values for the *number* argument and the corresponding *name* argument are listed in Table 2-4 from least to most important.

Command Default

Disabled

Command Modes

Route-map configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Table 2-4 lists the values for the *number* argument and the corresponding *name* argument for precedence values in the IP header. They are listed from least to most important.

Table 2-4 Number and Name Values for IP Precedence

Number	Name
0	**routine**
1	**priority**
2	**immediate**
3	**flash**
4	**flash-override**
5	**critical**
6	**internet**
7	**network**

You can set the precedence using either a number or the corresponding name. Once the IP Precedence bits are set, other QoS services such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set IP Precedence at the edge of the network (or administrative domain); data then is queued based on the precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from arguments such as **routine** and **priority** to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of the high-end Internet QoS available from Cisco, IP Precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network.

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

The **set** route-map configuration commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met.

Examples

The following example sets the IP Precedence to 5 (critical) for packets that pass the route map match:

```
interface gigabitethernet0/1
 ip policy route-map texas

route-map texas
match length 68 128
set ip precedence 5
```

Related Commands

Command	Description
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.

set ip precedence tunnel

To set the precedence value in the header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking, use the **set ip precedence tunnel** command in policy-map class configuration mode. To disable this functionality, use the **no** form of this command.

set ip precedence tunnel *precedence-value*

no set ip precedence tunnel *precedence-value*

Syntax Description

precedence-value	Number from 0 to 7 that identifies the precedence value of the tunnel header.

Command Default

The precedence value is not set.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

It is possible to configure L2TPv3 (or GRE) tunnel marking and the **ip tos** command at the same time. However, Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) (L2TPv3 or GRE) tunnel marking has higher priority over **ip tos** commands, meaning that tunnel marking always rewrites the IP header of the tunnel packet and overwrites the values set by **ip tos** commands. The order of enforcement is as follows when these commands are used simultaneously:

1. **set ip dscp tunnel** or **set ip precedence tunnel** (L2TPv3 or GRE tunnel marking)
2. **ip tos reflect**
3. **ip tos** *tos-value*

This is the designed behavior. We recommend that you configure only L2TPv3 (or GRE) tunnel marking and reconfigure any peers configured with the **ip tos** command to use L2TPv3 (or GRE) tunnel marking.

Note For Cisco IOS Release 12.4(15)T2, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco RPM-XF.

Examples

The following example shows the **set ip precedence tunnel** command used in a tunnel marking configuration. In this example, a class map called "MATCH_FRDE" has been configured to match traffic on the basis of the Frame Relay discard eligible (DE) bit setting. Also, a policy map called "policy1" has been created within which the **set ip precedence tunnel** command has been configured.

```
Router> enable
Router# configure terminal
```

```
Router(config)# class-map MATCH_FRDE
Router(config-cmap)# match fr-de
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class tunnel
Router(config-pmap-c)# set ip precedence tunnel 7
Router(config-pmap-c)# end
```

Related Commands

Command	Description
ip tos	Specifies the ToS level for IP traffic in the TN3270 server.
set ip dscp tunnel	Sets the DSCP value in the header of an L2TPv3 tunneled packet.

set ip tos (route-map)

To set the type of service (ToS) bits in the header of an IP packet, use the **set ip tos** command in route-map configuration mode. To leave the ToS bits unchanged, use the **no** form of this command.

set ip tos [*tos-bit-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**]

no set ip tos

Syntax Description

tos-bit-value	(Optional) A value (number) from 0 to 15 that sets the ToS bits in the IP header. See Table 2-5 for more information.
max-reliability	(Optional) Sets the maximum reliability ToS bits to 2.
max-throughput	(Optional) Sets the maximum throughput ToS bits to 4.
min-delay	(Optional) Sets the minimum delay ToS bits to 8.
min-monetary-cost	(Optional) Sets the minimum monetary cost ToS bits to 1.
normal	(Optional) Sets the normal ToS bits to 0.

Command Default

Disabled

Command Modes

Route-map configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

This command allows you to set four bits in the ToS byte header. Table 2-5 shows the format of the four bits in binary form.

Table 2-5 ToS Bits and Description

T3	T2	T1	T0	Description
0	0	0	0	0 normal forwarding
0	0	0	1	1 minimum monetary cost
0	0	1	0	2 maximum reliability
0	1	0	0	4 maximum throughput
1	0	0	0	8 minimum delay

The T3 bit sets the delay. Setting T3 to 0 equals normal delay, and setting it to 1 equals low delay.

The T2 bit sets the throughput. Setting this bit to 0 equals normal throughput, and setting it to 1 equals maximum throughput. Similarly, the T1 and T0 bits set reliability and cost, respectively. Therefore, as an example, if you want to set a packet with the following requirements:

minimum delay T3 = 1

normal throughput T2 = 0

normal reliability T1 = 0

minimum monetary cost T0 = 1

You would set the ToS to 9, which is 1001 in binary format.

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

The **set** (route-map) commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met.

Examples

The following example sets the IP ToS bits to 8 (minimum delay as shown in Table 2-5) for packets that pass the route-map match:

```
Router(config)# interface gigabitethernet0/1
Router(config-if)# ip policy route-map texas
!
Router(config-if)# route-map texas
Router(config-route-map)# match length 68 128
Router(config-route-map)# set ip tos 8
!
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set network-clocks

This command causes the router to reselect a network clock; the router selects a new clock based on clock priority.

set network-clocks [force-reselect | next-select]

Syntax Description

force-reselect	Forces the router to select a new network clock.
next-select	Forces the router to select the next available network clock.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Examples

The following example shows how to use the set network-clocks force-reselect command:

```
Router# set network-clocks force-reselect
```

Related Commands

Command	Description
show network-clocks	Displays information about all clocks configured on the router.

set precedence

To set the precedence value in the packet header, use the **set precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command.

set precedence {*precedence-value*}

no set precedence {*precedence-value*}

Syntax Description

precedence-value	A number from 0 to 7 that sets the precedence bit in the packet header.

Command Default

Disabled

Command Modes

Policy-map class configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Command Compatibility

If a router is loaded with an image from this version (that is, Cisco IOS Release 12.2(13)T) that contained an old configuration, the **set ip precedence** command is still recognized. However, the **set precedence** command will be used in place of the **set ip precedence** command.

The **set precedence** command cannot be used with the **set dscp** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can be one value or the other, but not both.

Bit Settings

Once the precedence bits are set, other quality of service (QoS) features such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

Precedence Value

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the specified precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

The **set precedence** command cannot be used with the **set dscp** command to mark the *same* packet. The two values, differentiated services code point (DSCP) and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

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 precedence value. The "from-field" packet-marking categories are as follows:

- CoS
- QoS group

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 precedence value. For instance, if you configure the **set precedence cos** command, the CoS value will be copied and used as the precedence value.

You can do the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value will be copied and used as the precedence value.

The valid value range for the precedence 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 precedence 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 QoS group value exceeds the precedence range (for example, 10), the packet-marking value will not be copied, and the packet will not be marked. No action is taken.

Setting Precedence Values for IPv4 Packets Only

To set the precedence values for IPv4 packets only, use a command involving the **ip** keyword like the **match ip precedence** or **match ip dscp** command or include the **match protocol ip** command along with the others in the class map. Without the additional **ip** keyword, the class-map may match both IPv6 and IPv4 packets (depending on the other match criteria) and the **set precedence** or **set dscp** command may act upon both types of packets.

Examples

The following example shows how to use the set precedence command.

```
Router(config)# policy-map policy-cos
Router(config-pmap)# class class-default
Router(config-pmap-c)# set precedence 4
Router(config-pmap-c)# end
```

The **set precedence** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface. For information on attaching a service policy to an interface, refer to the "Modular Quality of Service Command-Line Interface Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide.*

Related Commands

Command	Description
match dscp	Identifies a specific IP DSCP value as a match criterion.
match precedence	Identifies IP precedence values as match criteria.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

Command	Description
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
set dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
set qos-group	Sets a group ID that can be used later to classify packets.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration for all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
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.

shape (percent)

To specify average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface, use the **shape** command in policy-map class configuration mode. To remove traffic shaping, use the **no** form of this command.

shape {**average**} **percent** *percentage* [*sustained-burst-in-msec* **ms**] [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**]

no shape {**average**} **percent** *percentage* [*sustained-burst-in-msec* **ms**] [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**]

Syntax Description

average	Specifies average rate traffic shaping.
percent	Specifies that a percent of bandwidth will be used for either the average rate traffic shaping or peak rate traffic shaping.
percentage	Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
sustained-burst-in-msec	(Optional) Sustained burst size used by the first token bucket for policing traffic. Valid range is a number from 4 to 200.
ms	(Optional) Indicates that the burst value is specified in milliseconds (ms).
be	(Optional) Excess burst (be) size used by the second token bucket for policing traffic.
excess-burst-in-msec	(Optional) Specifies the be size in milliseconds. Valid range is a number from 0 to 200.
bc	(Optional) Committed burst (bc) size used by the first token bucket for policing traffic.
committed-burst-in-msec	(Optional) Specifies the bc value in milliseconds. Valid range is a number from 1 to 2000.

Command Default

The default bc and be is 4 ms.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Committed Information Rate

This command calculates the committed information rate (CIR) on the basis of a percentage of the available bandwidth on the interface. Once a policy map is attached to the interface, the equivalent CIR value in bits per second (bps) is calculated on the basis of the interface bandwidth and the percent value entered with this command. The **show policy-map interface** command can then be used to verify the CIR bps value calculated.

The calculated CIR bps rate must be in the range of 8000 and 154,400,000 bps. If the rate is less than 8000 bps, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the CIR bps values are recalculated on the basis of the revised amount of bandwidth. If the CIR percentage is changed after the policy map is attached to the interface, the bps value of the CIR is recalculated.

Conform Burst and Peak Burst Sizes in Milliseconds

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

The traffic shape converge rate depends on the traffic pattern and the time slice (Tc) parameter, which is directly affected by the bc that you configured. The Tc and the average rate configured are used to calculate bits per interval sustained. Therefore, to ensure that the shape rate is enforced, use a bc that results in a Tc greater than 10 ms.

How Bandwidth Is Calculated

The **shape** (percent) command is often used in conjunction with the **bandwidth** and **priority** commands. The **bandwidth** and **priority** commands can be used to calculate the total amount of bandwidth available on an entity (for example, a physical interface). When the **bandwidth** and **priority** commands calculate the total amount of bandwidth available on an entity, the following guideline is invoked:

- If the entity is a physical interface, the total bandwidth is the bandwidth on the physical interface.

For more information on bandwidth allocation, see the “Congestion Management Overview” chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide.*

Examples

The following example configures traffic shaping using an average shaping rate on the basis of a percentage of bandwidth. In this example, 25 percent of the bandwidth has been specified. Additionally, an optional be value and bc value (100 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# shape average percent 25 20 ms be 100 ms bc 400 ms
Router(config-pmap-c)# end
```

After the policy map and class maps are configured, the policy map is attached to interface as shown in the following example.

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy input policy1
Router(config-if)# end
```

Related Commands

Command	Description
bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class (policy-map)	Specifies the name of the class whose policy you want to create or change and the default class (commonly known as the class-default class) before you configure its policy.

Command	Description
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Gives priority to a class of traffic belonging to a policy map.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
shape max-buffers	Specifies the maximum number of buffers allowed on shaping queues.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

shape (policy-map class)

To shape traffic to the indicated bit rate according to the algorithm specified, use the **shape** command in policy-map class configuration mode. To remove shaping and leave the traffic unshaped, use the **no** form of this command.

shape [**average** | **peak**] *mean-rate* [*burst-size*] [*excess-burst-size*]

no shape [**average** | **peak**]

Syntax Description

average	(Optional) Committed Burst (Bc) is the maximum number of bits sent out in each interval.
peak	(Optional) Bc + Excess Burst (Be) is the maximum number of bits sent out in each interval.
mean-rate	(Optional) Also called committed information rate (CIR). Indicates the bit rate used to shape the traffic, in bits per second. When this command is used with backward explicit congestion notification (BECN) approximation, the bit rate is the upper bound of the range of bit rates that will be permitted. For a committed (average) burst rate, valid values are 30,000–10,000,000,000. For an excess (peak) burst rate, valid values are 8,000-10,000,000,000.
burst-size	(Optional) The number of bits in a measurement interval (Bc).
excess-burst-size	(Optional) The acceptable number of bits permitted to go over the Be.
aal5	Supports connection-oriented variable bit rate (VBR) services.

Command Default

When the excess burst size (Be) is not configured, the default Be value is equal to the committed burst size (Bc). For more information about burst size defaults, see the *Usage Guidelines* section.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The measurement interval is the committed burst size (Bc) divided by committed information rate (CIR). Bc cannot be set to 0. If the measurement interval is too large (greater than 128 milliseconds), the system subdivides it into smaller intervals.

If you do not specify the committed burst size (Bc) and the excess burst size (Be), the algorithm decides the default values for the shape entity. The algorithm uses a 4 milliseconds measurement interval, so Bc is CIR * (4 / 1000).

Burst sizes larger than the default committed burst size (Bc) need to be explicitly specified. The larger the Bc, the longer the measurement interval. A long measurement interval may affect voice traffic latency, if applicable.

When the excess burst size (Be) is not configured, the default value is equal to the committed burst size (Bc).

Examples

The following example configures a shape entity with a CIR of 1 Mbps and attaches the policy map called dts-interface-all-action to interface pos1/0/0:

```
policy-map dts-interface-all-action
 class class-interface-all
  shape average 1000000

interface pos1/0/0
 service-policy output dts-interface-all-action
```

show asr901 multicast-support

To display the platform support for IPv4 or IPv6 multicast, use the **show asr901 multicast-support** command.

show asr901 multicast-support

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.4(1)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Usage Guidelines

This command displays the platform support for IPv4 or IPv6 multicast.

Examples

This example shows the output from **show asr901 multicast-support** command on a Cisco ASR 901 series router:

```
Router# show asr901 multicast-support

 Platform support for IPv4(v6) Multicast: ENABLED
```

Related Commands

Command	Description
asr901-platf-multicast enable	Enables platform multicast.

show etherchannel

To display EtherChannel information for a channel, use the **show etherchannel** command in privileged EXEC mode.

show etherchannel [*channel-group*] **{port-channel | detail | summary | port | load-balance}**

Syntax Description

channel-group	(Optional) Number of the channel group. If you do not specify a value for the channel-group argument, all channel groups are displayed.
port-channel	Displays port channel information
detail	Displays detailed EtherChannel information.
summary	Displays a one-line summary per channel group.
port	Displays EtherChannel port information.
load-balance	Displays load-balance information.
protocol	Displays the enabled protocol.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

If you do not specify a value for the **channel-group** argument, all channel groups are displayed.

If the interface is configured as part of the channel in ON mode, the show etherchannel protocol command displays Protocol: - (Mode ON).

- In the output of the **show etherchannel summary** command, the following conventions apply:
- In the column that displays the protocol that is used for the channel, if the channel mode is ON, a hyphen (-) is displayed.

For LACP, multiple aggregators are supported. For example, if two different bundles are created, Po1 indicates the primary aggregator, and Po1A and Po1B indicates the secondary aggregators.

In the output of the **show etherchannel load-balance** command, the following conventions apply:

- For EtherChannel load balancing of IPv6 traffic, if the traffic is bridged onto an EtherChannel (for example, it is a Layer 2 channel and traffic in the same VLAN is bridged across it), the traffic is always load balanced by the IPv6 addresses or src, dest, or src-dest, depending on the configuration. For this reason, the switch ignores the MAC/IP/ports for bridged IPv6 traffic. If you configure src-dst-mac, the src-dst-ip(v6) address is displayed. If you configure src-mac, the src-ip(v6) address is displayed.
- IPv6 traffic that is routed over a Layer 2 or a Layer 3 channel is load balanced based on MAC addresses or IPv6 addresses, depending on the configuration. The MAC/IP and the src/dst/src-dst are supported, but load balancing that is based on Layer 4 ports is not supported. If you use the port keyword, the IPv6 addresses or either src, dst, or src-dst, is displayed.

Examples

The following example shows how to verify the configuration:

```
Router# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-mac

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination MAC address
  IPv6: Source XOR Destination MAC address (routed packets)
        Source XOR Destination IP address (bridged packets)
```

Related Commands

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
channel-protocol	Sets the protocol that is used on an interface to manage channeling.

show ethernet loopback

To display information about the per port Ethernet loopbacks configured on a router or an interface, use the **show ethernet loopback** command in privileged EXEC mode.

show ethernet loopback active [brief | [*interface-id***] [service-instance** *id***]]**

Syntax Description

active	Displays active ethernet loopback sessions.
brief	Displays brief description of the current loopback sessions
interface-id	(Optional) Displays loopback information for the specified interface. Only physical interfaces support ethernet loopback.
service-instance *id*	Specifies the service instance ID.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.2(2)SNG	This command was introduced on the Cisco ASR 901S router.

Usage Guidelines

If you do not specify an *interface-id,* all configured loopbacks appear. The router supports a maximum of two Ethernet loopback configurations.

Examples

The following example shows how to verify the configuration:

```
Router# show ethernet loopback active
============================================================
Interface               : GigabitEthernet0/3
Service Instance        : 32
Direction               : Terminal
Time out(sec)           : 300
Status                  : on
Start time              : 14:15:01.742 IST Tue Jun 18 2013
Time left               : 00:04:48
Source Mac Address      : 0000.0002.0002
Destination Mac Address : 4055.3989.751c
```

Related Commands

Command	Description
start ethernet loopback or **stop ethernet loopback**	Starts or stops the loopback operation.

show interface port-channel

To display the EtherChannel interfaces and channel identifiers, with their mode and operational status, use the **show interface port-channel** command in privileged EXEC mode.

show interface port-channel {*number*}

Syntax Description

number	Optional value enables the display of information for one port channel interface number. The range is from 1 to 8.

Command Default

No default behaviors or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

show interfaces rep

Use the **show interfaces rep** User EXEC command to display Resilient Ethernet Protocol (REP) configuration and status for a specified interface or for all interfaces.

show interfaces [*interface-id***] rep [detail]** [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Display REP configuration and status for a specified physical interface or port channel ID.
detail	(Optional) Display detailed REP configuration and status information.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

In the output for the **show interface rep** [**detail**] command, in addition to an *Open*, *Fail*, or AP (alternate port) state, the Port Role might show as *Fail Logical Open* (*FailLogOpen*) or *Fail No Ext Neighbor* (*FailNoNbr*). These states indicate that the port is physically up, but REP is not configured on the neighboring port. In this case, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. The Port Role for this port shows as Fail Logical Open; the port forwards all data traffic on all VLANs. The other failed Port Role shows as *Fail No Ext Neighbor;* this port blocks traffic for all VLANs.

When the external neighbors for the failed ports are configured, the failed ports go through the alternate port state transitions and eventually go to an Open state or remain as the alternate port, based on the alternate port election mechanism.

The output of this command is also included in the **show tech-support** privileged EXEC command output.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is sample output from the **show interface rep** command:

```
Switch # show interface rep
Interface                Seg-id   Type        LinkOp     Role
---------------------- ------ ------------ ----------- ----
GigabitEthernet 0/1        1    Primary Edge  TWO_WAY    Open
GigabitEthernet 0/2        1    Edge          TWO_WAY    Open
```

This is sample output from the **show interface rep** command when the edge port is configured to have no REP neighbor. Note the asterisk (*) next to *Primary Edge*.

```
Router# show interface rep
Interface              Seg-id Type            LinkOp      Role
---------------------- ------ --------------  ----------- ----
GigabitEthernet0/1     2                      TWO_WAY     Open
GigabitEthernet0/2     2      Primary Edge*   TWO_WAY     Open
```

This is sample output from the **show interface rep** command when external neighbors are not configured:

```
Switch # show interface rep
Interface                Seg-id   Type        LinkOp     Role
---------------------- ------ ------------ ----------- ----
GigabitEthernet0/1        1                 NO_NEIGHBOR FailNoNbr
GigabitEthernet0/2        2                 NO_NEIGHBOR FailLogOpen
```

This is sample output from the **show interface rep detail** command for a specified interface:

```
Switch # show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2   REP enabled
Segment-id: 1 (Segment)
PortID: 00030019E85BDD00
Preferred flag: No
Operational Link Status: INIT_DOWN
Current Key: 0000000000000000000
Port Role: Fail
Blocked VLAN: 1-4094
Admin-vlan: 1
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: 1234567890123456
Configured Load-balancing Block VLAN: 1-4094
STCN Propagate to: none
LSL PDU rx: 0, tx: 0
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

Related Commands

Command	Description
repsegment	Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port.
show reptopology [**detail**]	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

show ip vrf

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

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

Syntax Description

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

Defaults

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

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

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

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

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

Examples

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

```
Router# show ip vrf

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

```
                      Virtual-Access4 [D]

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

Table 2-6 describes the significant fields shown in the display.

Table 2-6 show ip vrf Field Descriptions

Field	Description
Name	Specifies the VRF name.
Default RD	Specifies the default route distinguisher.
Interface	Specifies the network interface.

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

```
Router# show ip vrf detail

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

Table 2-7 describes the significant fields shown in the display.

Table 2-7 show ip vrf detail Field Descriptions

Field	Description
VPNID	Specifies the VPN ID assigned to the VRF.
Interfaces	Specifies the network interfaces.
Virtual-Access*n* [D]	Specifies the downstream VRF.
Export	Specifies VPN route-target export communities.
Import	Specifies VPN route-target import communities.

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

```
Router# show ip vrf interfaces

InterfaceIP-AddressVRFProtocol
```

```
Ethernet210.22.0.33vrf1up
Ethernet410.77.0.33hubup
Router#
```

Table 2-8 describes the significant fields shown in the display.

Table 2-8 show ip vrf interfaces Field Descriptions

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

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

```
Router# show ip vrf id

VPN Id         Name                           RD
2:3            vpn2                           <not set>
A1:3F6C        vpn1                           100:1
```

Table 2-9 describes the significant fields shown in the display.

Table 2-9 show ip vrf id Field Descriptions

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

show mac-address-table

To display the MAC address table, use the show mac-address-table command in privileged EXEC mode.

show mac-address-table [address *mac-addr*] **[aging-time** *vlan-id*] **[count** *vlan-id*] **[dynamic [address** *mac-address* **| interface** *type slot/port* **| vlan** *vlan-id*]] **[interface** *type/number*] **[multicast [{igmp-snooping | mld-snooping | vlan** ***vlan-id*****}]] [static [[{address** ***mac-addr*****} | {interface** *interface/switch-num//slot/port*} **| vlan** *vlan-id*] **[vlan** *vlan-id*]

Syntax Description

address *mac-addr*	Displays information about the MAC-address table for a specific MAC address; see the "Usage Guidelines" section for format guidelines.
vlan *vlan-id*	(Optional) Displays information for a specific VLAN only. Range: 1 to 4094.
aging-time	Displays information about the MAC-address aging time.
count	Displays the number of entries that are currently in the MAC-address table.
dynamic	Displays information about the dynamic MAC-address table entries only.
interface *interface*	(Optional) Displays information about a specific interface type; possible valid values are gigabitethernet and tengigabitethernet.
multicast	Displays information about the multicast MAC-address table entries only.
igmp-snooping	Displays the addresses learned by Internet Group Management Protocol (IGMP0 snooping.
mld-snooping	Displays the addresses learned by multicast listener discovery version 2 (MLDv2) snooping.
static	Displays information about the static MAC-address table entries only.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The *mac-addr* is a 48-bit MAC address and the valid format is H.H.H.

The **count** keyword displays the number of multicast entries.

The **multicast** keyword displays the multicast MAC addresses (groups) in a VLAN or displays all statically installed or IGMP snooping-learned entries in the Layer 2 table.

The **dynamic** entries that are displayed in the Learn field are always set to Yes.

Examples

The following example shows the output for the **show mac address-table count** command:

```
Router#show mac address-table count
```

```
Mac Entries for Vlan 4094:
---------------------------
Dynamic Address Count  : 1
Static  Address Count  : 0
Total Mac Addresses    : 1

Mac Entries for Vlan 3107:
---------------------------
Dynamic Address Count  : 0
Static  Address Count  : 0
Total Mac Addresses    : 0

Total Mac Address Space Available: 32756
```

show network-clock synchronization

Displays the information about network-clock synchronization.

show network-clock synchronization [detail]

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

This command confirms if the system is in revertive mode or non-revertive mode and verify the non-revertive configurations.

Examples

This command shows the output of the **show network-clock synchronization** command to confirm if the system is in revertive mode:

```
RouterB#show network-clocks synchronization
Symbols:
En - Enable, Dis - Disable, Adis - Admin Disable
            NA - Not Applicable
            *  - Synchronization source selected
            #  - Synchronization source force selected
            &  - Synchronization source manually switched

Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : GigabitEthernet0/4
Hold-off (global) : 300 ms
Wait-to-restore (global) : 300 sec
Tsm Delay : 180 ms
Revertive : No

Nominated Interfaces

Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
Internal             NA          NA/Dis       251   QL-SEC    NA        NA
To0/6                NA          NA/En        1     QL-FAILED NA        NA
Gi0/1                NA          Sync/En      1     QL-DNU    -         -
*Gi0/4             NA          Sync/En      20    QL-SEC    -         -
```

Use the **show network-clock synchronization detail** command to display all details of network-clock synchronization parameters at the global and interface levels.

```
Router# show network-clocks synchronization detail
Symbols:     En - Enable, Dis - Disable, Adis - Admin Disable
            NA - Not Applicable
            *  - Synchronization source selected
            #  - Synchronization source force selected
            &  - Synchronization source manually switched
```

```
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock State : Frequency Locked
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : GigabitEthernet0/4
Hold-off (global) : 300 ms
Wait-to-restore (global) : 300 sec
Tsm Delay : 180 ms
Revertive : No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 3
Squelch Threshold: QL-SEC
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (begin)-> 1A (src_added)-> 1A (ql_change)-> 1A (src_added)-> 1A
(ql_change)-> 1A (sf_change)-> 1A (sf_change)-> 1A (sf_change)-> 1A (sf_change)-> 1A
(ql_change)-> 1A


Nominated Interfaces

Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
Internal             NA          NA/Dis       251   QL-SEC    NA        NA
To0/6                NA          NA/En        1     QL-FAILED NA        NA
Gi0/1                NA          Sync/En      1     QL-DNU    -         -
*Gi0/4                NA          Sync/En      20    QL-SEC    -         -

Interface:
---------------------------------------------
Local Interface: Internal
Signal Type: NA
Mode: NA(Ql-enabled)
SSM Tx: DISABLED
SSM Rx: DISABLED
Priority: 251
QL Receive: QL-SEC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 0
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE
SNMP input source index: 1
SNMP parent list index: 0
Description: None

Local Interface: To0/6
Signal Type: NA
Mode: NA(Ql-enabled)
SSM Tx: ENABLED
SSM Rx: ENABLED
Priority: 1
QL Receive: QL-DNU
QL Receive Configured: -
QL Receive Overrided: QL-FAILED
QL Transmit: -
QL Transmit Configured: -
```

```
Hold-off: 300
Wait-to-restore: 300
Lock Out: FALSE
Signal Fail: TRUE
Alarms: FALSE
Slot Disabled: FALSE
SNMP input source index: 2
SNMP parent list index: 0
Description: None

Local Interface: Gi0/1
Signal Type: NA
Mode: Synchronous(Ql-enabled)
ESMC Tx: ENABLED
ESMC Rx: ENABLED
Priority: 1
QL Receive: QL-DNU
QL Receive Configured: -
QL Receive Overrided: QL-DNU
QL Transmit: QL-SEC
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 300
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE
SNMP input source index: 3
SNMP parent list index: 0
Description: None

Local Interface: Gi0/4
Signal Type: NA
Mode: Synchronous(Ql-enabled)
ESMC Tx: ENABLED
ESMC Rx: ENABLED
Priority: 20
QL Receive: QL-SEC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: QL-DNU
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 300
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE
SNMP input source index: 4
SNMP parent list index: 0
Description: None
```

show platform hardware

To display the status of hardware devices on the Cisco ASR 901S, use the **show platform hardware** command. The command displays information about hardware devices on the Cisco ASR 901S for troubleshooting and debugging purposes.

show platform hardware {adrian | bits | cpld | cpu | ethernet | fio | hwic | rtm | stratum | ufe winpath

Syntax Description

adrian	Displays information about the adrian hardware.
cpld	Displays information about the CPLD hardware.
cpu	Displays information about the CPU.
ethernet	Displays information about the ethernet interfaces on the Cisco ASR 901S.
fio	Displays information about the FIO fpga hardware.
hwic	Displays information about the HWICs installed on the Cisco ASR 901S.
rtm	Displays information about the RTM Module (ASM-M2900-TOP daughter card).
stratum	Displays information about the stratum hardware.
ufe	Displays information about the UFE hardware.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

show platform ptp state

To display the status of ptp protocol on the Cisco ASR 901S router, use the **show platform ptp state** command.

show platform ptp state

Syntax Description

This command has no arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Examples

The following example shows sample output for **show platform ptp state** comamnd:

```
Router# show platform ptp state
flag = 2
     FLL State                     : 2 (Fast Loop)
     FLL Status Duration           : 7049 (sec)

     Forward Flow Weight           : 0.0
     Forward Flow Transient-Free   : 900 (900 sec Window)
     Forward Flow Transient-Free   : 3600 (3600 sec Window)
     Forward Flow Transactions Used: 23.0 (%)
     Forward Flow Oper. Min TDEV   : 4254.0 (nsec)
     Forward Mafie                 : 38.0
     Forward Flow Min Cluster Width: 7550.0 (nsec)
     Forward Flow Mode Width       : 21400.0 (nsec)

     Reverse Flow Weight           : 100.0
     Reverse Flow Transient-Free   : 900 (900 sec Window)
     Reverse Flow Transient-Free   : 3600 (3600 sec Window)
     Reverse Flow Transactions Used: 200.0 (%)
     Reverse Flow Oper. Min TDEV   : 487.0 (nsec)
     Reverse Mafie                 : 36.0
     Reverse Flow Min Cluster Width: 225.0 (nsec)
     Reverse Flow Mode Width       : 450.0 (nsec)

     Frequency Correction          : 257.0 (ppb)
     Phase Correction              : 0.0 (ppb)

     Output TDEV Estimate          : 1057.0 (nsec)
     Output MDEV Estimate          : 1.0 (ppb)

     Residual Phase Error          : 0.0 (nsec)
     Min. Roundtrip Delay          : 45.0 (nsec)

     Sync Packet Rate              : 65 (pkts/sec)
     Delay Packet Rate             : 65 (pkts/sec)

     Forward IPDV % Below Threshold: 0.0
     Forward Maximum IPDV          : 0.0 (usec)
Forward Interpacket Jitter    : 0.0 (usec)

Reverse IPDV % Below Threshold: 0.0
Reverse Maximum IPDV          : 0.0 (usec)
Reverse Interpacket Jitter    : 0.0 (usec)
```

Related Commands

Command	Description
show platform ptp stats	Displays statistics about the ptp protocol on the Cisco ASR 901S router.

show platform ptp stats

To display statistics about ptp protocol on the Cisco ASR 901S router, use the **show platform ptp stats** command.

show platform ptp stats

Syntax Description

This command has no arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Examples

The following example shows sample output for `show platform ptp stats` comamnd:

```
Router# show platform ptp stats
Statistics for PTP clock 0
###############################
Number of ports : 1
Pkts Sent : 1811997
Pkts Rcvd : 619038
Pkts Discarded : 0
Statistics for PTP clock port 1
##################################
Pkts Sent : 1811997
Pkts Rcvd : 619038
Pkts Discarded : 0
Signals Rejected : 0
Statistics for peer 1
########################
IP addr : 9.9.9.14
Pkts Sent : 355660
Pkts Rcvd : 124008
Statistics for peer 2
########################
IP addr : 9.9.9.13
Pkts Sent : 355550
Pkts Rcvd : 123973
Statistics for peer 3
########################
IP addr : 9.9.9.11
Pkts Sent : 354904
Pkts Rcvd : 123972
Statistics for peer 4
########################
IP addr : 9.9.9.12
Pkts Sent : 353815
Pkts Rcvd : 123525
Statistics for peer 5
########################
IP addr : 9.9.9.10
Pkts Sent : 352973
Pkts Rcvd : 123326
```

Related Commands

Command	Description
show platform ptp status	Displays the status of the ptp protocol on the Cisco ASR 901S router.

show platform ptp stats detailed

To display detailed statistics about ptp protocol on the Cisco ASR 901S router, use the **show platform ptp stats detailed** command.

show platform ptp stats detailed

Syntax Description

This command has no arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Examples

The following example shows sample output for `show platform ptp stats detailed` comamnd:

```
Router# show platform ptp stats detailed
Statistics for PTP clock 0
###############################
Number of ports   : 1
Pkts Sent         : 37416
Pkts Rcvd         : 113563
Invalid Pkts Rcvd : 0
        Statistics for PTP clock port 1
        ##################################
        Pkts Sent         : 37416
        Pkts Rcvd         : 113563
        Invalid Pkts Rcvd : 0
                Statistics for peer 0
                ########################
                IP address           : 10.10.10.10
                Announces Sent       : 0
                Announces Rcvd       : 297
                Syncs Sent           : 0
                Syncs Rcvd           : 37925
                Follow Ups Sent      : 0
                Follow Ups Rcvd      : 37925
                Delay Reqs Sent      : 37404
                Delay Reqs Rcvd      : 0
                Delay Resps Sent     : 0
                Delay Resps Rcvd     : 37404
                Mgmts Sent Rcvd      : 0
                Mgmts Rcvd           : 0
                Signals Sent         : 12
                Signals Rcvd         : 12
                Invalid Packets Rcvd : 0
```

Related Commands

Command	Description
show platform ptp stats	Displays the statistics of the ptp protocol on the Cisco ASR 901S router.

show platform tcam detailed

To display the current occupancy that includes per-TCAM rules information such as number of TCAM rules used or free and feature(s) using the TCAM rule, use the show platform tcam detailed command.

show platform tcam detailed

Syntax Description

This command has no arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.3(2)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Examples

The following is sample output from the **show platform tcam detailed** command:

```
Router# show platform tcam detailed

Ingress    : 2/8 slices, 512/2048 entries used
Pre-Ingress: 3/4 slices, 768/1024 entries used
Egress     : 0/4 slices, 0/512 entries used

Slice ID: 1
Stage: Pre-Ingress
Mode: Single
Entries used: 28/256
Slice allocated to: Layer-2 Classify and Assign Group

Slice ID: 4
Stage: Pre-Ingress
Mode: Double
Entries used: 10/128
Slice allocated to: L2CP

Slice ID: 2
Stage: Ingress
Mode: Double
Entries used: 29/128
Slice allocated to: L2 Post-Switch Processing Group

Slice ID: 3
Stage: Ingress
Mode: Single
Entries used: 13/256
Slice allocated to: CESoPSN-UDP, CEF, Layer-3 Control Protocols
```

show platform tcam summary

To display the current occupancy of TCAM with summary of the number of TCAM rules allocated or free, use the show platform tcam summary command.

show platform tcam summary

Syntax Description

This command has no arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.3(2)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Examples

The following is sample output freom the **show platform tcam summary** command:

```
Router# show platform tcam summary
Ingress    : 2/8 slices, 512/2048 entries used
Pre-Ingress: 3/4 slices, 768/1024 entries used
Egress     : 0/4 slices, 0/512 entries used
```

show policy-map

To display the configuration of all classes for a specified service policy map or of all classes for all existing policy maps, use the **show policy-map** command in user EXEC or privileged EXEC mode.

show policy-map [*policy-map*]

Syntax Description

policy-map	(Optional) Name of the service policy map whose complete configuration is to be displayed. The name can be a maximum of 40 characters.

Command Default

All existing policy map configurations are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The **show policy-map** command displays the configuration of a policy map created using the **policy-map** command. You can use the **show policy-map** command to display all class configurations comprising any existing service policy map, whether or not that policy map has been attached to an interface. The command displays:

- ECN marking information only if ECN is enabled on the interface.
- Bandwidth-remaining ratio configuration and statistical information, if configured and used to determine the amount of unused (excess) bandwidth to allocate to a class queue during periods of congestion.

Examples

This section provides sample output from typical **show policy-map** commands. Depending upon the interface or platform in use and the options enabled (for example, Weighted Fair Queueing [WFQ]), the output you see may vary slightly.

Traffic Policing: Example

The following is sample output from the **show policy-map** command. This sample output displays the contents of a policy map called “policy1.” In policy 1, traffic policing on the basis of a committed information rate (CIR) of 20 percent has been configured, and the bc and be have been specified in milliseconds. As part of the traffic policing configuration, optional conform, exceed, and violate actions have been specified.

```
Router# show policy-map policy1

  Policy Map policy1
    Class class1
     police cir percent 20 bc 300 ms pir percent 40 be 400 ms
```

```
      conform-action transmit
      exceed-action drop
      violate-action drop
```

Table 2-10 describes the significant fields shown in the display.

Table 2-10 show policy-map Field Descriptions—Configured for Traffic Policing

Field	Description
Policy Map	Name of policy map displayed.
Class	Name of the class configured in the policy map displayed.
police	Indicates that traffic policing on the basis of specified percentage of bandwidth has been enabled. The committed burst (Bc) and excess burst (Be) sizes have been specified in milliseconds (ms), and optional conform, exceed, and violate actions have been specified.

Related Commands

Command	Description
class (policy map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
class–map	Creates a class map to be used for matching packets to a specified class.
drop	Configures a traffic class to discard packets belonging to a specific class.
police	Configures traffic policing.
police (two rates)	Configures traffic policing using two rates, the CIR and the PIR.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
show table-map	Displays the configuration of a specified table map or of all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

show policy-map interface

To display the statistics and the configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command in user EXEC or privileged EXEC mode.

show policy-map interface [**type access-control**] *type number* [**dlci** *dlci*] [**input** | **output**]

Syntax Description

type	Type of interface or subinterface whose policy configuration is to be displayed.
number	Port, connector, or interface card number.
dlci	(Optional) Indicates a specific PVC for which policy configuration will be displayed.
dlci	(Optional) A specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC will be displayed when a DLCI is specified.
input	(Optional) Indicates that the statistics for the attached input policy will be displayed.
output	(Optional) Indicates that the statistics for the attached output policy will be displayed.

Command Default

This command displays the packet statistics of all classes that are configured for all service policies on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The **show policy-map interface** command displays the packet statistics for classes on the specified interface or the specified PVC only if a service policy has been attached to the interface or the PVC.

The counters displayed after the **show policy-map interface** command is entered are updated only if congestion is present on the interface.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
police	Configures traffic policing.
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
police (two rates)	Configures traffic policing using two rates, the CIR and the PIR.

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Specifies that low-latency behavior must be given to a traffic class and configures multiple priority queues.
shape (percent)	Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface.
show class-map	Display all class maps and their matching criteria.
show interfaces	Displays statistics for all interfaces configured on a router or access server.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map class	Displays the configuration for the specified class of the specified policy map.

show ptp port running detail

To display the running details of the PTP port, use the **show ptp port running detail** command.

show ptp port running detail

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.4(1)S	This command was introduced on the Cisco ASR 901S Series Aggregation Services Routers.

Usage Guidelines

This command is used to display running details of the PTP port.

Note Accuracy and log variance are not displayed for the telecom profile since the fields are not required for selecting the best master.

Examples

This example shows the output from **show ptp port running detail** command on a Cisco ASR 901 router:

```
Router# show ptp port running detail

PORT [SLAVE] CURRENT PTP MASTER PORT
  Protocol Address: 10.10.10.10
  Clock Identity: 0xE4:D3:F1:FF:FE:22:FD:B8

PORT [SLAVE] PREVIOUS PTP MASTER PORT
  Protocol Address: 30.30.30.30
  Clock Identity: 0xE0:2F:6D:FF:FE:74:EF:70
  Reason:

PORT [SLAVE] LIST OF PTP MASTER PORTS

LOCAL PRIORITY 0
  Protocol Address: 10.10.10.10
  Clock Identity:  0xE4:D3:F1:FF:FE:22:FD:B8
  PTSF Status:
  Alarm In Stream:
  Clock Stream Id: 0
  Priority1: 128
  Priority2: 128
  Class: 84
  Accuracy: Unknown   <===========
  Offset (log variance): 0 <==========
  Steps Removed: 0
```

```
LOCAL PRIORITY 1
  Protocol Address: 30.30.30.30
  Clock Identity:  0xE0:2F:6D:FF:FE:74:EF:70
  PTSF Status:
  Alarm In Stream:
  Clock Stream Id: 0
  Priority1: 1
  Priority2: 1
  Class: 104
  Accuracy: Unknown   <========
  Offset (log variance): 0   <======
  Steps Removed: 0
```

show rep topology

Use the **show rep topology** User EXEC command to display Resilient Ethernet Protocol (REP) topology information for a segment or for all segments, including the primary and secondary edge ports in the segment.

show rep topology [segment *segment_id*] [**archive**] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

segment-id	(Optional) Display REP topology information for the specified segment. The ID range is from 1 to 1024.
archive	(Optional) Display the previous topology of the segment. This keyword can be useful for troubleshooting a link failure.
detail	(Optional) Display detailed REP topology information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The output of this command is also included in the **show tech-support** privileged EXEC command output.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is a sample output from the **show rep topology segment** privileged EXEC command:

```
Switch # show rep topology segment 1
REP Segment 1
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
sw1_multseg_3750 Gi1/1/1    Pri  Alt
sw3_multseg_3400 Gi0/13          Open
sw3_multseg_3400 Gi0/14          Alt
sw4_multseg_3400 Gi0/13          Open
sw4_multseg_3400 Gi0/14          Open
sw5_multseg_3400 Gi0/13          Open
sw5_multseg_3400 Gi0/14          Open
sw2_multseg_3750 Gi1/1/2         Open
sw2_multseg_3750 Gi1/1/1         Open
sw1_multseg_3750 Gi1/1/2    Sec  Open
```

This is a sample output from the **show rep topology** command when the edge ports are configured to have no REP neighbor:

```
Switch # show rep topology
REP Segment 2
BridgeName       PortName   Edge  Role
---------------- ---------- ----  ----
sw8-ts8-51       Gi0/2      Pri*  Open
sw9-ts11-50      Gi1/0/4          Open
sw9-ts11-50      Gi1/0/2          Open
sw1-ts11-45      Gi0/2            Alt
sw1-ts11-45      Po1              Open
sw8-ts8-51       Gi0/1      Sec*  Open
```

This example shows output from the **show rep topology detail** command:

```
Router# show rep topology detail
REP Segment 2
repc_2_24ts, Fa0/2 (Primary Edge)
  Alternate Port, some vlans blocked
  Bridge MAC: 0019.e714.5380
  Port Number: 004
  Port Priority: 080
  Neighbor Number: 1 / [-10]
repc_3_12cs, Gi0/1 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 001
  Port Priority: 000
  Neighbor Number: 2 / [-9]
repc_3_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 3 / [-8]
repc_4_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a19d.7c80
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 4 / [-7]
repc_4_12cs, Gi0/2 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 001a.a19d.7c80
  Port Number: 002
  Port Priority: 040
  Neighbor Number: 5 / [-6]

<output truncated>
```

This example shows output from the **show rep topology segment archive** command:

```
Router# show rep topology segment 1 archive
REP Segment 1
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
sw1_multseg_3750 Gi1/1/1    Pri  Open
sw3_multseg_3400 Gi0/13          Open
sw3_multseg_3400 Gi0/14          Open
sw4_multseg_3400 Gi0/13          Open
sw4_multseg_3400 Gi0/14          Open
sw5_multseg_3400 Gi0/13          Open
sw5_multseg_3400 Gi0/14          Open
sw2_multseg_3750 Gi1/1/2         Alt
sw2_multseg_3750 Gi1/1/1         Open
sw1_multseg_3750 Gi1/1/2    Sec  Open
```

Related Commands

Command	Description
rep segment	Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port.

show table-map

To display the configuration of a specified table map or all table maps, use the **show table-map** command in EXEC mode.

show table-map *table-map-name*

Syntax Description

table-map-name	Name of table map used to map one packet-marking value to another. The name can be a maximum of 64 alphanumeric characters.

Command Modes

EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Examples

The sample output of the **show table-map** command shows the contents of a table map called “map 1”. In “map1”, a “to–from” relationship has been established and a default value has been defined. The fields for establishing the “to–from” mappings are further defined by the policy map in which the table map will be configured. (Configuring a policy map is the next logical step after creating a table map.)

For instance, a precedence or differentiated services code point (DSCP) value of 0 could be mapped to a class of service (CoS) value of 1, or vice versa, depending on the how the values are defined in the table map. Any values not explicitly defined in a “to–from” relationship will be set to a default value.

The following sample output of the **show table-map** command displays the contents of a table map called “map1”. In this table map, a packet-marking value of 0 is mapped to a packet-marking value of 1. All other packet-marking values are mapped to the default value 3.

```
Router# show table-map map1

 Table Map map1
 from 0 to 1
 default 3
```

Table 2-11 describes the fields shown in the display.

Table 2-11 show table-map Field Descriptions

Field	Description
Table Map	The name of the table map being displayed.
from, to	The values of the “to–from” relationship established by the **table-map** (value mapping) command and further defined by the policy map in which the table map will be configured.
default	The default action to be used for any values not explicitly defined in a “to–from” relationship by the **table-map** (value mapping) command. If a default action is not specified in the table-map (value mapping) command, the default action is “copy”.

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
table-map (**value mapping**)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

show xconnect

To display information about xconnect attachment circuits and pseudowires (PWs), use the **show xconnect all** command in privileged EXEC mode.

show xconnect {**all** | **interface** *interface* | **peer** *ip-address* {**all** | **vcid** *vcid*}} [**detail**]

Syntax Description

all	Displays information about all xconnect attachment circuits and PWs.
interface *interface*	Displays information about xconnect attachment circuits and PWs on the specified interface. Valid values for the argument are as follows: • **serial** *number*—Displays xconnect information for a specific serial interface. • **serial** *number dlci-number*—Displays xconnect information for a specific Frame Relay data-link connection identifier (DLCI). • **vlan** *vlan-number*—Displays vlan-mode xconnect information for a specific VLAN interface.
peer *ip-address* {**all** | **vcid** *vcid*}	Displays information about xconnect attachment circuits and PWs associated with the specified peer IP address. • **all**—Displays all xconnect information associated with the specified peer IP address. • **vcid** *vcid*—Displays xconnect information associated with the specified peer IP address and the specified VC ID.
detail	(Optional) Displays detailed information about the specified xconnect attachment circuits and PWs.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The **show xconnect all** command can be used to display, sort, and filter basic information about all xconnect attachment circuits and PWs.

You can use the **show xconnect all** command output to help determine the appropriate steps to troubleshoot an xconnect configuration problem. More specific information about a particular type of xconnect can be displayed using the commands listed in the Related Commands table.

Examples

The following example shows **show xconnect all** command output in the brief (default) display format. The output shows information about the interfaces and VCs that have been configured to transport various Layer 2 packets on the router.

```
Router# show xconnect all

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
```

```
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST     Segment 1  S1 Segment 2 S2
ST     Segment 1                        S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Et0/0(Ethernet)              UP mpls 10.55.55.2:1000              UP
UP     ac   Et1/0.1:200(Eth VLAN)        UP mpls 10.55.55.2:5200              UP
IA pri ac   Et1/0.2:100(Eth VLAN)        UP ac   Et2/0.2:100(Eth VLAN)        UP
UP sec ac   Et1/0.2:100(Eth VLAN)        UP mpls 10.55.55.3:1101              UP
```

Table 2-12 describes the significant fields shown in the display.

Table 2-12 show xconnect all Field Descriptions

Field	Description
XC ST	• State of the xconnect attachment circuit or PW. Valid states are: • UP—The xconnect attachment circuit or PW is up. Both segment 1 and segment 2 must be up for the xconnect to be up. • DN—The xconnect attachment circuit or PW is down. Either segment 1, segment 2, or both segments are down. • IA—The xconnect attachment circuit or PW is inactive. This state is valid only when PW redundancy is configured. • NH—One or both segments of this xconnect no longer has the required hardware resources available to the system.
Segment 1 or Segment 2	Information about the type of xconnect, the interface type, and the IP address the segment is using. Types of xconnects are: • ac—Attachment circuit. • pri ac—Primary attachment circuit. • sec ac—Secondary attachment circuit. • mpls—Multiprotocol Label Switching. • l2tp—Layer 2 Tunnel Protocol.
S1 or S2	State of the segment. Valid states are: • UP—The segment is up. • DN—The segment is down. • AD—The segment is administratively down.

The following example shows **show xconnect all** command output in the detailed display format:

```
Router# show xconnect all detail

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No HardwareXC
ST     Segment 1                        S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Et0/0(Ethernet)              UP mpls 10.55.55.2:1000              UP
            Interworking: ip                     Local VC label 16
                                                 Remote VC label 16
                                                 pw-class: mpls-ip
UP     ac   Et1/0.1:200(Eth VLAN)        UP mpls 10.55.55.2:5200              UP
            Interworking: ip                     Local VC label 17
                                                 Remote VC label 20
                                                 pw-class: mpls-ip
```

```
IA pri ac   Et1/0.2:100(Eth VLAN)       UP ac   Et2/0.2:100(Eth VLAN)        UP
            Interworking: none                  Interworking: none
UP sec ac   Et1/0.2:100(Eth VLAN)       UP mpls 10.55.55.3:1101              UP
            Interworking: none                  Local VC label 23
                                                Remote VC label 17
                                                pw-class: mpls
```

The additional fields displayed in the detailed output are self-explanatory.

Related Commands

Command	Description
show connect	Displays configuration information about drop-and-insert connections that have been configured on a router.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show mpls l2transport binding	Displays VC label binding information.
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

snmp mib rep trap-rate

To enable the router to send REP traps and sets the number of traps sent per second, use the **snmp mib rep trap-rate** command. To remove the traps, enter the **no snmp mib rep trap-rate** command.

snmp mib rep trap-rate *value*

no snmp mib rep trap-rate

Syntax Description

value	Specifies the number of traps sent per second. The range is from 0 to 1000. The default is 0 (no limit imposed; a trap is sent at every occurrence).

Command Modes

Global Configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The **snmp mib rep trap-rate** command configures the switch to send REP-specific traps to notify the SNMP server of link operational status changes and port role changes.

Examples

The example shows how to configure the switch to send REP-specific traps:

```
Router(config)# snmp mib rep trap-rate 500
```

speed

To configure the speed for a Fast Ethernet or Gigabit Ethernet interface, use the **speed** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

speed {**10** | **100** | **1000**}

no speed

Syntax Description

10	Configures the interface to transmit at 10 Mbps.
100	Configures the interface to transmit at 100 Mbps.
1000	Configures the interface to transmit at 1000 Mbps. This keyword is valid only for interfaces that support Gigabit Ethernet.

Defaults

1000 M

Command Modes

Interface configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Use the **speed** [**10** | **100** | **1000**] command for 10/100/1000 ports, the **speed 1000** command for Gigabit Ethernet ports.

Gigabit Ethernet Interfaces

The Gigabit Ethernet interfaces are full duplex only. You cannot change the duplex mode on the Gigabit Ethernet interfaces or on a 10/100/1000-Mbps interface that is configured for Gigabit Ethernet.

Speed Command Syntax Combinations

Table 2-1 lists the supported command options by interface.

Table 2-13 Supported Speed Command Options

Interface Type	Supported Syntax	Default Setting	Usage Guidelines
Gigabit Ethernet module	**speed 1000**	Speed is 1000	Speed, duplex, and flow control are enabled.
10-Mbps ports	Factory set	—	

When manually configuring the interface speed to either 10 or 100 Mbps, the switch prompts you to configure duplex mode on the interface.

Speed and Duplex Combinations

Table 2-14 describes the interface behavior for various combinations of the **duplex** and **speed** command settings. The specified **duplex** command configured with the specified **speed** command produces the resulting system action.

If you decide to configure the interface speed and duplex commands manually, and enter a value (for example, speed 10 or speed 100), ensure that you configure the connecting interface speed command to a matching speed.

You cannot set the duplex mode to **half** when the port speed is set at 1000 and similarly, you cannot set the port speed to **1000** when the mode is set to half duplex.

⚠ **Caution** Changing the interface speed and duplex mode might shut down and re-enable the interface during the reconfiguration.

Table 2-14 Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex half	**speed 10**	Forces 10-Mbps and half-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 10**	Forces 10-Mbps and full-duplex operation, and disables autonegotiation on the interface.
duplex half	**speed 100**	Forces 100-Mbps and half-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 100**	Forces 100-Mbps and full-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 1000**	Forces 1000-Mbps and full-duplex operation, and disables autonegotiation on the interface (Gigabit Ethernet only).

Examples

The following example specifies advertisement of 10 Mbps operation only, and either full-duplex or half-duplex capability during autonegotiation:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/1
Router(config-if)# speed 10
Router(config-if)# duplex full
```

With this configuration, the interface advertises the following capabilities during autonegotiation:

- 10 Mbps and half duplex
- 10 Mbps and full duplex

Related Commands

Command	Description
duplex	Configures the duplex operation on an interface.
interface gigabitethernet	Selects a particular Gigabit Ethernet interface for configuration.
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

synce state master

To configure the synchronous ethernet copper port as master, use the **synche state master** command. Use the **no** form of the command to disable the configuration.

synce state master

no synce state master

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
15.1(2)SNG	This command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The **synce state master** command configures the synchronous ethernet copper port as the master in the interface configuration mode.

Examples

The following command configures the ethernet copper port as master:

```
Router(config-if)# synce state master
```

Related Commands

Command	Description
synce state slave	Configures the synchronous ethernet copper port as slave.

synce state slave

To configure the synchronous ethernet copper port as slave, use the **synche state slave** command. Use the **no** form of the command to disable the configuration.

synce state slave

no synce state slave

Syntax Description

This command has no arguments.

Command Default

None.

Command Modes

Interface configuration mode.

Command History

Release	Modification
15.1(2)SNG	This command was introduced on the Cisco ASR 901S router.

Usage Guidelines

The **synce state slave** command configures the synchronous ethernet copper port as the slave in the interface configuration mode.

Examples

The following command configures the ethernet copper port as slave:

```
Router(config-if)# synce state slave
```

Related Commands

Command	Description
synce state master	Configures the synchronous ethernet copper port as master.

synchronous mode

To configure the ethernet interface to synchronous mode, use the **synchronous mode** command. Use the **no** form of the command to disable the configuration.

synchronous mode

no synchronous mode

Command Default

Asynchronous mode.

Command Modes

Interface configuration.

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

This command is applicable to Synchronous Ethernet capable interfaces. The default value is asynchronous mode.

Examples

This example configures the ethernet interface to synchronous mode:

```
Router(config-if)#synchronous mode
```

table-map

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the **table-map** command in address family or router configuration mode. To disable this function, use the **no** form of the command.

table-map *map-name*

no table-map *map-name*

Syntax Description

map-name	Route map name from the **route-map** command.

Defaults

This command is disabled by default.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

This command adds the route map name defined by the **route-map** command to the IP routing table. This command is used to set the tag name and the route metric to implement redistribution.

You can use **match** clauses of route maps in the **table-map** command. IP access list, autonomous system paths, and next hop match clauses are supported.

Examples

In the following router configuration mode example, the Cisco IOS software is configured to automatically compute the tag value for the BGP learned routes and to update the IP routing table:

```
route-map tag
 match as path 10
 set automatic-tag
!
router bgp 100
 table-map tag
```

In the following address family configuration mode example, the Cisco IOS software is configured to automatically compute the tag value for the BGP learned routes and to update the IP routing table:

```
route-map tag
 match as path 10
 set automatic-tag
!
```

```
router bgp 100
address-family ipv4 unicast
 table-map tag
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpn4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
match as-path	Matches a BGP autonomous system path access list.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

termination

Configures the DSL interface to function as central office equipment or customer premises equipment. Use the **no** form of this command to remove the configuration.

termination {co | cpe}

no termination {co | cpe}

Syntax Description

co	The WIC functions as central office equipment and can interface with another G.SHDSL WIC configured as cpe
cpe	The WIC functions as customer premises equipment and can interface with a DSLAM or with another G.SHDSL WIC configured as co.

Defaults

The default setting is **cpe**.

Command Modes

Controller configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

transport ipv4

Specifies the IP version, traffic type (multicast or unicast), and interface that a PTP clock port uses to send traffic.

transport ipv4 {unicast | multicast} *interface slot/port* **[negotiation]**

no transport ipv4 {unicast | multicast} interface *slot/port* **[negotiation]**

Syntax Description

unicast	Specifies that the router sends unicast PTP traffic.
multicast	Specifies that the router sends multicast PTP traffic.
interface	Specifies the interface used to send PTP traffic.
*slot***/***port*	Backplane slot number and port number on the interface. Refer to your hardware installation manual for the specific values and slot numbers.
subslot number	Defines the subslot on the router in which the HWIC is installed.
port	Port number of the controller. Valid numbers are 0 and 1. The slash mark (**/**) is required between the *slot* argument and the *port* argument.
negotiation	(Optional) Enables dynamic discovery of slave devices and their preferred format for sync interval and announce interval messages.

Defaults

The IP version, transmission mode, and interface are not specified for exchanging timing packets.

Command Modes

PTP clock-port configuration mode

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Examples

The following example shows how to enable ptp priority1 value:

```
Router# configure terminal
Router(config)# ptp clock ordinary domain 0
Router (config-ptp-clk)# clock-port MASTER Master
Router (config-ptp-port)# transport ipv4 unicast interface loopback 23 negotiation
Router(config-ptp-port)# exit
Router(config-ptp-clk)# exit
```

Related Commands

Command	Description
clock-port	Specifies the mode of a PTP clock port.

tune-buffer port

To configure hardware buffer values on the port to avoid traffic drops due to congestion, use the **tune-buffer port** command in global configuration mode. To remove this configuration, use the **no** form of this command.

tune-buffer port *port-no*

Syntax Description

port-no	Port number associated with Gigabit Ethernet interfaces. Valid values range from 0 to 11.

Command Default

This configuration is disabled by default.

Command Modes

Global configuration (config#)

Command History

Release	Modification
15.2(2)SNI	This command was introduced.

Usage Guidelines

This command is used only on the Gigabit Ethernet interfaces. Use this command to avoid traffic drops that occur due to congestion, as a result of formation of micro loops during link recovery.

Examples

The following example shows how to avoid traffic drops:

```
Router# configure terminal
Router(config)# tune-buffer port 2
```

xconnect logging redundancy

To enable system message log (syslog) reporting of the status of the xconnect redundancy group, use the **xconnect logging redundancy** command in global configuration mode. To disable syslog reporting of the status of the xconnect redundancy group, use the **no** form of this command.

xconnect logging redundancy

no xconnect logging redundancy

Syntax Description

This command has no arguments or keywords.

Defaults

Syslog reporting of the status of the xconnect redundancy group is disabled.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901S router.

Usage Guidelines

Use this command to enable syslog reporting of the status of the xconnect redundancy group.

Examples

The following example enables syslog reporting of the status of the xconnect redundancy group and shows the messages that are generated during switchover events:

```
Router# config t
Router(config)# xconnect logging redundancy
Router(config)# exit
```

Activating the Primary Member

```
00:01:07: %XCONNECT-5-REDUNDANCY: Activating primary member 10.55.55.2:1000
```

Activating the Backup Member:

```
00:01:05: %XCONNECT-5-REDUNDANCY: Activating secondary member 10.55.55.3:1001
```

Related Commands

Command	Description
xconnect	Binds an Ethernet, 802.1q VLAN, or Frame Relay attachment circuit to an Layer 2 PW for xconnect service and enters xconnect configuration mode.