A through C

access-list rate-limit

To configure an access list for use with committed access rate (CAR) policies, use the **access-listrate-limit**command in global configuration mode. To remove the access list from the configuration, use the **no** form of this command.

access-list rate-limit *acl-index* {*precedence*| *mac-address*| *exp*| **mask** *mask*}

no access-list rate-limit *acl-index* {*precedence*| *mac-address*| *exp*| **mask** *mask*}

Syntax Description

acl-index	Access list number. To classify packets by • IP precedence, use any number from 1 to 99 • MAC address, use any number from 100 to 199 • Multiprotocol Label Switching (MPLS) experimental field, use any number from 200 to 299
precedence	IP precedence. Valid values are numbers from 0 to 7.
mac-address	MAC address.
exp	MPLS experimental field. Valid values are numbers from 0 to 7.
mask *mask*	Mask. Use this option if you want to assign multiple IP precedences or MPLS experimental field values to the same rate-limit access list.

Command Default

No CAR access lists are configured.

Command Modes

Global configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.1(5)T	This command now includes an access list based on the MPLS experimental field.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Release	Modification
12.2(4)T	This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to classify packets by the specified IP precedence, MAC address, or MPLS experimental field values for a particular CAR access list. You can then apply CAR policies, using the **rate-limit** command, to individual rate-limit access lists. When packets in an access list are classified in this manner, the packets with different IP precedences, MAC addresses, or MPLS experimental field values are treated differently by the CAR process.

You can specify only one command for each rate-limit access list. If you enter this command multiple times using the same access list number, the new command overwrites the previous command.

Use the **mask** keyword to assign multiple IP precedences or MPLS experimental field values to the same rate-limit list. To ascertain the **mask** value, perform the following steps.

1. Decide which precedences you want to assign to this rate-limit access list.
2. Convert the precedences or MPLS experimental field values into 8-bit numbers with each bit corresponding to one value. For example, an MPLS experimental field value of 0 corresponds to 00000001; 1 corresponds to 00000010; 6 corresponds to 01000000; and 7 corresponds to 10000000.
3. Add the 8-bit numbers for the selected MPLS experimental field values. For example, the mask for MPLS experimental field values 1 and 6 is 01000010.
4. The **access-listrate-limit** command expects hexadecimal format. Convert the binary mask into the corresponding hexadecimal number. For example, 01000010 becomes 42 and is used in the command. Any packets that have an MPLS experimental field value of 1 or 6 will match this access list.

A mask of FF matches any precedence, and 00 does not match any precedence.

Examples

In the following example, MPLS experimental fields with the value of 7 are assigned to the rate-limit access list 200:

```
Router(config)# access-list rate-limit 200 7
```

You can then use the rate-limit access list in a **rate-limit** command so that the rate limit is applied only to packets matching the rate-limit access list.

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# rate-limit input access-group rate-limit 200 8000 8000 8000
conform-action set-mpls-exp-transmit 4 exceed-action set-mpls-exp-transmit 0
```

Related Commands

Command	Description
rate-limit	Configures CAR and DCAR policies.
show access-lists rate-limit	Displays information about rate-limit access lists.

account

To enable collection of statistics for packets matching the traffic class where this command is configured, use the **account** command in policy-map class configuration mode. To disable statistics collection, use the **no** form of this command.

account [drop]

no account

Syntax Description

drop	(Optional) Enables the collection of statistics for packets dropped for the traffic class where it is configured. This is the default behavior.

Command Default

When the **account** command is configured, the default behavior is collection of drop statistics. No statistics are collected if the **account** command is not configured.

Command Modes

Policy-map class (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

The **account** command was implemented as part of the QoS: Policies Aggregation Enhancements feature in Cisco IOS XE Release 2.6 on the Cisco ASR 1000 Series Aggregation Services Routers to support the collection of per-subscriber statistics.

By default when configured, the command enables collection of drop statistics for traffic in the class where it is configured. Therefore, the optional **drop** keyword is not required to enable collection of drop statistics.

You can display the subscriber statistics collected for a certain traffic class using the **showpolicy-mapinterface** command.

Examples

The following example shows enabling of drop statistics collection (the default) for the EF traffic class for the subscriber policy-map:

```
Router(config)# policy-map subscriber
Router(config-pmap)# class EF
Router(config-pmap-c)# account
```

Related Commands

Command	Description
class (policy-map)	Specifies 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.
policy-map	Enters policy-map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

atm-address (qos)

To specify the QoS parameters associated with a particular ATM address, use the **atm-address** command in LANE QoS database configuration mode. To revert to the default value, use the **no** form of this command.

atm-address *atm-address* [**ubr+** **pcr** *value* **mcr** *value*]

no atm-address *atm-address* [**ubr+** **pcr** *value* **mcr** *value*]

Syntax Description

atm-address	Control ATM address.
ubr+	(Optional) Unspecified bit rate plus virtual channel connection (VCC).
pcr	(Optional) Peak cell rate (PCR).
value	(Optional) UBR+ pcr value in kbps.
mcr *value*	(Optional) Minimum cell rate (MCR) value in kbps

Command Default

No default ATM address.

Command Modes

LANE QoS database configuration

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to enter the required QoS parameters using PCR and MCR values on a specific ATM address. This command is entered from LANE QoS database configuration mode.

```
Router(lane-qos)# atm-address 47.0091810000000061705B0C01.00E0B0951A40.0A ubr+ pcr 500000
mcr 100000
```

Related Commands

Command	Description
lane client qos	Applies a QoS over LANE database to an interface.
lane qos database	Begins the process of building a QoS over LANE database.
show lane qos database	Displays the contents of a specific QoS over LANE database.
ubr+ cos	Maps a CoS value to a UBR+ VCC.

attribute

To add attributes to an attribute profile, use the **attribute** command in attribute map configuration mode.

attribute *attribute-name attribute-value*

Syntax Description

attribute-name	Name of the attribute that you want to configure for your profile.
attribute-value	Value of the attribute.

Command Modes

Attribute map configuration (config-attribute-map)

Command History

Release	Modification
15.2(4)M2	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

This command does not have a **no** form.

Examples

The following example shows how to add application-group attributes for your profile:

```
Device# configure terminal
Device(config)# ip nbar attribute-map nntp-attrib
Device(config-attribute-map)# attribute application-group aol-group
Device(config-attribute-map)# end
```

Related Commands

Command	Description
ip nbar attribute-map	Configures attributes for protocols.
ip nbar attribute-set	Attaches a new attribute profile to a protocol.

auto discovery qos

To begin discovering and collecting data for configuring the AutoQoS for the Enterprise feature, use the **autodiscoveryqos** command in interface configuration mode. To stop discovering and collecting data, use the **no** form of this command.

auto discovery qos [trust]

no auto discovery qos

Syntax Description

trust	(Optional) Indicates that the differentiated services code point (DSCP) markings of a packet are trust (that is, relied on) for classification of the voice, video, and data traffic. If the optional **trust** keyword is not specified, the voice, video, and data traffic is classified using network-based application recognition (NBAR), and the packets are marked with the appropriate DSCP value.

Command Default

No data collection is performed.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	The trust mode was modified to classify packets by DSCP value rather than by protocol type.

Usage Guidelines

The **autodiscoveryqos** command initiates the Auto-Discovery (data collection) phase of the AutoQoS for the Enterprise feature. This command invokes NBAR protocol discovery to collect data and analyze the traffic at the egress direction of the interface.

The **noautodiscoveryqos**command terminates the Auto-Discovery phase and removes any data collection reports generated.

The **trust** keyword is used for the trusted model based on the specified DSCP marking. For more information, see the “Trusted Boundary” section of the *AutoQoS for the Enterprise* feature module, Cisco IOS Release 12.3(7)T.

Examples

The following is a sample configuration showing the Auto-Discovery (data collection) phase of the AutoQoS for the Enterprise feature enabled on a serial2/1/1 subinterface.

```
Router> enable
Router# configure terminal
Router(config)# interface serial2/1.1
Router(config-if)# frame-relay interface-dlci 58
Router(config-if)# auto discovery qos
Router(config-if)# end
```

Related Commands

Command	Description
auto qos	Installs the QoS class maps and policy maps created by the AutoQoS for the Enterprise feature.
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.
show auto qos	Displays the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces.

auto qos

To install the quality-of-service (QoS) class maps and policy maps created by the AutoQoS for the Enterprise feature, use the **autoqos** command in interface configuration mode. To remove the QoS policies, use the **no** form of this command.

auto qos

no auto qos

Syntax Description

This command has no arguments or keywords.

Command Default

No QoS policies are installed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The class maps and policy maps are created from the templates that are automatically generated by the AutoQoS for the Enterprise feature. These templates (and the resulting class maps and policy maps) are generated on the basis of the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature. For more information about the Auto-Discovery phase, see the “Configuration Phases” section of the *AutoQoS for the Enterprise* feature module, Cisco IOS Release 12.3(7)T.

The **noautoqos** command removes any AutoQoS-generated class maps and policy maps installed on the interface.

The**autoqos** command is not supported on gigabit interfaces.

Examples

The following is a sample configuration showing the AutoQoS for the Enterprise feature enabled on a serial2/1/1 subinterface. In this configuration, the AutoQoS class maps and policy maps will be installed on the serial2/1 interface.

```
Router> enable
Router# configure terminal
Router(config)# interface serial2/1
Router(config-if)# frame-relay interface-dlci 58
Router(config-if)# auto qos
Router(config-if)# end
```

Related Commands

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.
show auto qos	Displays the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces.

auto qos voip

To configure the AutoQoS--VoIP feature on an interface, use the **autoqosvoip** command in interface configuration mode or Frame Relay DLCI configuration mode. To remove the AutoQoS--VoIP feature from an interface, use the **no** form of this command.

auto qos voip [trust] [fr-atm]

no auto qos voip [trust] [fr-atm]

Syntax Description

trust	(Optional) Indicates that the differentiated services code point (DSCP) markings of a packet are trusted (relied on) for classification of the voice traffic. If the optional **trust** keyword is not specified, the voice traffic is classified using network-based application recognition (NBAR), and the packets are marked with the appropriate DSCP value.
fr-atm	(Optional) Enables the AutoQoS--VoIP feature for Frame-Relay-to-ATM links. This option is available on the Frame Relay data-link connection identifiers (DLCIs) for Frame-Relay-to-ATM interworking only.

Command Default

Default mode is disabled.

Command Modes

Interface configuration (config-if) Frame Relay DLCI configuration (for use with Frame Relay DLCIs) (config-fr-dlci)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To enable the AutoQoS--VoIP feature for Frame-Relay-to-ATM interworking, the **fr-atm**keyword must be configured explicitly. However, the **fr-atm** keyword affects low-speed DLCIs *only* . It does not affect high-speed DLCIs.

Note DLCIs with link speeds lower than or equal to 768 kbps are considered low-speed DLCIs; DLCIs with link speeds higher than 768 kbps are considered high-speed DLCIs.

Depending on whether the **trust** keyword has been configured for this command, the AutoQoS--VoIP feature automatically creates one of the following two policy maps:

- "AutoQoS-Policy-Trust" (created if the **trust** keyword is configured)
- "AutoQoS-Policy-UnTrust" (created if the **trust** keyword is *not* configured)

Both of these policy maps are designed to handle the Voice over IP (VoIP) traffic on an interface or a permanent virtual circuit (PVC) and can be modified to suit the quality of service (QoS) requirements of the network. To modify these policy maps, use the appropriate Cisco IOS command.

These policy maps should not be attached to an interface or PVC by using the **service-policy** command. If the policy maps are attached in this manner, the AutoQoS--VoIP feature (that is, the policy maps, class maps, and access control lists [ACLs]) will not be removed properly when the**noautoqosvoip** command is configured.

For low-speed Frame Relay DLCIs that are interconnected with ATM PVCs in the same network, the **fr-atm** keyword must be explicitly configured in the **autoqosvoip** command to configure the AutoQoS--VoIP feature properly. That is, the command must be configured as **autoqosvoipfr-atm**.

For low-speed Frame Relay DLCIs that are configured with Frame-Relay-to-ATM, Multilink PPP (MLP) over Frame Relay (MLPoFR) is configured automatically. The subinterface must have an IP address. When MLPoFR is configured, this IP address is removed and put on the MLP bundle. The AutoQoS--VoIP feature must also be configured on the ATM side by using the **autoqosvoip** command.

The **autoqosvoip**command is not supported on subinterfaces or gigabit interfaces.

The **autoqosvoip** command is available for Frame Relay DLCIs.

Disabling AutoQoS--VoIP

The **noautoqosvoip** command disables the AutoQoS--VoIP feature and removes the configurations associated with the feature.

When the **noautoqosvoip** command is used, the **no** forms of the individual commands originally generated by the AutoQoS--VoIP feature are configured. With the use of individual **no** forms of the commands, the system defaults are reinstated. The **no** forms of the commands will be applied just as if the user had entered the commands individually. As the configuration reinstating the default setting is applied, any messages resulting from the processing of the commands are displayed.

Note If you delete a subinterface or PVC (either ATM or Frame Relay PVCs) without configuring the **noautoqosvoip** command, the AutoQoS--VoIP feature will not be removed properly.

Examples

The following example shows the AutoQoS--VoIP feature configured on serial point-to-point subinterface 4/1.2. In this example, both the **trust** and **fr-atm**keywords are configured.

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/1.2 point-to-point
Router(config-if)# bandwidth 100
Router(config-if)# ip address 192.168.0.0 255.255.255.0
Router(config-if)# frame-relay interface-dlci 102
Router(config-fr-dlci)# auto qos voip trust fr-atm
Router(config-fr-dlci)# end
Router(config-if#

exit
```

Related Commands

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.
show auto qos	Displays the configurations created by the AutoQoS--VoIP feature on a specific interface or all interfaces.

auto qos voip (6500)

To configure AutoQoS on a voice over IP (VoIP) port interface, use the **autoqosvoip** command in interface configuration mode. To remove AutoQos from the configuration, use the **no** form of this command.

auto qos voip {**cisco-phone**| **cisco-softphone**| **trust**}

no auto qos voip {**cisco-phone**| **cisco-softphone**| **trust**}

Syntax Description

cisco-phone	Enables the quality of service (QoS) ingress macro for the Cisco IP Phone.
cisco-softphone	Enables the QoS ingress macro for the Cisco IP SoftPhone.
trust	Specifies AutoQoS for ports trusting differentiated services code point (DSCP) and class of service (CoS) traffic markings.

Command Default

AutoQos trusts DSCP and CoS traffic markings.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The **autoqosvoip**command is not supported on gigabit interfaces.

The automation of QoS (AutoQoS) allows you to specify the type of QoS parameters desired on a particular port. For example, entering the **autoqosvoipcisco-softphone** command enables the QoS ingress macro for the Cisco IP SoftPhone.

The Smartports feature provides a set of tools for configuring all switch settings related to a specific application with a single command. For example, entering the **autoqosvoipcisco-phone**command configures all the settings necessary to connect an IP phone to the switch.

You can enter the**showautoqos** command to display the configured AutoQoS macros.

AutoQoS and Smartports are supported on the following modules:

- WS-X6548-RJ45
- WS-X6548-RJ21

- WS-X6148-GE_TX
- WS-X6548-GE-TX-CR
- WS-X6148-RJ45V
- WS-X6148-RJ21V
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6248-TEL

Note The**noautoqosvoip** interface configuration command does not disable QoS globally or delete the received CoS-to-internal-DSCP maps created by AutoQoS.

The **autoqosvoipcisco-phone** and the **autoqosvoipcisco-softphone**commands allow you to enable the inbound QoS configuration macros for AutoQoS on an interface. In some cases, the interface-specific **autoqosvoip**commands also generate configuration commands that are applied globally.

You must configure the interface with the **switchport** command if you enter the **autoqosvoipcisco-phone** command. You cannot configure the interface with the **switchport** command if you enter the **autoqosvoipcisco-softphone** command.

If you configure an interface with the **switchport**command, AutoQoS configures the interface to trust CoS. If you do not configure the interface with the **switchport** command, AutoQoS configures the interface to trust DSCP.

AutoQoS uses a nondefault CoS-to-DSCP map. For this reason, you must configure port trust on a per-port-ASIC basis.

When you enter the **autoqosvoipcisco-phone** command, the following behavior occurs:

- QoS is enabled if it is disabled.
- The port is changed to port-based QoS.
- The appropriate CoS map is set.
- All ports are changed to port-based mode (if applicable).
- A trust-CoS QoS policy is created and applied for the ports that need a trust-CoS QoS policy (COIL2 and COIL1).
- A trusted boundary is enabled on the port.
- The CoS value for a trust boundary is set to zero.
- The port trust is set to trust-cos.
- Only 10/100 ports and 10/100/1000 ports are supported.
- A warning message is displayed if the CDP version is not version 2.

When you enter the **autoqosvoipcisco-softphone** command, the following behavior occurs:

- The **cisco-softphone**macro is a superset of the **cisco-phone** macro and configures all features that are required for a Cisco IP Phone to work properly on the Catalyst 6500 series switch.

- The global settings for AutoQoS policy maps, class maps, and access lists are created to classify VoIP packets and to put them in the priority queue or another low-latency queue. The interface settings are created depending on the type of interface and the link speed.
- Two rate limiters are associated with the interface on which the cisco-softphone port-based autoqos macro is executed. The two rate limiters ensure that all inbound traffic on a cisco-softphone port have the following characteristics:
  - The rate of DCSP 46 is at or less than that of the expected softphone rate.
  - The rate of DSCP 26 is at or less than the expected signaling rate.
  - All other traffic is re-marked to DSCP 0 (default traffic).
- DSCP 46 is policed at the rate of 320 kbps with a burst of 2 Kb. DSCP 26 is policed at 32 kbps with a burst of 8 Kb.
- The port is set to untrusted for all port types. The policed-dscp-map is set to ensure that DSCP 46 is marked down to DSCP 0 and DSCP 26 is marked down to DSCP 0. The default QoS IP ACL re-marks all other traffic to DSCP 0.

When you enter the **autoqosvoipsoft-phone** command, the following behavior occurs:

- Enables QoS if QoS is disabled.
- Changes the port to port-based QoS.
- Sets the appropriate police-dscp-map.
- Sets the appropriate CoS-to-DSCP map.
- Changes all ports to port-based mode (if applicable).
- Creates a trust-dscp QoS policy for the ports that need it (COIL2 and COIL1).
- Applies the trust-dscp QoS policy to the port (COIL2 and COIL1).
- Disables a trusted boundary on the port.
- Changes trust to untrusted.
- Allows 10/100 ports and 10/100/1000 ports only.
- Applies two rate limiters, one for DSCP 46 and one for DSCP 26 inbound traffic, and trusts only inbound DSCP 46 and DSCP 26 traffic.
- Marks violations of either rate limiter results in traffic down to DSCP 0.
- Re-marks all other (non-DSCP 26 and 46) inbound traffic to DSCP 0.

When you enter the **autoqosvoiptrust**command, the following applies:

- The DSCP and the CoS markings are trusted for classification of the voice traffic.
- Enables QoS if QoS is disabled.
- Changes the port to port-based QoS.
- Changes all ports to port-based mode (if applicable).
- Creates a trust-dscp and a trust-cos QoS policy for the ports that need it (COIL2 and COIL1).

- Applies the trust-dscp and a trust-cos QoS policy to the port (COIL2 and COIL1).
- Disables the trusted boundary on the port.
- Sets port trust to trust-cos.
- All ports are supported.
- Bases queueing for all ports that allow dscp-to-q mapping on DSCP. If not, queueing is based on CoS.

Examples

The following example shows how to enable the QoS ingress macro for the Cisco IP Phone:

```
Router(config-if)# auto qos voip cisco-phone
```

Related Commands

Command	Description
show auto qos	Displays AutoQoS information.
show running-config interface	Displays the status and configuration of the interface.
switchport	Configures the LAN interface as a Layer 2 switched interface.

bandwidth (policy-map class)

To specify or modify the bandwidth allocated for a class belonging to a policy map, or to enable ATM overhead accounting, use the **bandwidth** command in QoS policy-map class configuration mode. To remove the bandwidth specified for a class or disable ATM overhead accounting, use the **no** form of this command.

bandwidth {*kbps*| [**remaining**] **percent** *percentage*} [**account** {**qinq**| **dot1q**} **aal5** *subscriber-encapsulation*]

no bandwidth

Cisco 10000 Series Router (PRE3)

bandwidth {*kbps*| [**remaining**] **percent** *percentage*} **account** {**qinq**| **dot1q**} {**aal5**| **aal3**} *subscriber-encapsulation***user-defined** *offset* **[atm]**

no bandwidth

Syntax Description

kbps	Amount of bandwidth, in kilobits per second (kbps), to be assigned to the class. The amount of bandwidth varies according to the interface and platform in use. The value must be between 1 and 2,000,000 kbps.
remaining	(Optional) Specifies that the percentage of guaranteed bandwidth is based on a relative percent of available bandwidth.
percent *percentage*	Specifies the percentage of guaranteed bandwidth based on an absolute percent of available bandwidth to be set aside for the priority class or on a relative percent of available bandwidth. The valid range is 1 to 100.
account	(Optional) Enables ATM overhead accounting.
qinq	(Optional) Specifies queue-in-queue encapsulation as the broadband aggregation system (BRAS) to digital subscriber line access multiplexer (DSLAM) encapsulation type for ATM overhead accounting.
dot1q	(Optional) Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type for ATM overhead accounting.
aal5	(Optional) Specifies ATM Adaptation Layer 5 and the encapsulation type at the subscriber line for ATM overhead accounting. AAL5 supports connection-oriented variable bit rate (VBR) services. See the "Usage Guidelines" section for valid encapsulation types.

subscriber-encapsulation	The subscriber line encapsulation type. See the “Usage Guidelines” section for valid encapsulation types.
aal3	Specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either **aal3** or **aal5**.
user-defined *offset*	Specifies the offset size that the router uses when calculating ATM overhead. Valid values are from –127 to127 bytes; 0 is not a valid value. **Note** The router configures the offset size if you do not specify the **user-defined** *offset* option.
atm	Applies ATM cell tax in the ATM overhead calculation. **Note** Configuring both the *offset* and **atm** options adjusts the packet size to the offset size and then adds ATM cell tax.

Command Default

No bandwidth is specified.

ATM overhead accounting is disabled.

Command Modes

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

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE and implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers.
12.0(7)T	This command was modified. The **percent** keyword was added.
12.0(17)SL	This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on Cisco 10000 series routers.
12.0(22)S	This command was modified. Support for the **percent** keyword was added on Cisco 10000 series routers.
12.0(23)SX	This command was modified. Support for the**remaining percent** keyword was added on Cisco 10000 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T and implemented on VIP-enabled Cisco 7500 series routers.

Release	Modification
12.2(2)T	This command was modified. The **remaining percent** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on Cisco 10000 series routers.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the PRE3 for the Cisco 10000 series router, and was enhanced for ATM overhead accounting on the Cisco 10000 series router for the PRE3.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(31)SB6	This command was modified to specify an offset size when calculating ATM overhead and implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC and implemented on Cisco 7600 series routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on Cisco 7300 series routers.
12.4(20)T	This command was modified. Support was added for hierarchical queueing framework (HQF) using the modular quality of service (QoS)CLI (MQC).
15.1(1)T	This command was modified. The allowed values for the *kbps* argument were changed. The value must be from 8 to 2000000.
15.2(1)T	This command was modified. The allowed values for the offset argument and kbps arguments were changed.

Usage Guidelines

Configuring a Policy Map

Use the **bandwidth** command when you configure a policy map for a class defined by the **class-map** command. The **bandwidth** command specifies the bandwidth for traffic in that class. Class-based weighted fair queueing (CBWFQ) derives the weight for packets belonging to the class from the bandwidth allocated to the class. CBWFQ then uses the weight to ensure that the queue for the class is serviced fairly.

Configuring Strict Priority with Bandwidth

You can configure only one class with strict priority. Other classes cannot have priority or bandwidth configuration. To configure minimum bandwidth for another class, use the**bandwidthremainingpercent** command.

Specifying Bandwidth as a Percentage for All Supported Platforms Except the Cisco 10000 Series Routers

Besides specifying the amount of bandwidth in kilobits per second (kbps), you can specify bandwidth as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages. The bandwidth percentage is based on the interface bandwidth. Available bandwidth is equal to the interface bandwidth minus the sum of all bandwidths reserved by the Resource Reservation Protocol (RSVP) feature, the IP RTP Priority feature, and the low latency queueing (LLQ) feature.

Note It is important to remember that when the **bandwidth remaining percent** command is configured, hard bandwidth guarantees may not be provided and only relative bandwidths are assured. That is, class bandwidths are always proportional to the specified percentages of the interface bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. If the link bandwidth is unknown or variable, the router cannot compute class bandwidth guarantees in kbps.

Specifying Bandwidth as a Percentage for the Cisco 10000 Series Routers

Besides specifying the amount of bandwidth in kilobits per second (kbps), you can specify bandwidth as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages. The minimum bandwidth percentage is based on the nearest parent shape rate.

Note It is important to remember that when the **bandwidth remaining percent** command is configured, hard bandwidth guarantees may not be provided and only relative bandwidths are assured. That is, class bandwidths are always proportional to the specified percentages of the interface bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. If the link bandwidth is unknown or variable, the router cannot compute class bandwidth guarantees in kbps.

The router converts the specified bandwidth to the nearest multiple of 1/255 (ESR-PRE1) or 1/65535 (ESR-PRE2) of the interface speed. Use the **show policy-map interface** command to display the actual bandwidth.

Restrictions for All Supported Platforms

The following restrictions apply to the **bandwidth** command:

- The amount of bandwidth configured should be large enough to also accommodate Layer 2 overhead.
- A policy map can have all the class bandwidths specified in either kbps or percentage, but not both, in the same class. However, the unit for the **priority**command in the priority class can be different from the bandwidth unit of the nonpriority class.
- When the **bandwidth percent** command is configured, and a policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached. This restriction does not apply to the **bandwidth remaining percent** command.

Note With CSCsy73939, if the **bandwidth percent** command results in a bandwidth value that is lower than the valid range then the policy map specifying this value cannot be attached to an interface, and the router displays the following error message: "service-policy output parent Configured Percent results in out of range kbps. Allowed range is *min-value–max-value*. The present CIR value is *n*."

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

Note that when the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, then the policy is removed from all interfaces to which it was successfully attached.

Modular QoS CLI Queue Limits

The **bandwidth** command can be used with MQC to specify the bandwidth for a particular class. When used with MQC, the **bandwidth** command uses a default queue limit for the class. This queue limit can be modified using the **queue-limit** command, thereby overriding the default set by the **bandwidth** command.

Note To meet the minimum bandwidth guarantees required by interfaces, modify the default queue limit of high-speed interfaces by using the **queue-limit** command.

Cisco 10000 Series Router

The Cisco 10000 series routers supports the **bandwidth** command on outbound interfaces only. They do not support this command on inbound interfaces.

On the PRE2, you specify a bandwidth value and a unit for the bandwidth value. Valid values for the bandwidth are from 1 to 2488320000. The units are bps, kbps, mbps, and gbps. The default unit is kbps. For example, the following commands configure a bandwidth of 10000 bps and 10000 kbps on the PRE2:

```
bandwidth 10000 bps
bandwidth 10000
```

On the PRE3, youspecify only a bandwidth value. Because the unit is always kbps, the PRE3 does not support the unit argument. Valid values are from 1 to 2000000. For example, the following command configures a bandwidth of 128,000 kbps on the PRE3:

```
bandwidth 128000
```

The PRE3 accepts the PRE2 **bandwidth** command only if the command is used without the unit argument. The PRE3 rejects the PRE2 **bandwidth** command if the specified bandwidth is outside the valid PRE3 bandwidth value range (1 to 2000000).

Besides specifying the amount of bandwidth in kilobits per second (kbps), you can specify bandwidth as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages. The bandwidth percentage is based on the interface bandwidth. However, in a hierarchical policy the minimum bandwidth percentage is based on the nearest parent shape rate.

Note When the **bandwidth remaining percent** command is configured, hard bandwidth guarantees may not be provided and only relative bandwidths are assured. Class bandwidths are always proportional to the specified percentages of the interface bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. If the link bandwidth is unknown or variable, the router cannot compute class bandwidth guarantees in kbps.

The router converts the specified bandwidth to the nearest multiple of 1/255 (PRE1) or 1/65535 (PRE2, PRE3) of the interface speed. Use the **show policy-map interface** command to display the actual bandwidth.

Overhead Accounting for ATM (Cisco 10000 Series Router)

When configuring ATM overhead accounting, you must specify the BRAS-DSLAM, DSLAM-CPE, and subscriber line encapsulation types. The router supports the following subscriber line encapsulation types:

- mux-1483routed
- mux-dot1q-rbe
- snap-pppoa
- mux-rbe
- snap-1483routed
- snap-dot1q-rbe
- mux-pppoa
- snap-rbe

The router calculates the offset size unless you specify the **user-defined** *offset* option.

For hierarchical policies, configure ATM overhead accounting in the following ways:

- Enabled on parent--If you enable ATM overhead accounting on a parent policy, you are not required to enable accounting on the child policy.
- Enabled on child and parent--If you enable ATM overhead accounting on a child policy, then you must enable ATM overhead accounting on the parent policy.

The encapsulation types must match for the child and parent policies.

The user-defined offset values must match for the child and parent policies.

Examples

Examples

In the following example, the policy map named VLAN guarantees 30 percent of the bandwidth to the class named Customer1 and 60 percent of the bandwidth to the class named Customer2. If you apply the VLAN policy map to a 1-Mbps link, 300 kbps (30 percent of 1 Mbps) is guaranteed to class Customer1 and 600 kbps (60 percent of 1 Mbps) is guaranteed to class Customer2, with 100 kbps remaining for the class-default class. If the class-default class does not need additional bandwidth, the unused 100 kbps is available for use by class Customer1 and class Customer2. If both classes need the bandwidth, they share it in proportion to the configured rates. In this example, the sharing ratio is 30:60 or 1:2:

```
router(config)# policy-map VLAN
router(config-pmap)# class Customer1
router(config-pmap-c)# bandwidth percent 30
router(config-pmap-c)# exit
router(config-pmap)# class Customer2
router(config-pmap-c)# bandwidth percent 60
```

Examples

The following example shows how to create a policy map with two classes, shows how bandwidth is guaranteed when only CBWFQ is configured, and shows how to attach the policy to serial interface 3/2/1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth percent 25
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/2/1
Router(config-if)# service output policy1
Router(config-if)# end
```

The following output from the **show policy-map** command shows the configuration for the policy map named policy1:

```
Router# show policy-map policy1

Policy Map policy1
 Class class1
  Weighted Fair Queuing
   Bandwidth 50 (%) Max Threshold 64 (packets)
 Class class2
  Weighted Fair Queuing
   Bandwidth 25 (%) Max Threshold 64 (packets)
```

The output from the **show policy-map interface**command shows that 50 percent of the interface bandwidth is guaranteed for the class named class1, and 25 percent is guaranteed for the class named class2. The output displays the amount of bandwidth as both a percentage and a number of kbps.

```
Router# show policy-map interface serial3/2

Serial3/2
Service-policy output:policy1
Class-map:class1 (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match:none
 Weighted Fair Queuing
  Output Queue:Conversation 265
  Bandwidth 50 (%)
  Bandwidth 772 (kbps) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
Class-map:class2 (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match:none
 Weighted Fair Queuing
  Output Queue:Conversation 266
  Bandwidth 25 (%)
  Bandwidth 386 (kbps) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
Class-map:class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match:any
```

In this example, serial interface 3/2 has a total bandwidth of 1544 kbps. During periods of congestion, 50 percent (or 772 kbps) of the bandwidth is guaranteed to the class named class1, and 25 percent (or 386 kbps) of the link bandwidth is guaranteed to the class named class2.

Examples

In the following example, the interface has a total bandwidth of 1544 kbps. During periods of congestion, 50 percent (or 772 kbps) of the bandwidth is guaranteed to the class named class1, and 25 percent (or 386 kbps) of the link bandwidth is guaranteed to the class named class2.

The following sample output from the **show policy-map** command shows the configuration of a policy map named p1:

```
Router# show policy-map p1
Policy Map p1
 Class voice
  Weighted Fair Queuing
   Strict Priority
   Bandwidth 500 (kbps) Burst 12500 (Bytes)
 Class class1
  Weighted Fair Queuing
   Bandwidth remaining 50 (%) Max Threshold 64 (packets)
 Class class2
  Weighted Fair Queuing
   Bandwidth remaining 25 (%) Max Threshold 64 (packets)
```

The following output from the **show policy-map interface** command on serial interface 3/2 shows that 500 kbps of bandwidth is guaranteed for the class named voice1. The classes named class1 and class2 receive 50 percent and 25 percent of the remaining bandwidth, respectively. Any unallocated bandwidth is divided proportionally among class1, class2, and any best-effort traffic classes.

Note In this sample output (unlike many of the others earlier in this section) the bandwidth is displayed only as a percentage for class 1 and class 2. Bandwidth expressed as a number of kbps is not displayed because the **percent** keyword was used with the **bandwidth remaining** command. The **bandwidth remaining percent** command allows you to allocate bandwidth as a relative percentage of the total bandwidth available on the interface.

```
Router# show policy-map interface serial3/2

Serial3/2
Service-policy output:p1
 Class-map:voice (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:ip precedence 5
  Weighted Fair Queuing
   Strict Priority
   Output Queue:Conversation 264
   Bandwidth 500 (kbps) Burst 12500 (Bytes)
   (pkts matched/bytes matched) 0/0
   (total drops/bytes drops) 0/0
 Class-map:class1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:none
  Weighted Fair Queuing
   Output Queue:Conversation 265
   Bandwidth remaining 50 (%) Max Threshold 64 (packets)
   (pkts matched/bytes matched) 0/0
   (depth/total drops/no-buffer drops) 0/0/0
 Class-map:class2 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:none
  Weighted Fair Queuing
   Output Queue:Conversation 266
   Bandwidth remaining 25 (%) Max Threshold 64 (packets)
   (pkts matched/bytes matched) 0/0
   (depth/total drops/no-buffer drops) 0/0/0
 Class-map:class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:any
```

Examples

When a parent policy has ATM overhead accounting enabled, you are not required to enable ATM overhead accounting on a child traffic class that does not contain the **bandwidth** or **shape** command. In the following configuration example, ATM overhead accounting is enabled for bandwidth on the gaming and class-default class of the child policy map named subscriber_classes and on the class-default class of the parent policy map named subscriber_line. The voip and video classes do not have ATM overhead accounting explicitly enabled; these priority queues have overhead accounting implicitly enabled because ATM overhead accounting is enabled on the parent policy. Notice that the features in the parent and child policies use the same encapsulation type.

```
Router(config)# policy-map subscriber_classes
Router(config-pmap)# class voip
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 8000
Router(config-pmap-c)# exit
Router(config-pmap)# class video
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# police 20
Router(config-pmap-c)# exit
Router(config-pmap)# class gaming
Router(config-pmap-c)# bandwidth remaining percent 80 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining percent 20 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# policy-map subscriber_line
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining ratio 10 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# shape average 512 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# service policy subscriber_classes
```

In the following example, the router uses 20 overhead bytes and ATM cell tax in calculating ATM overhead. The child and parent policies contain the required matching offset values. The parent policy is attached to virtual template 1.

```
Router(config)# policy-map child
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 500 account user-defined 20 atm
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# shape average 30000 account user-defined 20 atm
Router(config-pmap)# exit
Router(config)# exit
Router(config)#
```

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.

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
max-reserved-bandwidth	Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Specifies the priority of a class of traffic belonging to a policy map.
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.
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.

bandwidth qos-reference

To configure bandwidth to be used as a reference for calculating rates of quality of service (QoS) percent configurations on a physical or logical interface, use the **bandwidthqos-reference** command in interface configuration or subinterface configuration mode. To remove this explicitly specified reference bandwidth, use the **no** form of this command.

bandwidth qos-reference *bandwidth-amount*

no bandwidth qos-reference *bandwidth-amount*

Syntax Description

bandwidth-amount	Amount of bandwidth in kilobits per second (kb/s). Valid values are 1 to 10000000.

Command Default

This command is disabled. Reference bandwidth for a logical interface is derived from the main interface or the main interface QoS policy.

Command Modes

Interface configuration (config-if) Subinterface configuration (config-subif)

Command History

Release	Modification
12.2(33)XNE	This command was introduced.
15.1(3)T	Support for logical interfaces is expanded to include the main interface, subinterface, and Frame Relay.

Usage Guidelines

The **bandwidthqos-reference**command is used only as reference for calculating rates of QoS percent configurations on a logical interface. This command does not actually allocate a specified amount of bandwidth for a logical interface.

Note In Cisco IOS Release 12.2(33)XNE, the **bandwidthqos-reference**command is supported only on a tunnel logical interface. In Cisco IOS Release 15.1(3)T, support is expanded to include main interface, subinterface, and Frame Relay as well as tunnel logical interfaces.

Compatibility with the shape (percent) and the police (percent) Commands

The **bandwidthqos-reference**command is compatible with and related to the **shape**(percent) and **police**(percent) commands. The **shape**(percent) command allows you to configure average-rate or peak-rate traffic shaping on the basis of a percentage of bandwidth available on an interface. The **police**(percent) command allows you to configure traffic policing on the basis of a percentage of bandwidth available on an interface.

The **bandwidthqos-reference**command interacts with the**shape**(percent) and **police** (percent) commands in the following ways:

- If the **bandwidthqos-reference**command is used to specify the bandwidth, the**shape** (percent) command and the **police** (percent) commands will use this specified amount to calculate the respective bandwidth percentages.
- If the **bandwidthqos-reference**command is *not* used to specify the bandwidth, the **shape** (percent) command and the **police**(percent) commands will use the amount of bandwidth available on the interface to calculate the respective bandwidth percentages.

Compatibility with bandwidth (interface) Command

The **bandwidth**(interface) command allows you to set the inherited and received bandwidth values for an interface.

If both the **bandwidth** (interface) and **bandwidthqos-reference**commands are enabled on any interface, the value specified by the **bandwidthqos-reference**command is used as the reference for calculating rates for QoS percent configurations on that particular physical or logical interface. The value specified by the **bandwidth**(interface) command is disregarded.

In the sample configuration shown below, the value for the **bandwidthqos-reference** command is entered as 8000 kb/s, and the value for the **bandwidth** (interface) command is entered as 900 kb/s. The value for the **shapeaveragepercent** command is set to 50. The effect is seen in the output for the **targetshaperate** command, which is set to 4000000 bits per second (50 percent of 8000 kb/s):

```
Router(config)# interface e0/1
Router(config-if)# bandwidth qos-reference 8000
Router(config-if)# bandwidth 900

Router(config)# interface e0/1
Router(config-if)# bandwidth 900
Router(config-if)# end
Router# show running-config interface e0/1
interface Ethernet0/1
 bandwidth 900
 bandwidth qos-reference 8000
 no ip address
 load-interval 30
end
Router(config-if)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# interface e0/1
Router(config-if)# service-policy out test
Router# show policy-map interface
 Ethernet0/1
Service-policy output: test
 Class-map: class-default (match-any)
  79 packets, 7837 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 79/7837
  shape (average) cir 4000000, bc 40000, be 40000
  target shape rate 4000000
```

Examples

The following example shows how to configure the**bandwidthqos-reference**command to allocate 2000 kb/s of bandwidth as a reference rate for tunnel interface 1:

```
Router> enable
Router# configure terminal
Router(config)# interface tunnel1
Router#(config-if)# bandwidth qos-reference 2000
```

The following example shows how to configure the**bandwidthqos-reference**command to use 700 kb/s of bandwidth as a reference rate for the main interface e0/1:

```
Router(config)# interface e0/1
Router(config-if)# bandwidth qos-ref 700
Router(config-if)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# interface e0/1
Router(config-if)# service-policy out test
```

The following example shows how to configure the**bandwidthqos-reference**command to use 500 kb/s of bandwidth as a reference rate for the subinterface e0/1.1:

```
Router(config-subif)# interface e0/1
Router(config-if)# no service-policy out test
Router(config-if)# interface e0/1.1
Router(config-subif)# bandwidth qos-ref 500
Router(config-subif)# service-policy ou test
```

The following example shows how to configure the**bandwidthqos-reference**command to use 400 kb/s of bandwidth as a reference rate for the Frame Relay interface s6/0.1:

```
Router(config)# no policy-map test
Router(config)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# map-class frame-relay fr1
Router(config-map-class)# service-policy out test
Router(config-map-class)# end
Router# configure terminal
Router(config)# interface s6/0.1
Router(config-subif)# bandwidth qos-ref 400
Router(config-subif)# end
```

Related Commands

Command	Description
bandwidth (interface)	Sets the inherited and received bandwidth values for an interface.
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
shape (percent)	Specifies average-rate or peak-rate traffic shaping on the basis of a percentage of bandwidth available on an interface.

bandwidth remaining ratio

To specify a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to nonpriority queues, use the**bandwidthremainingratio** command in policy-map class configuration mode. To remove the bandwidth-remaining ratio, use the **no** form of this command.

bandwidth remaining ratio *ratio*

no bandwidth remaining ratio *ratio*

bandwidth remaining ratio *ratio* [**account** {**qinq**| **dot1q**} **[aal5]** {*subscriber-encapsulation*| **user-defined** *offset*}]

no bandwidth remaining ratio *ratio* [**account** {**qinq**| **dot1q**} **[aal5]** {*subscriber-encapsulation*| **user-defined** *offset*}]

bandwidth remaining ratio *ratio*

no bandwidth remaining ratio *ratio*

Syntax Description

ratio	Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues. Valid values are from 1 to 1000. At the subinterface level, the default value is platform dependent. At the class queue level, the default is 1.
Cisco 7300 Series Router, Cisco 7600 Series Router, and Cisco 10000 Series Router	
ratio	Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues. **Note** For the Cisco 7300 series router and 7600 series router, valid values are from 1 to 10000, and the default value is 1. **Note** For the Cisco 10000 series router, valid values are from 1 to 1000, and the default is 1.
account	(Optional) Enables ATM overhead accounting.
qinq	(Optional) Specifies queue-in-queue encapsulation as the Broadband Remote Access Server - Digital Subscriber Line Access Multiplexer (BRAS-DSLAM) encapsulation type.
dot1q	(Optional) Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type.

aal5	(Optional) Specifies the ATM adaptation layer 5 that supports connection-oriented variable bit rate (VBR) services.
subscriber-encapsulation	(Optional) Specifies the encapsulation type at the subscriber line. Encapsulation type varies according to subscriber line.
user-defined *offset*	(Optional) Specifies the offset size, in bytes, that the router uses when calculating the ATM overhead. **Note** For the Cisco 7300 series router and 7600 series router, valid values are from -48 to +48. **Note** For the Cisco 10000 series router, valid values are from -63 to +63.
Cisco ASR 1000 Series Routers	
ratio	Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues. Valid values are from 1 to 1000. At the subinterface level and class-queue level, the default is 1.

For most platforms, the default bandwidth ratio is 1.

Command Default

When you use default bandwidth-remaining ratios at the subinterface level, the Cisco 10000 series router distinguishes between interface types. At the subinterface level, the default bandwidth-remaining ratio is 1 for VLAN subinterfaces and Frame Relay Data Link Connection Identifiers (DLCI). For ATM subinterfaces, the router computes the default bandwidth-remaining ratio based on the subinterface speed.

When you use default bandwidth-remaining ratios at the class level, the Cisco 10000 series router makes no distinction between interface types. At the class level, the default bandwidth-remaining ratio is 1.

Command Modes

Policy-map class (config-pmap-c)

Command History

Release	Modification
12.2(31)SB2	This command was introduced. This command was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SRC	This command was modified. It was implemented on the Cisco 7600 series routers. Additional keywords and arguments were added to support ATM overhead accounting (optional) on the Cisco 7600 series router and the Cisco 10000 series router for the PRE3.

Release	Modification
12.2(33)SB	This comand was modified. Support for the Cisco 7300 series routers was added. The additional keyword and arguments associated with ATM overhead accounting were also supported.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Cisco 10000 Series Router

The scheduler uses the ratio specified in the **bandwidthremainingratio** command to determine the amount of excess bandwidth (unused by priority traffic) to allocate to a class-level queue or a subinterface-level queue during periods of congestion. The scheduler allocates the unused bandwidth relative to other queues or subinterfaces.

The **bandwidthremainingratio** command cannot coexist with another **bandwidth** command in different traffic classes of the same policy map. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
 class precedence_0
  bandwidth remaining ratio 10
 class precedence_2
  bandwidth 1000
```

For the PRE2, the **bandwidthremainingratio** command can coexist with another **bandwidth** command in the same class of a policy map. On the PRE3, the **bandwidthremainingratio** command cannot coexist with another **bandwidth**command in the same class. For example, the following configuration is not valid on the PRE3 and causes an error message to display:

```
policy-map Prec1
 class precedence_0
  bandwidth 1000
  bandwidth remaining ratio 10
```

In a hierarchical policy map in which the parent policy has only the class-default class defined with a child queuing policy applied, the router accepts only the **bandwidthremainingratio** form of the **bandwidth** command in the class-default class.

The **bandwidthremainingratio** command cannot coexist with the **priority** command in the same class. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
 class precedence_1
  priority
  police percent 30
  bandwidth remaining ratio 10
```

All of the queues for which the **bandwidthremainingratio** command is not specified receive the platform-specified minimum bandwidth-remaining ratio. The router determines the minimum committed information rate (CIR) based on the configuration.

ATM Overhead Accounting (Optional)

The **bandwidthremainingratio** command can also be used to enable ATM overhead accounting. To enable ATM overhead accounting, use the **account** keyword and the subsequent keywords and arguments as documented in the Syntax Description table.

Cisco 7200 Series Routers

The**bandwidthremainingratio** command is not supported on the Cisco 7200 series routers. If you have upgraded from Cisco IOS Release 12.2(33)SRD to Cisco IOS Release 12.2(33)SRE, you may see parser errors when you run this command. You can use the **bandwidthremainingpercent** command in place of the **bandwidthremainingratio**command on Cisco 7200 series routers to achieve the same functionality.

Examples

Examples

The following example shows how to configure a bandwidth-remaining ratio on an ATM subinterface. In the example, the router guarantees a peak cell rate of 50 Mbps for the variable bit rate nonreal-time (VBR-nrt) PVC 0/200. During periods of congestion, the subinterface receives a share of excess bandwidth (unused by priority traffic) based on the bandwidth-remaining ratio of 10, relative to the other subinterfaces configured on the physical interface.

```
policy-map Child
 class precedence_0
  bandwidth 10000
 class precedence_1
  shape average 100000
  bandwidth 100
!
policy-map Parent
 class class-default
  bandwidth remaining ratio 10
  shape average 20000000
  service-policy Child
!
interface ATM2/0/3.200 point-to-point
 ip address 10.20.1.1 255.255.255.0
 pvc 0/200
 protocol ip 10.20.1.2
 vbr-nrt 50000
 encapsulation aal5snap
 service-policy output Parent
```

The following example shows how to configure bandwidth remaining ratios for individual class queues. Some of the classes configured have bandwidth guarantees and a bandwidth-remaining ratio explicitly specified. When congestion occurs within a subinterface level, the class queues receive excess bandwidth (unused by priority traffic) based on their class-level bandwidth-remaining ratios: 20, 30, 120, and 100, respectively, for the precedence_0, precedence_1, precedence_2, and precedence_5 classes. Normally, the precedence_3 class (without a defined ratio) would receive bandwidth based on the bandwidth-remaining ratio of the class-default class defined in the Child policy. However, in the example, the Child policy does not define a class-default bandwidth remaining ratio. Therefore, the router uses a ratio of 1 to allocate excess bandwidth to precedence_3 traffic.

```
policy-map Child
 class precedence_0
  shape average 100000
  bandwidth remaining ratio 20
 class precedence_1
  shape 10000
  bandwidth remaining ratio 30
 class precedence_2
  shape average 200000
  bandwidth remaining ratio 120
 class precedence_3
  set ip precedence 3
 class precedence_5
  set ip precedence 5
  bandwidth remaining ratio 100
policy-map Parent
 class class-default
  bandwidth remaining ratio 10
  service-policy Child
```

```
!
interface GigabitEthernet 2/0/1.10
 encapsulation dot1q 10
 service-policy output Parent
```

Examples

The following example shows how to configure overhead accounting by using the optional **account**keyword and associated keywords and arguments:

```
policy-map subscriber_line
 class class-default
  bandwidth remaining ratio 10 account dot1q aal5 snap-rbe-dot1q
  shape average 512 account dot1q
aal5 snap-rbe-dot1q
  service policy subscriber_classes
```

Related Commands

Command	Description
bandwidth remaining percent	Specifies a bandwidth-remaining percentage for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to nonpriority queues.
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.

bump

To configure the bump ing rules for a virtual circuit (VC) class that can be assigned to a VC bundle, use the **bump** command in VC-class configuration mode. To remove the explicit bumping rules for the VCs assigned to this class and return to the default condition of implicit bumping, use the **nobumpexplicit**commandor the **bumpimplicit** command. To specify that the VC bundle members do not accept any bumped traffic, use the **no**form of thiscommand.

To configure the bumping rules for a specific VC or permanent virtual circuit (PVC) member of a bundle, use the **bump** command in bundle-vc or SVC-bundle-member configuration mode. To remove the explicit bumping rules for the VC or PVC bundle member and return to the default condition of implicit bumping, use the **bumpimplicit**command. To specify that the VC or PVC bundle member does not accept any bumped traffic, use the **nobumptraffic**command.

bump {**explicit** *precedence-level*| **implicit**| **traffic**}

no bump {**explicit** *precedence-level*| **implicit**| **traffic**}

Syntax Description

explicit *precedence-level*	Specifies the precedence level to which traffic on a VC or PVC will be bumped when the VC or PVC goes down. Valid values for the *precedence-level* argument are numbers from 0 to 7.
implicit	Applies the implicit bumping rule, which is the default, to a single VC or PVC bundle member or to all VCs in the bundle (VC-class mode). The implicit bumping rule stipulates that bumped traffic is to be carried by a VC or PVC with a lower precedence level.
traffic	Specifies that the VC or PVC accepts bumped traffic (the default condition). The **no**form stipulates that the VC or PVC does not accept any bumped traffic.

Command Default

Implicit bumping

Permit bumping (VCs accept bumped traffic)

Command Modes

VC-class configuration (for a VC class) Bundle-vc configuration (for an ATM VC bundle member) SVC-bundle-member configuration (for an SVC bundle member)

Command History

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

Release	Modification
12.2(4)T	This command was made available in SVC-bundle-member configuration mode.
12.0(23)S	This command was made available in VC-class and bundle-vc configuration modes on the 8-port OC-3 STM-1 ATM line card for Cisco 12000 series Internet routers.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S and implemented on the Cisco 10000 series router.
12.2(16)BX	This command was implemented on the ESR-PRE2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **bump** command in bundle-vc configuration mode (for an ATM VC bundle member) or SVC-bundle-member configuration mode (for an SVC bundle member) to configure bumping rules for a discrete VC or PVC bundle member. Use the **bump** command in VC-class configuration mode to configure a VC class that can be assigned to a bundle member.

The effects of different bumping configuration approaches are as follows:

- Implicit bumping--If you configure implicit bumping, bumped traffic is sent to the VC or PVC configured to handle the next lower precedence level. When the original VC or PVC that bumped the traffic comes back up, the traffic that it is configured to carry is restored to it. If no other positive forms of the **bump** command are configured, the **bumpimplicit**commandtakes effect.
- Explicit bumping--If you configure a VC or PVC with the **bumpexplicit** command, you can specify the precedence level to which traffic will be bumped when that VC or PVC goes down, and the traffic will be directed to a VC or PVC mapped with that precedence level. If the VC or PVC that picks up and carries the traffic goes down, the traffic is subject to the bumping rules for that VC or PVC. You can specify only one precedence level for bumping.
- Permit bumping--The VC or PVC accepts bumped traffic by default. If the VC or PVC has been previously configured to reject bumped traffic, you must use the **bumptraffic** command to return the VC or PVC to its default condition.
- Reject bumping--To configure a discrete VC or PVC to reject bumped traffic when the traffic is directed to it, use the **nobumptraffic** command.

Note When no alternative VC or PVC can be found to handle bumped traffic, the bundle is declared down. To avoid this occurrence, configure explicitly the bundle member VC or PVC that has the lowest precedence level.

To use this command in VC-class configuration mode, you must enter the **vc-classatm** global configuration command before you enter this command.

To use this command to configure an individual bundle member in bundle-VC configuration mode, first issue the **bundle** command to enter bundle configuration mode for the bundle to which you want to add or modify the VC member to be configured. Then use the **pvc-bundle** command to specify the VC to be created or modified and enter bundle-vc configuration mode.

This command has no effect if the VC class that contains the command is attached to a standalone VC; that is, if the VC is not a bundle member. In this case, the attributes are ignored by the VC.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next-highest precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with the effect of assigned VC-class configuration)
- Subinterface configuration in subinterface mode

Examples

The following example configures the class called “five” to define parameters applicable to a VC in a bundle. If the VC goes down, traffic will be directed (bumped explicitly) to a VC mapped with precedence level 7:

```
vc-class atm five
 ubr 5000
 precedence 5
 bump explicit 7
```

The following example configures the class called “premium-class” to define parameters applicable to a VC in a bundle. Unless overridden with a bundle-vc **bump** configuration, the VC that uses this class will not allow other traffic to be bumped onto it:

```
vc-class atm premium-class
 no bump traffic
 bump explicit 7
```

Related Commands

Command	Description
bundle	Enters bundle configuration mode to create a bundle or modify an existing bundle.
class	Assigns a map class or VC class to a PVC or PVC bundle member.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.

Command	Description
dscp (frame-relay vc-bundle-member)	Specifies the DSCP value or values for a specific Frame Relay PVC bundle member.
precedence	Configures precedence levels for a VC or PVC class that can be assigned to a VC or PVC bundle and thus applied to all members of that bundle.
protect	Configures a VC or PVC class with protected group or protected VC or PVC status for application to a VC or PVC bundle member.
pvc-bundle	Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member.
pvc (frame-relay vc-bundle)	Creates a PVC and PVC bundle member and enters frame-relay vc-bundle-member configuration mode.
svc-bundle	Creates or modifies a member of an SVC bundle.
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.
vc-class atm	Configures a VC class or an ATM VC or interface.

bundle

To create a bundle or modify an existing bundle to enter bundle configuration mode, use the **bundle** command in subinterface configuration mode. To remove the specified bundle, use the **no**form of this command.

bundle *bundle-name*

no bundle *bundle-name*

Syntax Description

bundle-name	The name of the bundle to be created. The limit is 16 alphanumeric characters.

Command Default

No bundle is specified.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S and implemented on the Cisco 10000 series router.
12.2(16)BX	This command was implemented on the ESR-PRE2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

From within bundle configuration mode you can configure the characteristics and attributes of the bundle and its members, such as the encapsulation type for all virtual circuits (VCs) in the bundle, the bundle management parameters, and the service type. Attributes and parameters you configure in bundle configuration mode are applied to all VC members of the bundle.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next highest precedence):

- VC configuration in bundle-vc mode

- Bundle configuration in bundle mode
- Subinterface configuration in subinterface mode

To display status on bundles, use the **showatmbundle** and **showatmbundlestatistics**commands.

Examples

The following example shows how to configure a bundle called bundle1. The example specifies the IP address of the subinterface and the router protocol--the router uses Intermediate System-to-Intermediate System (IS-IS) as an IP routing protocol--then configures the bundle:

```
interface atm1/0.1 multipoint
 ip address 10.0.0.1 255.255.255.0
 ip router isis
 bundle bundle1
```

Related Commands

Command	Description
class-bundle	Configures a VC bundle with the bundle-level commands contained in the specified VC class.
oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for all VC members of a bundle, or for a VC class that can be applied to a VC bundle.
pvc-bundle	Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member.
show atm bundle	Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members.
show atm bundle statistics	Displays statistics on the specified bundle.

bundle svc

To create or modify a switched virtual circuit (SVC) bundle, use the **bundlesvc**command in interface configuration mode. To remove the specified bundle, use the **no**form of this command.

bundle svc *bundle-name* **nsap** *nsap-address*

no bundle svc *bundle-name* **nsap** *nsap-address*

Syntax Description

bundle-name	Unique bundle name that identifies the SVC bundle in the router. The bundle names at each end of the virtual circuit (VC) must be the same. Length limit is 16 alphanumeric characters.
nsap *nsap-address*	Destination network services access point (NSAP) address of the SVC bundle.

Command Default

No SVC bundle is created or modified.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command causes the system to enter SVC-bundle configuration mode. The bundle name must be the same on both sides of the VC.

From SVC-bundle configuration mode, you can configure the characteristics and attributes of the bundle and its members, such as the encapsulation type for all virtual circuits (VCs) in the bundle, the bundle management parameters, the service type, and so on. Attributes and parameters you configure in SVC-bundle configuration mode are applied to all VC members of the bundle.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next-highest precedence):

- VC configuration in bundle-VC mode

- Bundle configuration in bundle mode
- Subinterface configuration in subinterface mode

To display the status of bundles, use the **showatmbundlesvc** and **showatmbundlesvcstatistics**commands.

Examples

The following example shows how to configure an SVC bundle called “sanfrancisco”:

```
interface ATM1/0.1 multipoint
 ip address 10.0.0.1 255.255.255.0
 atm esi-address 111111111111.11
 bundle svc sanfrancisco nsap 47.0091810000000003E3924F01.999999999999.99
  protocol ip 10.0.0.2
broadcast
 oam retry 4 3 10
 encapsulation aal5snap
 oam-bundle manage
 svc-bundle seven
  class-vc seven
 svc-bundle six
  class-vc six
 svc-bundle five
  class-vc five
 svc-bundle four
  class-vc four
 svc-bundle three
  class-vc three
 svc-bundle two
  class-vc two
 svc-bundle one
  class-vc one
 svc-bundle zero
  class-vc zero
```

Related Commands

Command	Description
class-bundle	Configures a VC bundle with the bundle-level commands contained in the specified VC class.
oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for all VC members of a bundle, or for a VC class that can be applied to a VC bundle.
pvc-bundle	Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member.
show atm bundle svc	Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members.
show atm bundle svc statistics	Displays statistics on the specified bundle.

class (EtherSwitch)

To define a traffic classification for a policy to act on using the class-map name or access group, use the class command in policy-map configuration mode. To delete an existing class map, use the **no**form of this command.

class *class-map-name* [**access-group** *acl-index-or-name*]

no class *class-map-name*

Syntax Description

class-map-name	Name of the class map.
access-group *acl-index-or-name*	(Optional) Number or name of an IP standard or extended access control list (ACL). For an IP standard ACL, the index range is 1 to 99 and 1300 to 1999; for an IP extended ACL, the index range is 100 to 199 and 2000 to 2699.

Command Default

No policy-map class maps are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

Before you use the **class** (EtherSwitch) command, use the **policy-map** global configuration command to identify the policy map and to enter policy-map configuration mode. After you specify a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to an interface by using the **service-policy**interface configuration command; however, you cannot attach one that uses an ACL classification to the egress direction.

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

The **class** (EtherSwitch) command performs the same function as the**class-map**global configuration command. Use the **class** (EtherSwitch) command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

Note In a policy map, the class named “class-default” is not supported. The Ethernet switch network module does not filter traffic on the basis of the policy map defined by the **classclass-default** policy-map configuration command.

After entering the **class** (EtherSwitch) command, you enter policy-map class configuration mode. When you are in this mode, these configuration commands are available:

- **default** --Sets a command to its default.
- **exit** --Exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no** --Returns a command to its default setting.
- **police** --Defines a policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see the **police** command.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Note For more information about configuring IP ACLs, refer to the “Configuring IP Services” chapter in the Cisco IOS IP Application Services Configuration Guide.

Examples

The following example shows how to create a policy map named “policy1.” When attached to the ingress port, it matches all the incoming traffic defined in class1 and polices the traffic at an average rate of 1 Mbps and bursts at 131072 bytes. Traffic exceeding the profile is dropped.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police 1000000 131072 exceed-action drop
Router(config-pmap-c)# exit
```

You can verify your settings by entering the **showpolicy-map** privileged EXEC command.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
match (class-map configuration)	Defines the match criteria to classify traffic.
police	Configures traffic policing.
policy-map	Creates or modifies a policy map that can be attached to multiple 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.
show policy-map	Displays QoS policy maps.

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** [**fragment** *fragment-class-name*]} [**insert-before** *class-name*] [**service-fragment** *fragment-class-name*]

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.
fragment *f ragment-class-name*	(Optional) Specifies the default traffic class as a fragment, and names the fragment traffic class.
insert-before *class-name*	(Optional) Adds a class map between any two existing class maps. Inserting a new class map between two existing class map provides more flexibility when modifying existing policy map configurations. Without this option, the class map is appended to the end of the policy map. This keyword is supported only on flexible packet matching (FPM) policies.
service-fragment *fragment-class-name*	(Optional) Specifies that the class is classifying a collection of fragments. The fragments being classified by this class must all share the same *fragment-class-name*.

Command Default

No class is specified.

Command Modes

Policy-map configuration (config-pmap)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(14)SX	Support for this command was introduced on Cisco 7600 routers.
12.2(17d)SXB	This command was implemented on the Cisco 7600 router and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXE	The **class-default** keyword was added to the Cisco 7600 router.
12.4(4)T	The**insert-before***class-name* option was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.
12.2(18)ZY	The **insert-before***class-name* option was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 series routers. The **fragment***fragment-class-name* and *service-fragmentfragment-class-name* options were introduced.

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.

Tail Drop or WRED

You can define a class policy to use either tail drop by using the **queue-limit** command or Weighted Random Early Detection (WRED) by using the **random-detect** command. When using either tail drop or WRED, note the following points:

- The **queue-limit** and **random-detect** commands cannot be used in the same class policy, but they can be used in two class policies in the same policy map.
- You can configure the **bandwidth** command when either the **queue-limit** command or the **random-detect** command is configured in a class policy. The **bandwidth** command specifies the amount of bandwidth allocated for the class.
- For the predefined default class, you can configure the **fair-queue** (class-default) command. The **fair-queue** command specifies the number of dynamic queues for the default class. The **fair-queue** command can be used in the same class policy as either the **queue-limit** command or the **random-detect** command. It cannot be used with the **bandwidth** command.

Fragments

A default traffic class is marked as a fragment within a policy map class statement using the **fragment**keyword. Multiple fragments can then be classified collectively in a separate policy map that is created using the **service-fragment** keyword. When fragments are used, default traffic classes marked as fragments have QoS applied separately from the non-default traffic classes.

When using fragments, note the following guidelines:

- Only default traffic classes can be marked as fragments.
- The**fragment***fragment-class-name*option within a default class statement marks that default class as a fragment.
- The**service-fragment***fragment-class-name*option when defining a class in a policy map is used to specify a class of traffic within the Modular QoS CLI that contains all fragments sharing the same *fragment-class-name*.
- Fragments can only be used within the same physical interface. Policy maps with fragments sharing the same *fragment-class-name* on different interfaces cannot be classified collectively using a class with the **service-fragment***fragment-class-name* option.

Cisco 10000 Series Router

The PRE2 allows you to configure 31 class queues in a policy map.

In a policy map, the PRE3 allows you to configure one priority level 1 queue, plus one priority level 2 queue, plus 12 class queues, plus one default queue.

Cisco ASR 1000 Series Routers

The maximum number of classes that you can configure for a Cisco ASR 1000 Series Router--and, therefore, within a policy map--is 8.

Examples

The following example shows how to configure three class policies included in the policy map called policy1. Class1 specifies policy for traffic that matches access control list 136. Class2 specifies policy for traffic on interface ethernet101. The third class is the default class to which packets that do not satisfy configured match criteria are directed:

```
! The following commands create class-maps class1 and class2
! and define their match criteria:
class-map class1
 match access-group 136
class-map class2
 match input-interface ethernet101
! The following commands create the policy map, which is defined to contain policy
! specification for class1, class2, and the default class:
policy-map policy1
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect exponential-weighting-constant 10
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 16
Router(config-pmap-c)# queue-limit 20
```

- Class1--A minimum of 2000 kbps of bandwidth is expected to be delivered to this class in the event of congestion, and the queue reserved for this class can enqueue 40 packets before tail drop is enacted to handle additional packets.
- Class2--A minimum of 3000 kbps of bandwidth is expected to be delivered to this class in the event of congestion, and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop.
- The default class--16 dynamic queues are reserved for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy1, and a maximum of 20 packets per queue is enqueued before tail drop is enacted to handle additional packets.

Note When the policy map that contains these classes is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed, taking into account all class policies and Resource Reservation Protocol (RSVP), if configured.

The following example shows how to configure policy for the default class included in the policy map called policy8. The default class has these characteristics:20 dynamic queues are available for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy8, and a weight factor of 14 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop:

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

The following example shows how to configure policy for a class called acl136 included in the policy map called policy1. Class acl136 has these characteristics:a minimum of 2000 kbps of bandwidth is expected to be delivered to this class in the event of congestion, and the queue reserved for this class can enqueue 40 packets before tail drop is enacted to handle additional packets. Note that when the policy map that contains this class is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed, taking into account all class policies and RSVP, if configured:

```
Router(config)# policy-map policy1
Router(config-pmap)# class acl136
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40
```

The following example shows how to configure policy for a class called int101 included in the policy map called policy8. Class int101 has these characteristics:a minimum of 3000 kbps of bandwidth are expected to be delivered to this class in the event of congestion, and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop. Note that when the policy map that contains this class is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed:

```
Router(config)# policy-map policy8
Router(config-pmap)# class int101
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect exponential-weighting-constant 10
```

The following example shows how to configure policy for the **class-default** default class included in the policy map called policy1. The **class-default** default class has these characteristics:10 hashed queues for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy1; and a maximum of 20 packets per queue before tail drop is enacted to handle additional enqueued packets:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue
Router(config-pmap-c)# queue-limit 20
```

The following example shows how to configure policy for the **class-default** default class included in the policy map called policy8. The **class-default** default class has these characteristics:20 hashed queues for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy8; and a weight factor of 14 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop:

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header:

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
Router(config-cmap)# match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
```

```
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

The following example shows how to create a fragment class of traffic to classify the default traffic class named BestEffort. All default traffic from the policy maps named subscriber1 and subscriber2 is part of the fragment default traffic class named BestEffort. This default traffic is then shaped collectively by creating a class called data that uses the **service-fragment** keyword and the **shape** command:

Note the following about this example:

- The *class-name* for each fragment default traffic class is “BestEffort.”
- The*class-name* of “BestEffort” is also used to define the class where the**service-fragment**keyword is entered. This class applies a shaping policy to all traffic forwarded using the fragment default traffic classes named “BestEffort.”

```
policy-map subscriber1
class voice
set cos 5
priority level 1
class video
set cos 4
priority level 2
class class-default fragment BestEffort
shape average 200
bandwidth remaining ratio 10
policy-map subscriber 2
class voice
set cos 5
priority level 1
class video
set cos 4
priority level 2
class class-default fragment BestEffort
shape average 200
bandwidth remaining ratio 10
policy-map input_policy
class class-default
set dscp default
policy-map main-interface
class data service-fragment BestEffort
shape average 400
interface portchannel1.1001
encapsulation dot1q 1001service-policy output subscriber1
service-policy input input_policy
interface portchannel1.1002
encapsulation dot1q 1002
service-policy output subscriber2
service-policy input input_policy
interface gigabitethernet 0/1
description member-link1
port channel 1
service-policy output main-interface
interface gigabitethernet 0/2
```

```
description member-link2
port channel 1
```

service-policy output main-interface

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.

class-map arp-peruser

To create a class map to be used for matching Address Resolution Protocol (ARP) per-user packets, use the **class-maparp-peruse**r command in global configuration mode. To disable this functionality, use the **no** form of the command.

class-map arp-peruser

no class map arp-peruser

Syntax Description

This command has no arguments or keywords.

Command Default

No class map is configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command to create an ARP class map when configuring CoPP.

Examples

The following example shows how to create an ARP class-map:

```
Router(config)# class-map arp-peruser
Router(config-cmap)# match protocol arp
Router(config-cmap)# match subscriber access
```

Related Commands

Command	Description
match protocol arp	Matches ARP traffic to a policy map.
match subscriber access	Matches subscriber access traffic to a policy map.

class-bundle

To configure a virtual circuit (VC) bundle with the bundle-level commands contained in the specified VC class, use the **class-bundle** command in bundle or SVC-bundle configuration mode. To remove the VC class parameters from a VC bundle, use the **no** form of this command.

class-bundle *vc-class-name*

no class-bundle *vc-class-name*

Syntax Description

vc-class-name	Name of the VC class that you are assigning to your VC bundle.

Command Default

No VC class is assigned to the VC bundle.

Command Modes

Bundle configuration SVC-bundle configuration

Command History

Release	Modification
12.0T	This command was introduced, replacing the **class** command for configuring ATM VC bundles.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S and implemented on the Cisco 10000 series router.
12.2(16)BX	This command was implemented on the ESR-PRE2.
12.2(4)T	This command was made available in SVC-bundle configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To use this command, you must first enter the **bundle** or **bundlesvc**command to create the bundle and enter bundle or SVC-bundle configuration mode.

Use this command to assign a previously defined set of parameters (defined in a VC class) to an ATM VC bundle. Parameters set through bundle-level commands that are contained in a VC class are applied to the bundle and its VC members.

You can add the following commands to a VC class to be used to configure a VC bundle: **broadcast**, **encapsulation**, **inarp,oam-bundle**, **oamretry,** and **protocol**.

Bundle-level parameters applied through commands that are configured directly on a bundle supersede bundle-level parameters applied through a VC class by the **class-bundle** command. Some bundle-level parameters applied through a VC class or directly to the bundle can be superseded by commands that you directly apply to individual VCs in bundle-VC configuration mode.

Examples

In the following example, a class called “class1” is created and then applied to the bundle called “bundle1”:

```
! The following commands create the class class1:
vc-class atm class1
 encapsulation aal5snap
 broadcast
 protocol ip inarp
 oam-bundle manage 3
 oam 4 3 10
! The following commands apply class1 to the bundle called bundle1:
bundle bundle1
 class-bundle class1
```

With hierarchy precedence rules taken into account, VCs belonging to the bundle called “bundle1” will be characterized by these parameters: aal5snap, encapsulation, broadcast on, use of Inverse Address Resolution Protocol (Inverse ARP) to resolve IP addresses, and Operation, Administration, and Maintenance (OAM) enabled.

Related Commands

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

Command	Description
oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or VC bundle.
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by configuring Inverse ARP either directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).
pvc-bundle	Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member.

class-map

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

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

class-map [**type** {**stack**| **access-control**| **port-filter**| **queue-threshold**| **logging** *log-class*}] [**match-all**| **match-any**] *class-map-name*

no class-map [**type** {**stack**| **access-control**| **port-filter**| **queue-threshold**| **logging** *log-class*}] [**match-all**| **match-any**] *class-map-name*

Cisco 7600 Series Routers

class-map *class-map-name* [**match-all**| **match-any**]

no class-map *class-map-name* [**match-all**| **match-any**]

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

class-map *class-map-name*

no class-map *class-map-name*

Syntax Description

type	(Optional) Specifies the class-map type.
stack	(Optional) Enables the flexible packet matching (FPM) functionality to determine the protocol stack to examine. When you use the **load protocol** command to load protocol header description files (PHDFs) on the device, a stack of protocol headers can be defined so that the filter can determine which headers are present and in what order.
access-control	(Optional) Determines the pattern to look for in the configured protocol stack. **Note** You must specify a stack class map (by using the **type stack** keywords) before specifying an access-control class map (by using the **type access-control** keywords).
port-filter	(Optional) Creates a port-filter class map that enables the TCP or UDP port policing of control plane packets. When this keyword is enabled, the command filters the traffic that is destined to specific ports on the control-plane host subinterface.

queue-threshold	(Optional) Enables queue thresholding, which limits the total number of packets for a specified protocol allowed in the control plane IP input queue. The queue-thresholding applies only to the control-plane host subinterface.
logging *log-class*	(Optional) Enables the logging of packet traffic on the control plane. The value for the *log-class* argument is the name of the log class.
match-all	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical AND function. A packet must match all statements to be accepted. If you do not specify the **match-all** or **match-any** keyword, the default keyword used is **match-all**.
match-any	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical OR function. A packet must match any of the match statements to be accepted. If you do not specify the **match-any** or **match-all** keyword, the default keyword is used **match-all**.
class-map-name	Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map. **Note** You can enter the value for the *class-map-name* argument within quotation marks. The software does not accept spaces in a class map name entered without quotation marks.

Command Default

A class map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.

Release	Modification
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and implemented on Cisco 7600 series routers.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB and implemented on Cisco 7600 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)T	This command was modified. The **stack** and **access-control** keywords were added to support FPM. The **port-filter** and **queue-threshold** keywords were added to support control-plane protection.
12.4(6)T	This command was modified. The **logging** *log-class* keyword and argument pair was added to support control-plane packet logging.
12.2(18)ZY	This command was modified. The **stack** and **access-control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on Catalyst 6500 series switches equipped with the programmable intelligent services accelerator (PISA).
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor with the *class-map-name* argument as the only syntax element available.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor with the *class-map-name* argument.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
15.2(3)T	This command was modified. The software does not accept spaces in a class map name entered without quotation marks.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

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

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

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

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

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

Cisco 7600 Series Routers

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 1: match command Syntax Description

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

Examples

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

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

The following example shows how to define FPM traffic classes for slammer and UDP packets. The match criteria defined within class maps are for slammer and UDP packets with an IP length that does not exceed 404 (0x194) bytes, UDP port 1434 (0x59A), and pattern 0x4011010 at 224 bytes from the start of the IP header.

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

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

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

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

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

Examples

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

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

Examples

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

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

Related Commands

Command	Description
description	Specifies the description for a class map or policy map configuration.
drop	Configures the traffic class to discard packets belonging to a specific class map.
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class before you configure its policy.
load protocol	Loads a PHDF onto a router.
match (class-map)	Configures the match criteria for a class map on the basis of port filter or protocol queue policies.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.

Command	Description
match ip dscp	Identifies one or more DSCP, AF, and CS value as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
protocol	Configures a timer and authentication method for a control interface.
qos-group	Associates a QoS group value for a class map.
service-policy	Attaches a policy map to an input interface or VC or to an output interface or VC to be used as the service policy for that interface or VC.
show class-map	Displays class map information.
show policy-map interface	Displays statistics and configurations of input and output policies that are attached to an interface.
source-address	Configures the source-address control on a port.

class-map arp-peruser

To create a class map to be used for matching Address Resolution Protocol (ARP) per-user packets, use the **class-maparp-peruse**r command in global configuration mode. To disable, use the **no** form of the command.

class-map arp-peruser

no class map arp-peruser

Syntax Description

arp per-user	Specifies Address Resolution Protocol per user.

Command Default

Enabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command to create an ARP class map when configuring CoPP.

Examples

The following example shows creating an ARP class-map:

```
Router(config)#class-map arp-peruser
Router(config-cmap)#match protocol arp
Router(config-cmap)#match subscriber access
```

Related Commands

Command	Description
match protocol arp	Matches ARP traffic to a policy map.
match subscriber access	Matches subscriber access traffic to a policy map.

class type tag

To associate a class map with a policy map, use the **classtypetag**command in policy map configuration mode. To disassociate the command, use the **no** form of this command.

class type tag *class-name* [**insert-before** *class-name*]

no class type tag *class-name* [**insert-before** *class-name*]

Syntax Description

class-name	Name of the class map.
insert-before *class-name*	(Optional) Adds a class map between any two existing class maps. **Note** Inserting a new class map between two existing class maps provides more flexibility when modifying existing policy map configurations. Without this option, the class map is appended to the end of the policy map.

Command Default

A class map is not associated with a policy map.

Command Modes

Policy map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If this command is used and the class is not configured, an error is generated. The error may be something such as "% class map {*name* } not configured." If the class needs to be inserted before a specific class map, the **insert-before** keyword can be used. The **insert-before** keyword is typically needed if the administrator is configuring any per-host class maps and would like it inserted before a specific class map. The **classtypetag** command creates the policy-map class configuration mode. There can be multiple classes under the policy map.

Examples

The following example shows how to associate the class map "usergroup1_class" with a policy map:

```
class type tag usergroup1_class
```

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.

clear control-plane

To clear counters for control-plane interfaces or subinterfaces, use the **clearcontrol-plane** command in privileged EXEC mode.

clear control-plane [***| aggregate| host| transit| cef-exception**]

Syntax Description

*****	(Optional) Clears counters for all control-plane features.
aggregate	(Optional) Clears counters for all features on the control-plane aggregate path.
host	(Optional) Clears counters for all features on the control-plane host feature path.
transit	(Optional) Clears counters for all features on the control-plane transit feature path.
cef-exception	(Optional) Clears counters for all features on the control-plane CEF-exception feature path.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use the **clearcontrol-plane** command to clear counters for all features on the control-plane interfaces or subinterfaces.

Examples

The following example clears the counters for all features on the control-plane host feature path.

```
Router# clear control-plane host
```

Related Commands

Command	Description
control-plane	Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control plane of the device.
debug control-plane	Displays debugging output from the control-plane routines.
show control-plane cef-exception counters	Displays the control plane packet counters for the control-plane CEF-exception subinterface.
show control-plane cef-exception features	Displays the configured features for the control-plane CEF-exception subinterface.
show control-plane counters	Displays the control-plane packet counters for the aggregate control-plane interface.
show control-plane features	Displays the configured features for the aggregate control-plane interface.
show control-plane host counters	Displays the control-plane packet counters for the control-plane host subinterface.
show control-plane host features	Displays the configured features for the control-plane host subinterface.
show control-plane host open-ports	Displays a list of open TCP/UDP ports that are registered with the port-filter database.
show control-plane transit counters	Displays the control-plane packet counters for the control-plane transit subinterface.
show control-plane transit features	Displays the configured features for the control-plane transit subinterface.

clear ip nbar

To clear buffers, filters, and port statistics gathered by Network-Based Application Recognition (NBAR), use the **clear ip nbar** command in privileged EXEC mode.

clear ip nbar [**capture**| **filter**| **trace**{**detail**| **summary**}| **statistics**| **unclassified-port-stats**]

Syntax Description

capture	(Optional) Specifies the packet capture buffers.
filter	(Optional) Specifies the session selection filter.
trace	(Optional) Specifies state-graph tracing buffers.
detail	(Optional) Specifies detailed classification information of NBAR.
summary	(Optional) Specifies classification summary of NBAR.
unclassified-port-stats	(Optional) Specifies the port statistics for unclassified packets.
statistics	(Optional) Specifies NBAR statistics for packets.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.2(4)M	This command was modified. The **statistics**, **trace**, and **detail** keywords were added.

Examples

The following example shows how to clear the port statistics gathered by NBAR:

```
Device# clear ip nbar unclassified-port-stats
```

The following example shows how to clear the statistics gathered by NBAR:

```
Device# clear ip nbar statistics
```

Related Commands

Command	Description
clear ip nbar protocol-discovery	Clears statistics gathered by the NBAR protocol discovery.
show ip nbar statistics	Displays statistics gathered by NBAR.

clear ip nbar protocol-discovery

To clear the statistics gathered by the network-based application recognition (NBAR) Protocol Discovery feature, use the **clearipnbarprotocol-discovery** command in privileged EXEC mode.

clear ip nbar protocol-discovery [**interface** *type number*]

Syntax Description

interface	(Optional) Specifies the type of interface to be configured.
type	(Optional) Type of interface.
number	(Optional) Interface or subinterface number.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **clearipnbarprotocol-discovery** command to clear the statistics gathered by the NBAR Protocol Discovery feature. By default, this command clears the statistics for all the interfaces on which the protocol discovery feature is enabled.

Examples

The following example shows how to clear the statistics gathered by the NBAR Protocol Discovery feature:

```
Router# clear ip nbar protocol-discovery interface serial 3/1
```

Related Commands

Command	Description
clear ip nbar	Clears the buffers, filters, and port statistics gathered by the NBAR feature.

clear ip rsvp authentication

To eliminate Resource Reservation Protocol (RSVP) security associations before their lifetimes expire, use the clear **iprsvpauthentication**command in privileged EXEC mode.

clear ip rsvp authentication [*ip-address*| *hostname*]

Syntax Description

ip-address	(Optional) Frees security associations with a specific neighbor.
hostname	(Optional) Frees security associations with a specific host.

Note The difference between the*ip-address* and*hostname* arguments is the difference of specifying the neighbor by its IP address or by its name.

Command Default

The default behavior is to clear all security associations.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the clear **iprsvpauthentication** command for the following reasons:

- To eliminate security associations before their lifetimes expire
- To free up memory
- To resolve a problem with a security association being in some indeterminate state
- To force reauthentication of neighbors

You can delete all RSVP security associations if you do not enter an IP address or a hostname, or just the ones with a specific RSVP neighbor or host.

If you delete a security association, it is re-created as needed when the trusted RSVP neighbors start sending more RSVP messages.

Examples

The following command shows how to clear all security associations before they expire:

```
Router# clear ip rsvp authentication
```

Related Commands

Command	Description
ip rsvp authentication lifetime	Controls how long RSVP maintains security associations with other trusted RSVP neighbors.
show ip rsvp authentication	Displays the security associations that RSVP has established with other RSVP neighbors.

clear ip rsvp counters

To clear (set to zero) all IP Resource Reservation Protocol (RSVP) counters that are being maintained, use the **cleariprsvpcounters**command in privileged EXEC mode.

clear ip rsvp counters [confirm]

Syntax Description

confirm	(Optional) Requests a confirmation that all IP RSVP counters were cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command allows you to set all IP RSVP counters to zero so that you can see changes easily.

Examples

In the following example, all IP RSVP counters that are being maintained are cleared:

```
Router# clear ip rsvp counters
Clear rsvp counters [confirm]
```

Related Commands

Command	Description
show ip rsvp counters	Displays counts of RSVP messages that were sent and received.

clear ip rsvp hello instance counters

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

clear ip rsvp hello instance counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

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

```
Router# show ip rsvp hello instance detail
Neighbor 10.0.0.2  Source  10.0.0.1
 State: UP      (for 2d18h)
 Type: PASSIVE  (responding to requests)
 I/F: Et1/1
 LSPs protecting: 0
 Refresh Interval (msec) (used when ACTIVE)
  Configured: 100
  Statistics: (from 2398195 samples)
   Min:      100
   Max:      132
   Average:  100
   Waverage: 100 (Weight = 0.8)
   Current:  100
 Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
 Counters:
 Communication with neighbor lost:
  Num times: 0
  Reasons:
   Missed acks:             0
   Bad Src_Inst received:   0
   Bad Dst_Inst received:   0
   I/F went down:           0
   Neighbor disabled Hello: 0
  Msgs Received:   2398194
   Sent:       2398195
   Suppressed: 0
Router# clear ip rsvp hello instance counters
Neighbor 10.0.0.2  Source  10.0.0.1
 State: UP      (for 2d18h)
 Type: PASSIVE  (responding to requests)
 I/F: Et1/1
 LSPs protecting: 0
 Refresh Interval (msec) (used when ACTIVE)
  Configured: 100
  Statistics:
   Min:        0
   Max:        0
   Average:    0
   Waverage:   0
   Current:    0
 Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
 Counters:
  Communication with neighbor lost:
  Num times: 0
  Reasons:
   Missed acks:             0
   Bad Src_Inst received:   0
   Bad Dst_Inst received:   0
   I/F went down:           0
   Neighbor disabled Hello: 0
  Msgs Received:   2398194
   Sent:       2398195
   Suppressed: 0
```

Related Commands

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

clear ip rsvp hello instance statistics

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

clear ip rsvp hello instance statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Hello statistics are not cleared for an instance.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

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

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


Router# clear ip rsvp hello instance statistics
Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
```

```
    Weighted Average:0 (weight = 0.8)
    Max:0
  Current length: 0 (max:500)
Number of samples taken: 0
```

Related Commands

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

clear ip rsvp hello statistics

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

clear ip rsvp hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Hello statistics are not globally cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2s	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

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

Examples

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

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

```
    Weighted Average:0 (weight = 0.8)
    Max:0
  Current length: 0 (max:500)
Number of samples taken: 16
```

Related Commands

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

clear ip rsvp high-availability counters

To clear (set to zero) the Resource Reservation Protocol (RSVP) traffic engineering (TE) high availability (HA) counters that are being maintained by a Route Processor (RP), use the **clear ip rsvp high-availability counters** command in privileged EXEC mode.

clear ip rsvp high-availability counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.2(33)SRB	Support for In-Service Software Upgrade (ISSU) was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **clear ip rsvp high-availability counters**command to clear (set to zero) the HA counters, which include state, ISSU, resource failures, and historical information.

Examples

The following example clears all the HA information currently being maintained by the RP:

```
Router# clear ip rsvp high-availability counters
```

Related Commands

Command	Description
show ip rsvp high-availability counters	Displays the RSVP TE HA counters that are being maintained by an RP.

clear ip rsvp msg-pacing

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

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

clear ip rsvp msg-pacing

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(13)T	This command was replaced by the**cleariprsvpsignallingrate-limit** command.
12.4(20)T	This command was removed.

Examples

The following example clears the RSVP message pacing output:

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

Related Commands

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

clear ip rsvp reservation

To remove Resource Reservation Protocol (RSVP) RESV-related receiver information currently in the database, use the **cleariprsvpreservation**command in EXEC mode.

clear ip rsvp reservation {*session-ip-address sender-ip-address* {**tcp**| **udp**| *ip-protocol*} *session-dport sender-sport*| *****}

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
sender-ip-address	The IP address of the sender.
tcp | **udp** | *ip-protocol*	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 65535.
session-dport	The destination port. **Note** Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero).
sender-sport	The source port. **Note** Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero).
*	Wildcard used to clear all senders.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **cleariprsvpreservation**command to remove the RESV-related sender information currently in the database so that when reservation requests arrive, based on the RSVP admission policy, the relevant ones can be reestablished.

Whenever you change the clockrate or bandwidth of an interface, RSVP does not update its database to reflect the change. This is because such a change requires that RSVP reestablish reservations based on the new clockrate or bandwidth value and arbitrarily dropping some reservations while retaining others is not desired. The solution is to clear the RESV state by issuing the **cleariprsvpreservation**command.

The **cleariprsvpreservation**command clears the RESV state from the router on which you issued the command and causes the router to send a PATH TEAR message to the upstream routers thereby clearing the RESV state for that reservation on all the upstream routers.

Examples

The following example clears all the RESV-related receiver information currently in the database:

```
Router# clear ip rsvp reservation *
```

The following example clears all the RESV-related receiver information for a specified reservation currently in the database:

```
Router# clear ip rsvp reservation 10.2.1.1 10.1.1.2 udp 10 20
```

Related Commands

Command	Description
clear ip rsvp sender	Removes RSVP PATH-related sender information currently in the database.

clear ip rsvp sender

To remove Resource Reservation Protocol (RSVP) PATH-related sender information currently in the database, use the **cleariprsvpsender**command in EXEC mode.

clear ip rsvp sender {*session-ip-address sender-ip-address* {**tcp**| **udp**| *ip-protocol*} *session-dport sender-sport*| *****}

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
sender-ip-address	The IP address of the sender.
tcp | **udp** | *ip-protocol*	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 65535.
session-dport	The destination port. **Note** Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero).
sender-sport	The source port. **Note** Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero).
*	Wildcard used to clear all senders.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **cleariprsvpsender** command to remove the PATH-related sender information currently in the database so that when reservation requests arrive, based on the RSVP admission policy, the relevant ones can be reestablished.

Whenever you change the clockrate or bandwidth of an interface, RSVP does not update its database to reflect the change. This is because such a change requires that RSVP reestablish reservations based on the new clockrate or bandwidth value and arbitrarily dropping some reservations while retaining others is not desired. The solution is to clear the PATH state by issuing the **cleariprsvpsender** command.

The **cleariprsvpsender** command clears the PATH state from the router on which you issued the command and causes the router to send a PATH TEAR message to the downstream routers thereby clearing the PATH state for that reservation on all the downstream routers.

Examples

The following example clears all the PATH-related sender information currently in the database:

```
Router# clear ip rsvp sender *
```

The following example clears all the PATH-related sender information for a specified reservation currently in the database:

```
Router# clear ip rsvp sender 10.2.1.1 10.1.1.2 udp 10 20
```

Related Commands

Command	Description
clear ip rsvp reservation	Removes RSVP RESV-related receiver information currently in the database.

clear ip rsvp signalling fast-local-repair statistics

To clear (set to zero) the Resource Reservation Protocol (RSVP) fast local repair (FLR) counters, use the **cleariprsvpsignallingfast-local-repairstatistics** command in user EXEC or privileged EXEC mode.

clear ip rsvp signalling fast-local-repair statistics

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to clear all the RSVP FLR counters.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use the **cleariprsvpsignallingfast-local-repairstatistics**command to set all the RSVP FLR counters to zero. The statistics include information about FLR procedures such as the current state, the start time, and the repair rate.

Examples

The following example clears all the RSVP FLR counters being maintained in the database:

```
Router# clear ip rsvp signalling fast-local-repair statistics
```

Related Commands

Command	Description
show ip rsvp signalling fast-local-repair	Displays FLR-related information.

clear ip rsvp signalling rate-limit

To clear (set to zero) the number of Resource Reservation Protocol (RSVP) messages that were dropped because of a full queue, use the **cleariprsvpsignallingrate-limit** command in privileged EXEC mode.

clear ip rsvp signalling rate-limit

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **cleariprsvpmsg-pacing** command.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **cleariprsvpsignallingrate-limit** command to clear the counters recording dropped messages.

Examples

The following command shows how to clear all dropped messages:

```
Router# clear ip rsvp signalling rate-limit
```

Related Commands

Command	Description
debug ip rsvp rate-limit	Displays debug messages for RSVP rate-limiting events.
ip rsvp signalling rate-limit	Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time.
show ip rsvp signalling rate-limit	Displays rate-limiting parameters for RSVP messages.

clear ip rsvp signalling refresh reduction

To clear (set to zero) the counters associated with the number of retransmissions and the number of out-of-order Resource Reservation Protocol (RSVP) messages, use the **cleariprsvpsignallingrefreshreduction** command in EXEC mode.

clear ip rsvp signalling refresh reduction

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

Use the **cleariprsvpsignallingrefreshreduction**command to clear the counters recording retransmissions and out-of-order RSVP messages.

Examples

The following command shows how all the retransmissions and out-of-order messages are cleared:

```
Router# clear ip rsvp signalling refresh reduction
```

Related Commands

Command	Description
ip rsvp signalling refresh reduction	Enables refresh reduction.
show ip rsvp signalling refresh reduction	Displays refresh-reduction parameters for RSVP messages.

clear mls qos

To clear the multilayer switching (MLS) aggregate-quality of service (QoS) statistics, use the **clearmlsqos** command in privileged EXEC mode.

clear mls qos [**ip**| **ipx**| **mac**| **mpls**| **ipv6**| **arp** [*interface-type interface-number*| **null** *interface-number*| **port-channel** *number*| **vlan** *vlan-id*]]

Syntax Description

ip	(Optional) Clears MLS IP aggregate-QoS statistics.
ipx	(Optional) Clears MLS IPX aggregate-QoS statistics.
mac	(Optional) Clears MLS MAC aggregate-QoS statistics.
mpls	(Optional) Clears MLS MPLS aggregate-QoS statistics.
ipv6	(Optional) Clears MLS IPv6 aggregate QoS statistics.
arp	(Optional) Clears MLS ARP aggregate QoS statistics.
interface-type	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**. See the “Usage Guidelines” section for additional valid values.
interface-number	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
null *interface-number*	(Optional) Specifies the null interface; the valid value is 0 .
port-channel *number*	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 2.
12.2(17a)SX	This command was changed to include the **mpls** keyword .
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	This command was changed to include the **arp** keywor d.
12.2(18)SXE	This command was changed to include the **ipv6**and **arp** k eywor ds on the Supervisor Engine 2 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The valid values for *interface-type* include th e **ge-wan**, **atm**, and **pos** keywords that are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **ipx** keyword is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

The **ipv6** and **arp** keywo r ds are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

If you enter the **clearmlsqos** command with no arguments, the global and per-interface aggregate QoS counters for all protocols are cleared.

If you do not enter an interface type, the protocol aggregate-QoS counters for all interfaces are cleared.

Note Entering the **clearmlsqos** command affects the policing token bucket counters and might briefly allow traffic to be forwarded that would otherwise be policed.

Examples

This example shows how to clear the global and per-interface aggregate-QoS counters for all protocols:

```
Router# clear mls qos
```

This example shows how to clear the specific protocol aggregate-QoS counters for all interfaces:

```
Ro
uter# clear mls qos ip
```

Related Commands

Command	Description
show mls qos	Displays MLS QoS information.

clear service-group traffic-stats

To clear the traffic statistics for one or all service groups, use the **clearservice-grouptraffic-stats**command in privileged EXEC mode.

clear service-group traffic-stats [**group** *service-group-identifier*]

Syntax Description

group	(Optional) Service group.
service-group-identifier	(Optional) Service group number. Enter the number of the service group for which you want to clear statistics.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

If a service group number is not specified, statistics for all service groups are cleared.

Note Clearing the traffic statistics for the service group does not clear the traffic statistics for the group members. To clear the traffic statistics for the group members, use the **clearethernetserviceinstance** command. For more information about the **clearethernetserviceinstance**command, see the *Cisco IOS Carrier Ethernet Command Reference*.

Examples

The following shows how to clear the traffic statistics for all service groups:

```
Router> enable
Router# clear service-group traffic-stats
```

Related Commands

Command	Description
clear ethernet service instance	Clears Ethernet service instance attributes such as MAC addresses and statistics or purges Ethernet service instance errors.

compression header ip

To configure Real-Time Transport Protocol (RTP) or TCP IP header compression for a specific class, use the **compressionheaderip** command in policy-map class configuration mode. To remove RTP or TCP IP header compression for a specific class, use the **no** form of this command.

compression header ip [**rtp**| **tcp**]

no compression header ip

Syntax Description

rtp	(Optional) Configures RTP header compression.
tcp	(Optional) Configures TCP header compression.

Command Default

If you do not specify either RTP or TCP header compression (that is, you press the enter key after the command name) both RTP and TCP header compressions are configured. This is intended to cover the "all compressions" scenario.

Command Modes

Policy-map class configuration

Command History

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

Usage Guidelines

Using any form of the **compressionheaderip**commandoverrides any previously entered form.

The **compressionheaderip**commandcan be used at any level in the policy map hierarchy configured with the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) feature.

Examples

In the following example, the **compressionheaderip** command has been configured to use RTP header compression for a class called "class1". Class1 is part of policy map called "policy1".

```
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# compression header ip rtp
Router(config-pmap-c)# end
```

Related Commands

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 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.

control-plane

To enter control-plane configuration mode, which allows users to associate or modify attributes or parameters (such as a service policy) that are associated with the control plane of the device, use the **control-plane**command in global configuration mode. To remove an existing control-plane configuration from the router, use the **no**form of this command.

Syntax for T Releases

control-plane [**host**| **transit**| **cef-exception**]

no control-plane [**host**| **transit**| **cef-exception**]

Syntax for 12.0S Releases

control-plane [**slot** *slot-number*] [**host**| **transit**| **cef-exception**]

no control-plane [**slot** *slot-number*] [**host**| **transit**| **cef-exception**]

Syntax for 12.2S Releases for Cisco 7600 Series Routers

control-plane

no control-plane

Syntax for ASR 1000 Series Routers

control-plane [host]

no control-plane [host]

Syntax Description

host	(Optional) Applies policies to host control-plane traffic.
transit	(Optional) Applies policies to transit control-plane traffic.
cef-exception	(Optional) Applies policies to CEF-exception control-plane traffic.
slot *slot-number*	(Optional) Specifies the slot number for the line card to which you want to attach a QoS policy to configure distributed Control-Plane (CP) services.

Command Default

No control-plane service policies are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(29)S	This command was integrated into Cisco IOS Release 12.0(29)S.
12.0(30)S	The **slot**_slot-number_ parameter was added to configure distributed Control-Plane (CP) services.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.4(4)T	The **host**,**transit**, and **cef-exception**keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.2	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

After you enter the **control-plane** command, you can apply a control-plane policing (CoPP), port-filter, or queue-threshold policy to police traffic destined for the control plane. You can define aggregate CoPPs for the route processor (RP) and configure a service policy to police all traffic destined to the control plane:

- From all line cards on the router (aggregate CP services)
- From all interfaces on a line card (distributed CP services)

Aggregate CP services manage traffic destined for the control plane and received on the central switch engine from all line cards in the router.

Distributed CP services manage CP traffic from interfaces on a specified line card before CP packets are forwarded to the central switch engine where aggregate CP services are applied.

Note On the Cisco 12000 series Internet router, you can combine distributed and aggregate CP services to protect the control plane from DoS attacks and provide packet QoS. The **slot**_slot-number_ parameter is used only for distributed CP services configurations.

Control-plane policing includes enhanced control-plane functionality. It provides a mechanism for early dropping of packets directed toward closed or nonlistened Cisco IOS TCP/UPD ports on the router. It also provides the ability to limit protocol queue usage such that no single misbehaving protocol process can wedge the control-plane interface hold queue.

Note The **control-plane**command is supported by Cisco IOS Release 12.2S only for the Cisco 7600 router. For other Cisco IOS releases, the Cisco 7600 supports only the **nocontrol-plane** command to discontinue a previously existing configuration condition.

With this enhancement, you can classify control-plane traffic into different categories of traffic. These categories are as follows:

- Control-plane host subinterface--Subinterface that receives all control-plane IP traffic that is directly destined for one of the router interfaces. Examples of control-plane host IP traffic include tunnel termination traffic, management traffic, or routing protocols such as SSH, SNMP, BGP, OSPF, and EIGRP. All host traffic terminates on and is processed by the router. Most control-plane protection features and policies operate strictly on the control-plane host subinterface. Since most critical router control-plane services, such as routing protocols and management traffic, are received on the control-plane host subinterface, it is critical to protect this traffic through policing and protection policies. CoPP, port-filtering, and per-protocol queue thresholding protection features can be applied on the control-plane host subinterface.
- Control-plane transit subinterface--Subinterface that receives all control-plane IP traffic that is software switched by the route processor. This means packets not directly destined to the router itself but rather traffic traversing through the router. Nonterminating tunnels handled by the router are an example of this type of control-plane traffic. Control-plane protection allows specific aggregate policing of all traffic received at this subinterface.
- Control-plane CEF-exception subinterface--Subinterface that receives all traffic that is either redirected as a result of a configured input feature in the CEF packet forwarding path for process switching or directly enqueued in the control-plane input queue by the interface driver (for example, ARP, L2 keepalives, and all non-IP host traffic). Control-plane protection allows specific aggregate policing of this specific type of control-plane traffic.

Examples

The following example shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate. The QoS policy is then applied for aggregate CP services to all packets that are entering the control plane from all line cards in the router.

```
! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class map “telnet-class.”
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-in
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control-plane service for the active route processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# end
```

The next example also shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets that enter through slot 1 to be policed at the specified rate. The QoS policy is applied for distributed CP services to all packets that enter through the interfaces on the line card in slot 1 and that are destined for the control plane:

```
! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class map "telnet-class."
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-in
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control-plane service for the active route processor.
Router(config)# control-plane slot 1
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# end
```

The following example shows how to apply an aggregate CoPP policy to the host control-plane traffic by applying it to the host control-plane feature path:

```
Router(config)# control-plane host
Router(config-cp)# service-policy input cpp-policy-host
```

The following example shows how to apply an aggregate CoPP policy to the transit control-plane traffic by applying it to the control-plane transit feature path:

```
Router(config)# control-plane transit
Router(config-cp)# service-policy input cpp-policy-transit
```

The following example shows how to apply an aggregate CoPP policy to the CEF-exception control-plane traffic by applying it to the control-plane CEF-exception feature path:

```
Router(config)# control-plane cef-exception
Router(config-cp)# service-policy input cpp-policy-cef-exception
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.
class-map	Accesses the QoS class-map configuration mode to configure QoS class maps.
drop	Configures a traffic class to discard packets that belonging to a specific class.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.

Command	Description
policy-map	Accesses QoS policy-map configuration mode to configure the QoS policy map.
service-policy (control-plane)	Attaches a policy map to the control plane for aggregate or distributed control-plane services.
show policy-map control-plane	Displays the configuration of a class or all classes for the policy map attached to the control plane.

copy interface

To configure a traffic class to copy packets belonging to a specific class to the interface that is specified in the command, use the **copyinterface** command in policy-map class configuration mode. To prevent the packets from getting copied, use the **no** form of the command.

copy interface *interface type number*

no copy interface *interface type number*

Syntax Description

interface type number	Type and number of the interace to which the packets need to be sent.

Command Default

If this command is not specified, the packets are not copied to an interface.

Command Modes

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

Command History

Release	Modification
12.2(18)ZYA1	This command was introduced.

Usage Guidelines

Use this command to copy packets to a predefined interface. The original packet goes to the predefined destination and the copied packet goes to the target interface. You can also configure the **copyinterface** command with the**log** command but not with a **drop** or **redirectinterface**command. This command cannot be configured with a service policy for a stack class. The packets can be copied only to the following interfaces:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- Ten Gigabit Ethernet

Examples

In the following example, a traffic class called cmtest has been created and configured for use in a policy map called pmtest. The policy map (service policy) is attached to FastEthernet interface 4/18. All packets in the cmtest class are copied to FastEthernet interface 4/15.

```
Router(config)# policy-map type access-control pmtest
Router(config-pmap)# class cmtest
Router(config-pmap-c)# copy interface FastEthernet 4/15
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
Router(config)# interface FastEthernet 4/18
Router(config-if)#
service-policy input pmtest
```

Related Commands

Command	Description
log	Generates a log of messages in the policy-map class configuration mode or class-map configuration mode.
show class-map	Displays all class maps and their matching criteria.
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.

custom-queue-list

Note Effective with Cisco IOS XE Release 2.6 and Cisco IOS Release 15.1(3)T, the **custom-queue-list** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **custom-queue-list**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To assign a custom queue list to an interface, use the**custom-queue-list** command in interface configuration mode. To remove a specific list or all list assignments, use the **no** form of this command.

custom-queue-list [*list-number*]

no custom-queue-list [*list-number*]

Syntax Description

list-number	Any number from 1 to 16 for the custom queue list.

Command Default

No custom queue list is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.

Release	Modification
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

Only one queue list can be assigned per interface. Use this command in place of the **priority-listinterface**command (not in addition to it). Custom queueing allows a fairness not provided with priority queueing. With custom queueing, you can control the bandwidth available on the interface when the interface is unable to accommodate the aggregate traffic enqueued. Associated with each output queue is a configurable byte count, which specifies how many bytes of data should be delivered from the current queue by the system before the system moves on to the next queue. When a particular queue is being processed, packets are sent until the number of bytes sent exceeds the queue byte count or until the queue is empty.

Use the**showqueueingcustom**and**showinterfaces** commands to display the current status of the custom output queues.

Examples

In the following example, custom queue list number 3 is assigned to serial interface 0:

```
interface serial 0
 custom-queue-list 3
```

Related Commands

Command	Description
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
queue-list default	Assigns a priority queue for those packets that do not match any other rule in the queue list.
queue-list interface	Establishes queueing priorities on packets entering on an interface.
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.
queue-list queue limit	Designates the queue length limit for a queue.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.