QoS Commands

- class, on page 2
- class-map, on page 4
- match (class-map configuration), on page 6
- policy-map, on page 9
- priority, on page 11
- queue-buffers ratio, on page 13
- queue-limit, on page 14
- random-detect cos, on page 16
- random-detect cos-based, on page 17
- random-detect dscp, on page 18
- random-detect dscp-based, on page 20
- random-detect precedence, on page 21
- random-detect precedence-based, on page 23
- service-policy (Wired), on page 24
- set, on page 26
- show class-map, on page 32
- show platform hardware fed switch, on page 33
- show platform software fed switch qos, on page 36
- show platform software fed switch qos qsb, on page 37
- show policy-map, on page 40
- show tech-support qos, on page 42
- trust device, on page 44

class

To define a traffic classification match criteria for the specified class-map name, use the **class** command in policy-map configuration mode. Use the **no** form of this command to delete an existing class map.

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

Syntax Description

class-map-name	The class map name.
class-default	Refers to a system default class that matches unclassified packets.

Command Default

No policy map class-maps are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and enter policy-map configuration mode. After specifying 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 a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter the policy-map class configuration mode. These configuration commands are available:

- **admit**—Admits a request for Call Admission Control (CAC)
- **bandwidth**—Specifies the bandwidth allocated to the class.
- **exit**—Exits the policy-map class configuration mode and returns to policy-map configuration mode.
- **no**—Returns a command to its default setting.
- **police**—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.
- **priority**—Assigns scheduling priority to a class of traffic belonging to a policy map.
- **queue-buffers**—Configures the queue buffer for the class.
- **queue-limit**—Specifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
- **service-policy**—Configures a QoS service policy.
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see the *set* command.
- **shape**—Specifies average or peak rate traffic shaping. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.

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

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** 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.

You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

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

Examples

This example shows how to create a policy map called policy1. When attached to the ingress direction, it matches all the incoming traffic defined in class1 and polices the traffic at an average rate of 1 Mb/s and bursts at 1000 bytes, marking down exceeding traffic via a table-map.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police cir 1000000 bc 1000 conform-action
transmit exceed-action set-dscp-transmit dscp table EXEC_TABLE
Device(config-pmap-c)# exit
```

This example shows how to configure a default traffic class to a policy map. It also shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit

Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit

Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-4
Device(config-pmap-c)# set precedence 5
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
  Class class-default
    set dscp af11
```

class-map

To create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode, use the **class-map** command in global configuration mode. Use the **no** form of this command to delete an existing class map and to return to global or policy map configuration mode.

class-map *class-map name* {**match-any** | **match-all**}
no class-map *class-map name* {**match-any** | **match-all**}

Syntax Description

match-any	(Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria must be matched.
match-all	(Optional) Performs a logical-AND of the matching statements under this class map. All criterias must match.
class-map-name	The class map name.

Command Default

No class maps are defined.

Command Modes

Global configuration

Policy map configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description**—Describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit**—Exits from QoS class-map configuration mode.
- **match**—Configures classification criteria.
- **no**—Removes a match statement from a class map.

If you enter the **match-any** keyword, you can only use it to specify an extended named access control list (ACL) with the **match access-group** class-map configuration command.

To define packet classification on a physical-port basis, only one **match** command per class map is supported.

The ACL can have multiple access control entries (ACEs).

Note You cannot configure IPv4 and IPv6 classification criteria simultaneously in the same class-map. However, they can be configured in different class-maps in the same policy.

Examples

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Device(config)# no class-map class1
```

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

match (class-map configuration)

To define the match criteria to classify traffic, use the **match** command in class-map configuration mode. Use the **no** form of this command to remove the match criteria.

Cisco IOS XE Everest 16.5.x and Earlier Releases

match {**access-group** {**name***acl-name acl-index*} | **class-map** *class-map-name* | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **precedence** *precedence-value1...value4* | **qos-group** *qos-group-value* | **vlan** *vlan-id*}
no match {**access-group** {**name***acl-name acl-index*} | **class-map** *class-map-name* | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **precedence** *precedence-value1...value4* | **qos-group** *qos-group-value* | **vlan** *vlan-id*}

Cisco IOS XE Everest 16.6.x and Later Releases

match {**access-group** {**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}
no match {**access-group** {**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}

Syntax Description

access-group	Specifies an access group.
name *acl-name*	Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL.
acl-index	Specifies the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
class-map *class-map-name*	Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion.
cos *cos-value*	Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one **match cos** statement, separated by a space.
dscp *dscp-value*	Specifies the parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value.

ip dscp *dscp-list*	Specifies a list of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
ip precedence *ip-precedence-list*	Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
precedence *precedence-value1...value4*	Assigns an IP precedence value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
qos-group *qos-group-value*	Identifies a specific QoS group value as a match criterion. The range is 0 to 31.
vlan *vlan-id*	Identifies a specific VLAN as a match criterion. The range is 1 to 4094.
non-client-nrt	Matches a non-client NRT (non-real-time).
protocol *protocol-name*	Specifies the type of protocol.
wlan *wlan-id*	Identifies 802.11 specific values.

Command Default

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introc

Usage Guidelines

The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching to the Ether Type/Len are supported.

If you enter the **class-map match-any***class-map-name* global configuration command, you can enter the following **match** commands:

- **match access-group name** *acl-name*

Note The ACL must be an extended named ACL.

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

The **match access-group** *acl-index* command is not supported.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-any** keyword is equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

Use the **input-interface** *interface-id-list* keyword when you are configuring an interface-level class map in a hierarchical policy map. For the *interface-id-list*, you can specify up to six entries.

Examples

This example shows how to create a class map called class2, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(config-cmap)# exit
```

This example shows how to create a class map called class3, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

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

policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

policy-map *policy-map-name*
no policy-map *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map.

Command Default

No policy maps are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface.

Note Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Deviceconfig-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

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

priority

To assign priority to a class of traffic belonging to a policy map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

priority [*Kbps* [*burst -in-bytes*] | **level** *level-value* [*Kbps* [*burst -in-bytes*]] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*]]]
no priority [*Kb/s* [*burst -in-bytes*] | **level** *level value* [*Kb/s* [*burst -in-bytes*]] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*]]]

Syntax Description

Kb/s	(Optional) Guaranteed allowed bandwidth, in kilobits per second (kbps), for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved. The value must be between 1 and 2,000,000 kbps.
burst -in-bytes	(Optional) Burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. The range of the burst is from 32 to 2000000 bytes.
level *level-value*	(Optional) Assigns priority level. Available values for *level-value* are 1 and 2. Level 1 is a higher priority than Level 2. Level 1 reserves bandwidth and goes first, so latency is very low.
percent *percentage*	(Optional) Specifies the amount of guaranteed bandwidth to be specified by the percent of available bandwidth.

Command Default

No priority is set.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The bandwidth and priority commands cannot be used in the same class, within the same policy map. However, these commands can be used together in the same policy map.

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, the policy is removed from all interfaces to which it was successfully attached.

Example

The following example shows how to configure the priority of the class in policy map policy1:

```
Device(config)# class-map cm1
Device(config-cmap)#match precedence 2
Device(config-cmap)#exit

Device(config)#class-map cm2
Device(config-cmap)#match dscp 30
Device(config-cmap)#exit

Device(config)# policy-map policy1
Device(config-pmap)# class cm1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police 1m
Device(config-pmap-c-police)#exit
Device(config-pmap-c)#exit
Device(config-pmap)#exit

Device(config)#policy-map policy1
Device(config-pmap)#class cm2
Device(config-pmap-c)#priority level 2
Device(config-pmap-c)#police 1m
```

queue-buffers ratio

To configure the queue buffer for the class, use the **queue-buffers ratio** command in policy-map class configuration mode. Use the **no** form of this command to remove the ratio limit.

queue-buffers ratio *ratio limit*
no queue-buffers ratio *ratio limit*

Syntax Description

ratio limit	(Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0-100).

Command Default

No queue buffer for the class is defined.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Either the **bandwidth**, **shape**, or **priority** command must be used before using this command. For more information about these commands, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com

The allows you to allocate buffers to queues. If buffers are not allocated, then they are divided equally amongst all queues. You can use the queue-buffer ratio to divide it in a particular ratio. The buffers are soft buffers because Dynamic Threshold and Scaling (DTS) is active on all queues by default.

Example

The following example sets the queue buffers ratio to 10 percent:

```
Device(config)# policy-map policy_queuebuf01
Device(config-pmap)# class-map class_queuebuf01
Device(config-cmap)# exit
Device(config)# policy policy_queuebuf01
Device(config-pmap)# class class_queuebuf01
Device(config-pmap-c)# bandwidth percent 80
Device(config-pmap-c)# queue-buffers ratio 10
Device(config-pmap)# end
```

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

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** policy-map class configuration command. To remove the queue packet limit from a class, use the **no** form of this command.

queue-limit *queue-limit-size* [**packets**] {**cos** *cos-value* | **dscp** *dscp-value*} **percent** *percentage-of-packets*
no queue-limit *queue-limit-size* [**packets**] {**cos** *cos-value* | **dscp** *dscp-value*} **percent** *percentage-of-packets*

Syntax Description

queue-limit-size	The maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified (bytes, ms, us, or packets).
cos *cos-value*	Specifies parameters for each cos value. CoS values are from 0 to 7.
dscp *dscp-value*	Specifies parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value for the type of queue limit .
percent *percentage-of-packets*	A percentage in the range 1 to 100 specifying the maximum percentage of packets that the queue for this class can accumulate.

Command Default

None

Command Modes

Policy-map class configuration (policy-map-c)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Although visible in the command line help-strings, the **packets** unit of measure is not supported; use the **percent** unit of measure.

Note This command is supported only on wired ports in the egress direction.

Weighted fair queuing (WFQ) creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queuing process. When the maximum packet threshold you defined for the class is reached, queuing of any further packets to the class queue causes tail drop.

You use queue limits to configure Weighted Tail Drop (WTD). WTD ensures the configuration of more than one threshold per queue. Each class of service is dropped at a different threshold value to provide for QoS differentiation.

You can configure the maximum queue thresholds for the different subclasses of traffic, that is, DSCP and CoS and configure the maximum queue thresholds for each subclass.

Example

The following example configures a policy map called port-queue to contain policy for a class called dscp-1. The policy for this class is set so that the queue reserved for it has a maximum packet limit of 20 percent:

```
Device(config)# policy-map policy11
Device(config-pmap)# class dscp-1
Device(config-pmap-c)# bandwidth percent 20
Device(config-pmap-c)# queue-limit dscp 1 percent 20
```

random-detect cos

To change the minimum and maximum packet thresholds for the Class of service (CoS) value, use the **random-detect cos** command in QoS policy-map class configuration mode. To return the minimum and maximum packet thresholds to the default for the CoS value, use the **no** form of this command.

random-detect cos *cos-value* **percent** *min-threshold max-threshold*
no random-detect cos *cos-value* **percent***min-threshold max-threshold*

Syntax Description

cos-value	The CoS value, which is IEEE 802.1Q/ISL class of service/user priority value. The CoS value can be a number from 0 to 7.
percent	Specifies that the minimum and threshold values are in percentage.
min-threshold	Minimum threshold in number of packets. The value range of this argument is from 1 to 512000000. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) randomly drop some packets with the specified CoS value.
max-threshold	Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 512000000. When the average queue length exceeds the maximum threshold, WRED or dWRED drop all packets with the specified CoS value.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **random-detect cos** command in conjunction with the **random-detect** command in QoS policy-map class configuration mode.

The **random-detect cos** command is available only if you have specified the *cos-based* argument when using the **random-detect** command in interface configuration mode.

Examples

The following example enables WRED to use the CoS value 8. The minimum threshold for the CoS value 8 is 20, the maximum threshold is 40.

```
random-detect cos-based
random-detect cos percent 5 20 40
```

Related Commands

Command	Description
random-detect	Enables WRED

random-detect cos-based

To enable weighted random early detection (WRED) on the basis of the class of service (CoS) value of a packet, use the **random-detectcos-based** command in policy-map class configuration mode. To disable WRED, use the **no** form of this command.

random-detect cos-based
no random-detect cos-based

Command Default

When WRED is configured, the default minimum and maximum thresholds are determined on the basis of output buffering capacity and the transmission speed for the interface.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

In the following example, WRED is configured on the basis of the CoS value.

```
Switch> enable
Switch# configure terminal
Switch(config)# policy-map policymap1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# random-detect cos-based
Switch(config-pmap-c)#

end
```

Related Commands

Command	Description
random-detect cos	Specifies the CoS value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.
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.

random-detect dscp

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the **random-detect dscp** command in QoS policy-map class configuration mode. To return the minimum and maximum packet thresholds to the default for the DSCP value, use the **no** form of this command.

random-detect dscp *dscp-value* **percent** *min-threshold max-threshold*
no random-detect dscp *dscp-value* **percent***min-threshold max-threshold*

Syntax Description

dscp-value	The DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs7**, **ef**, or **rsvp**.
percent	Specifies that the minimum and threshold values are in percentage.
min-threshold	Minimum threshold in number of packets. The value range of this argument is from 1 to 512000000. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) randomly drop some packets with the specified DSCP value.
max-threshold	Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 512000000. When the average queue length exceeds the maximum threshold, WRED or dWRED drop all packets with the specified DSCP value.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **random-detect dscp** command in conjunction with the **random-detect** command in QoS policy-map class configuration mode.

The **random-detect dscp** command is available only if you specified the *dscp-based* argument when using the **random-detect** command in interface configuration mode.

Specifying the DSCP Value

The **random-detect dscp** command allows you to specify the DSCP value per traffic class. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs7**, **ef**, or **rsvp**.

On a particular traffic class, eight DSCP values can be configured per traffic class. Overall, 29 values can be configured on a traffic class: 8 precedence values, 12 Assured Forwarding (AF) code points, 1 Expedited Forwarding code point, and 8 user-defined DSCP values.

Assured Forwarding Code Points

The AF code points provide a means for a domain to offer four different levels (four different AF classes) of forwarding assurances for IP packets received from other (such as customer) domains. Each one of the four AF classes is allocated a certain amount of forwarding services (buffer space and bandwidth).

Within each AF class, IP packets are marked with one of three possible drop precedence values (binary 2{010}, 4{100}, or 6{110}), which exist as the three lowest bits in the DSCP header. In congested network environments, the drop precedence value of the packet determines the importance of the packet within the AF class. Packets with higher drop precedence values are discarded before packets with lower drop precedence values.

The upper three bits of the DSCP value determine the AF class; the lower three values determine the drop probability.

Examples

The following example enables WRED to use the DSCP value 8. The minimum threshold for the DSCP value 8 is 20, the maximum threshold is 40, and the mark probability is 1/10.

```
random-detect dscp percent 8 20 40
```

Related Commands

Command	Description
random-detect	Enables WRED

random-detect dscp-based

To base weighted random early detection (WRED) on the Differnciated Services Code Point (dscp) value of a packet, use the **random-detectdscp-based** command in policy-map class configuration mode. To disable this feature, use the **no** form of this command.

random-detect dscp-based
no random-detect dscp-based

Syntax Description

This command has no arguments or keywords.

Command Default

WRED is disabled by default.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

With the **random-detectdscp-based** command, WRED is based on the dscp value of the packet.

Use the **random-detectdscp-based** command before configuring the **random-detectdscp** command.

Examples

The following example shows that random detect is based on the precedence value of a packet:

```
Switch> enable
Switch# configure terminal
Switch(config)#

policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth percent 80
Switch(config-pmap-c)# random-detect dscp-based
Switch(config-pmap-c)# random-detect dscp 2 percent 10 40
Switch(config-pmap-c)# exit
```

Related Commands

Command	Description
random-detect	Enables WRED.
random-detect dscp	Configures the WRED parameters for a particular DSCP value for a class policy in a policy map.

random-detect precedence

To configure Weighted Random Early Detection (WRED) parameters for a particular IP precedence for a class policy in a policy map, use the **random-detect precedence** command in QoS policy-map class configuration mode. To return the values to the default for the precedence, use the **no** form of this command.

random-detect precedence *precedence* **percent** *min-threshold max-threshold*
no random-detect precedence

Syntax Description

precedence	IP precedence number. The value range is from 0 to 7; see Table 1 in the "Usage Guidelines" section.
percent	Indicates that the threshold values are in percentage.
min-threshold	Minimum threshold in number of packets. The value range of this argument is from 1 to 512000000. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP precedence.
max-threshold	Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 512000000. When the average queue length exceeds the maximum threshold, WRED or dWRED drop all packets with the specified IP precedence.

Command Default

The default *min-threshold* value depends on the precedence. The *min-threshold* value for IP precedence 0 corresponds to half of the *max-threshold* value. The values for the remaining precedences fall between half the *max-threshold* value and the *max-threshold* value at evenly spaced intervals. See the table in the "Usage Guidelines" section of this command for a list of the default minimum threshold values for each IP precedence.

Command Modes

Interface configuration (config-if)

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

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists.

When you configure the **random-detect** command on an interface, packets are given preferential treatment based on the IP precedence of the packet. Use the **random-detect precedence** command to adjust the treatment for different precedences.

If you want WRED to ignore the precedence when determining which packets to drop, enter this command with the same parameters for each precedence. Remember to use appropriate values for the minimum and maximum thresholds.

Note that if you use the **random-detect precedence** command to adjust the treatment for different precedences within class policy, you must ensure that WRED is not configured for the interface to which you attach that service policy.

Note Although the range of values for the *min-threshold* and *max-threshold* arguments is from 1 to 512000000, the actual values that you can specify depend on the type of random detect you are configuring. For example, the maximum threshold value cannot exceed the queue limit.

Examples

The following example shows the configuration to enable WRED on the interface and to specify parameters for the different IP precedences:

```
interface FortyGigE1/0/1
 description 45Mbps to R1
 ip address 10.200.14.250 255.255.255.252
 random-detect
 random-detect precedence 7 percent 20 50
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
show queuing	Lists all or selected configured queuing strategies.

random-detect precedence-based

To base weighted random early detection (WRED) on the precedence value of a packet, use the **random-detect precedence-based** command in policy-map class configuration mode. To disable this feature, use the **no** form of this command.

random-detect precedence-based
no random-detect precedence-based

Syntax Description

This command has no arguments or keywords.

Command Default

WRED is disabled by default.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

With the **random-detect precedence-based** command, WRED is based on the IP precedence value of the packet.

Use the **random-detect precedence-based** command before configuring the **random-detect precedence-based** command.

Examples

The following example shows that random detect is based on the precedence value of a packet:

```
Device> enable
Device# configure terminal
Device(config)#

policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# bandwidth percent 80
Device(config-pmap-c)# random-detect precedence-based
Device(config-pmap-c)# random-detect precedence 2 percent 30 50
Device(config-pmap-c)# exit
```

Related Commands

Command	Description
random-detect	Enables WRED.
random-detect precedence	Configures the WRED parameters for a particular IP precedence for a class policy in a policy map.

service-policy (Wired)

To apply a policy map to a physical port or a switch virtual interface (SVI), use the **service-policy** command in interface configuration mode. Use the **no** form of this command to remove the policy map and port association.

service-policy {**input** | **output**} *policy-map-name*
no service-policy {**input** | **output**} *policy-map-name*

Syntax Description

input *policy-map-name*	Apply the specified policy map to the input of a physical port or an SVI.
output *policy-map-name*	Apply the specified policy map to the output of a physical port or an SVI.

Command Default

No policy maps are attached to the port.

Command Modes

WLAN interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

A policy map is defined by the **policy map** command.

Only one policy map is supported per port, per direction. In other words, only one input policy and one output policy is allowed on any one port.

You can apply a policy map to incoming traffic on a physical port or on an SVI.

Examples

This example shows how to apply plcmap1 to an physical ingress port:

```
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# service-policy input plcmap1
```

This example shows how to remove plcmap2 from a physical port:

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# no service-policy input plcmap2
```

The following example displays a VLAN policer configuration. At the end of this configuration, the VLAN policy map is applied to an interface for QoS:

```
Device# configure terminal
Device(config)# class-map vlan100
Device(config-cmap)# match vlan 100
Device(config-cmap)# exit
Device(config)# policy-map vlan100
Device(config-pmap)# policy-map class vlan100
Device(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Device(config-pmap-c-police)# end
Device# configure terminal
```

```
Device(config)# interface gigabitethernet 1/0/5
Device(config-if)#  service-policy input vlan100
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

set

To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the **set** command in policy-map class configuration mode. Use the **no** form of this command to remove traffic classification.

set
cos | **dscp** | **precedence** | **ip** | **qos-group**
set cos
{*cos-value* } | {**cos** | **dscp** | **precedence** | **qos-group**} [**table** *table-map-name*]
set dscp
{*dscp-value* } | {**cos** | **dscp** | **precedence** | **qos-group**} [**table** *table-map-name*]
set ip {**dscp** | **precedence**}
set precedence {*precedence-value* } | {**cos** | **dscp** | **precedence** | **qos-group**} [**table** *table-map-name*]
set qos-group
{*qos-group-value* | **dscp** [**table** *table-map-name*] | **precedence** [**table** *table-map-name*]}

Syntax Description

cos	Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values:
	• *cos-value*—CoS value from 0 to 7. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet-marking category to set the CoS value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
	  • **cos**—Sets a value from the CoS value or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map are used to set the CoS value. Enter the name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence (packet-marking category) value is copied and used as the CoS value.

dscp	Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values:
	• *cos-value*—Number that sets the DSCP value. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet-marking category to set the DSCP value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
	  • **cos**—Sets a value from the CoS value or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP value. Enter the name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value (packet-marking category) is copied and used as the DSCP value.

ip	Sets IP values to the classified traffic. You can specify these values: • **dscp**—Specify an IP DSCP value from 0 to 63 or a packet marking category. • **precedence**—Specify a precedence-bit value in the IP header; valid values are from 0 to 7 or specify a packet marking category.

precedence	Sets the precedence value in the packet header. You can specify these values:
	• *precedence-value*— Sets the precedence bit in the packet header; valid values are from 0 to 7. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet marking category to set the precedence value of the packet.
	  • **cos**—Sets a value from the CoS or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the precedence value. Enter the name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value (packet-marking category) is copied and used as the precedence value.

qos-group	Assigns a QoS group identifier that can be used later to classify packets. • *qos-group-value*—Sets a QoS value to the classified traffic. The range is 0 to 31. You also can enter a mnemonic name for a commonly used value. • **dscp**—Sets the original DSCP field value of the packet as the QoS group value. • **precedence**—Sets the original precedence field value of the packet as the QoS group value. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP or precedence value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category (**dscp** or **precedence**) but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the QoS group value. For example, if you enter the **set qos-group precedence** command, the precedence value (packet-marking category) is copied and used as the QoS group value.

Command Default

No traffic classification is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was intro
	The **cos**, **dscp**, **qos-grou**

Usage Guidelines

For the **set dscp** *dscp-value* command, the **set cos** *cos-value* command, and the **set ip precedence** *precedence-value* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **set dscp af11** command, which is the same as entering the **set dscp 10** command. You can enter the **set ip precedence critical** command, which is the same as entering the **set ip precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

When you configure the **set dscp cos**command, note the following: The CoS value is a 3-bit field, and the DSCP value is a 6-bit field. Only the three bits of the CoS field are used.

When you configure the **set dscp qos-group** command, note the following:

- The valid range for the DSCP value is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99.
- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value is copied and the packets is marked.

- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value is not be copied and the packet is not marked. No action is taken.

The **set qos-group** command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC).

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

Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(config-pmap)# exit
```

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

show class-map

To display quality of service (QoS) class maps, which define the match criteria to classify traffic, use the **show class-map** command in EXEC mode.

show class-map [*class-map-name* | **type control subscriber** {**all** | *class-map-name*}]

Syntax Description

class-map-name	(Optional) Class map name.
type control subscriber	(Optional) Displays information about control class maps.
all	(Optional) Displays information about all control class maps.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This is an example of output from the **show class-map** command:

```
Device# show class-map
 Class Map match-any videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-any dscp5 (id 3)
   Match ip dscp 5
```

show platform hardware fed switch

To display device-specific hardware information, use the **show platform hardware fed switch***switch_number* command.

This topic elaborates only the QoS-specific options, that is, the options available with the **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **qos** command.

show platform hardware fed switch {*switch_num* | **active** | **standby**} **qos** {**afd** | {**config type** *type* | [**asic** *asic_num*] | **stats clients** {**all** | **bssid** *id* | **wlanid** *id* }} | **dscp-cos counters** {**iifd_id** *id* | **interface***type number*} | **le-info** | {**iifd_id** *id* | **interface** *type number*} | **policer config** {**iifd_id** *id* | **interface** *type number*} | **queue** | {**config** | {**iifd_id** *id* | **interface** *type number* | **internal port-type** *type* {**asic** *number* [**port_num**]}} | **label2qmap** | [**aqmrepqostbl** | **iqslabeltable** | **sqslabeltable**] | {**asic***number*} | **stats** | {**iifd_id** *id* | **interface** *type number* | **internal** {**cpu policer** | **port-type** *type* **asic** *number*} {**asic***number* [**port_num**]}}} | **resource**}

Syntax Description

switch {*switch_num* | **active** | **standby** }	Switch for which you want to display information. You have the following options: • *switch_num*—ID of the switch. • **active**—Displays information relating to the active switch. • **standby**—Displays information relating to the standby switch, if available.
qos	Displays QoS hardware information. You must choose from the following options: • **afd** —Displays Approximate Fair Drop (AFD) information in hardware. • **dscp-cos**—Displays information dscp-cos counters for each port. • **leinfo**—Displays logical entity information. • **policer**—Displays QoS policer information in hardware. • **queue**—Displays queue information in hardware. • **resource**—Displays hardware resource information.
afd {**config type** | **stats client** }	You must choose from the options under **config type** or **stats client** : **config type**: • **client**—Displays wireless client information • **port**—Displays port-specific information • **radio**—Displays wireless radio information • **ssid**—Displays wireless SSID information **stats client** : • **all**—Displays statistics of all client. • **bssid**—Valid range is from 1 to 4294967295. • **wlanid**—Valid range is from to 1 4294967295

asic*asic_num*	(Optional) ASIC number. Valid range is from 0 to 255.
dscp-cos counters { **iifd_id** *id* | **interface** *type number* }	Displays per port dscp-cos counters. You must choose from the following options under **dscp-cos counters**: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID.
leinfo	You must choose from the following options under **dscp-cos counters**: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID.
policer config	Displays configuration information related to policers in hardware. You must choose from the following options: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID.
queue {**config** {**iif_id** *id* | **interface** *type number* | **internal**} | **label2qmap** | **stats**}	Displays queue information in hardware. You must choose from the following options: • **config**—Configuration information. You must choose from the following options: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID. • **internal**—Displays internal queue related information. • **label2qmap**—Displays hardware label to queue mapping information. You can choose from the following options: • (Optional) **aqmrepqostbl**— AQM REP QoS label table lookup. • (Optional) **iqslabeltable**—IQS QoS label table lookup. • (Optional) **sqslabeltable**—SQS and local QoS label table lookup. • **stats**—Displays queue statistics. You must choose from the following options: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID. • **internal** {**cpu policer** | **port_type** *port_type* **asic** *asic_num* [**port_num** *port_num*] }—Displays internal queue related information.
resource	Displays hardware resource usage information. You must enter the following keyword: **usage**

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
	This command was introduced.

This is an example of output from the**show platform hardware fed switch***switch_number***qos queue stats internal cpu policer** command

```
Device#show platform hardware fed switch 3 qos queue stats internal cpu policer

                                                (default)  (set)
QId PlcIdx  Queue Name                 Enabled   Rate     Rate      Drop
-----------------------------------------------------------------------------
0    11     DOT1X Auth                   No      1000      1000        0
1    1      L2 Control                   No      500       500         0
2    14     Forus traffic                No      1000      1000        0
3    0      ICMP GEN                     Yes     200       200         0
4    2      Routing Control              Yes     1800      1800        0
5    14     Forus Address resolution     No      1000      1000        0
6    3      ICMP Redirect                No      500       500         0
7    6      WLESS PRI-5                  No      1000      1000        0
8    4      WLESS PRI-1                  No      1000      1000        0
9    5      WLESS PRI-2                  No      1000      1000        0
10   6      WLESS PRI-3                  No      1000      1000        0
11   6      WLESS PRI-4                  No      1000      1000        0
12   0      BROADCAST                    Yes     200       200         0
13   10     Learning cache ovfl          Yes     100       100         0
14   13     Sw forwarding                Yes     1000      1000        0
15   8      Topology Control             No      13000     13000       0
16   12     Proto Snooping               No      500       500         0
17   16     DHCP Snooping                No      1000      1000        0
18   9      Transit Traffic              Yes     500       500         0
19   10     RPF Failed                   Yes     100       100         0
20   15     MCAST END STATION            Yes     2000      2000        0
21   13     LOGGING                      Yes     1000      1000        0
22   7      Punt Webauth                 No      1000      1000        0
23   10     Crypto Control               Yes     100       100         0
24   10     Exception                    Yes     100       100         0
25   3      General Punt                 No      500       500         0
26   10     NFL SAMPLED DATA             Yes     100       100         0
27   2      SGT Cache Full               Yes     1800      1800        0
28   10     EGR Exception                Yes     100       100         0
29   16     Show frwd                    No      1000      1000        0
30   9      MCAST Data                   Yes     500       500         0
31   10     Gold Pkt                     Yes     100       100         0
```

show platform software fed switch qos

To display device-specific software information, use the **show platform hardware fed switch** *switch_number* command.

This topic elaborates only the QoS-specific options available with the **show platform software fed switch** {*switch_num* | **active** | **standby** } **qos** command.

show platform software fed switch {*switch number* | **active** | **standby**}**qos** {**avc** | **internal** | **label2qmap** | **nflqos** | **policer** | **policy** | **qsb** | **tablemap**}

Syntax Description

switch {*switch_num* | **active** | **standby** }	The device for which you want to display information. • *switch_num*—Enter the switch ID. Displays information for the specified switch. • **active**—Displays information for the active switch. • **standby**—Displays information for the standby switch, if available.
qos	Displays QoS software information. Choose one the following options: • **avc** —Displays Application Visibility and Control (AVC) QoS information. • **internal**—Displays internal queue-related information. • **label2qmap**—Displays label to queue map table information. • **nflqos**—Displays NetFlow QoS information. • **policer**—Displays QoS policer information in hardware. • **policy**—Displays QoS policy information. • **qsb**—Displays QoS sub-block information. • **tablemap**—Displays table mapping information for QoS egress and ingress queues.

Command Modes

User EXEC

Privileged EXEC

show platform software fed switch qos qsb

To display QoS sub-block information, use the **show platform software fed switch** *switch_number* **qos qsb** command.

show platform software fed switch {*switch number* | **active** | **standby**}**qosqsb** {**brief** | [**all** | **type** | {**client***client_id* | **port** *port_number* | **radio***radio_type* | **ssid***ssid*}] | **iif_id***id* | **interface** | {**Auto-Template***interface_number* | **BDI***interface_number* | **Capwap***interface_number* | **GigabitEthernet***interface_number* | **InternalInterface***interface_number* | **Loopback***interface_number* | **Null***interface_number* | **Port-channel***interface_number* | **TenGigabitEthernet***interface_number* | **Tunnel***interface_number* | **Vlan***interface_number*}}

Syntax Description

switch {*switch_num* | **active** | **standby** }	The switch for which you want to display information. • *switch_num*—Enter the ID of the switch. Displays information for the specified switch. • **active**—Displays information for the active switch. • **standby**—Displays information for the standby switch, if available.
qos qsb	Displays QoS sub-block software information.

qsb {**brief** | **iif_id** | **interface**}	**brief**
	• **all**—Displays information for all client.
	• **type**—Displays qsb information for the specified target type:
	  • **client**—Displays QoS qsb information for wireless clients
	  • **port**—Displays port-specific information
	  • **radio**—Displays QoS qsb information for wireless radios
	  • **ssid**—Displays QoS qsb information for wireless networks
	
	iif_id—Displays information for the iif_ID
	interface—Displays QoS qsb information for the specified interface:
	• **Auto-Template**—Auto-template interface between 1 and 999.
	• **BDI**—Bridge-domain interface between 1 and 16000.
	• **Capwap**—CAPWAP interface between 0 and 2147483647.
	• **GigabitEthernet**—GigabitEthernet interface between 0 and 9.
	• **InternalInterface**—Internal interface between 0 and 9.
	• **Loopback**—Loopback interface between 0 and 2147483647.
	• **Null**—Null interface 0-0
	• **Port-Channel**—Port-channel interface between 1 and 128.
	• **TenGigabitEthernet**—TenGigabitEthernet interface between 0 and 9.
	• **Tunnel**—Tunnel interface between 0 and 2147483647.
	• **Vlan**—VLAN interface between 1 and 4094.

Command Modes

User EXEC

Privileged EXEC

Command History

This is an example of the output for the**show platform software fed switch***switch_number***qos qsb** command

```
Device#sh pl so fed sw 3 qos qsb interface g3/0/2

  QoS subblock information:
  Name:GigabitEthernet3/0/2 iif_id:0x0000000000007b iif_type:ETHER(146)
  qsb ptr:0xffd8573350
  Port type = Wired port
  asic_num:0 is_uplink:false init_done:true
  FRU events: Active-0, Inactive-0
  def_qos_label:0 def_le_priority:13
  trust_enabled:false trust_type:TRUST_DSCP ifm_trust_type:1
  LE priority:13 LE trans_index(in, out): (0,0)
  Stats (plc,q) export counters (in/out): 0/0
```

```
 Policy Info:
   Ingress Policy: pmap::{(0xffd8685180,AutoQos-4.0-CiscoPhone-Input-Policy,1083231504,)}
    tcg::{0xffd867ad10,GigabitEthernet3/0/2 tgt(0x7b,IN) level:0 num_tccg:4 num_child:0},
status:VALID,SET_INHW
   Egress Policy: pmap::{(0xffd86857d0,AutoQos-4.0-Output-Policy,1076629088,)}
    tcg::{0xffd8685b40,GigabitEthernet3/0/2 tgt(0x7b,OUT) level:0 num_tccg:8 num_child:0},
status:VALID,SET_INHW
   TCG(in,out):(0xffd867ad10, 0xffd8685b40) le_label_id(in,out):(2, 1)
 Policer Info:
   num_ag_policers(in,out)[1r2c,2r3c]: ([0,0],[0,0])
   num_mf_policers(in,out): (0,0)
   num_afd_policers:0
   [ag_plc_handle(in,out) = (0xd8688220,0)]
   [mf_plc_handle(in,out)=((nil),(nil)) num_mf_policers:(0,0)
     base:(0xffffffff,0xffffffff) rc:(0,0)]
 Queueing Info:
   def_queuing = 0, shape_rate:0 interface_rate_kbps:1000000
   Port shaper:false
   lbl_to_qmap_index:1
   Physical qparams:
    Queue Config: NodeType:Physical Id:0x40000049 parent:0x40000049 qid:0 attr:0x1 defq:0

       PARAMS: Excess Ratio:1 Min Cir:1000000 QBuffer:0
       Queue Limit Type:Single Unit:Percent Queue Limit:44192
       SHARED Queue
```

show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming traffic, use the **show policy-map** command in EXEC mode.

show policy-map [*policy-map-name* | **interface** *interface-id*]

show policy-map interface {**Auto-template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Lspvif** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan** | **brief** | **class** | **input** | **output**

Syntax Description

policy-map-name	(Optional) Name of the policy-map.
interface *interface-id*	(Optional) Displays the statistics and the configurations of the input and output policies that are attached to the interface.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command w

Usage Guidelines

Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

Note Though visible in the command-line help string, the **control-plane**, **session**, and **type** keywords are not supported, and the statistics shown in the display should be ignored.

This is an example of the output for the **show policy-map interface** command.

```
Device# show policy-map interface gigabitethernet1/0/48GigabitEthernet1/0/48

  Service-policy output: port_shape_parent

    Class-map: class-default (match-any)
      191509734 packets
      Match: any
      Queueing

      (total drops) 524940551420
      (bytes output) 14937264500
      shape (average) cir 250000000, bc 2500000, be 2500000
      target shape rate 250000000

      Service-policy : child_trip_play

        queue stats for all priority classes:
          Queueing
          priority level 1
```

```
  (total drops) 524940551420
  (bytes output) 14937180648

queue stats for all priority classes:
  Queueing
  priority level 2

  (total drops) 0
  (bytes output) 0

Class-map: dscp56 (match-any)
  191508445 packets
  Match:  dscp cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: Strict,

  Priority Level: 1
  police:
      cir 10 %
      cir 25000000 bps, bc 781250 bytes
    conformed 0 bytes; actions: >>>>>counters not supported
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceeded 0000 bps  >>>>>counters not supported
```

show tech-support qos

To display quality of service (QoS)-related information for use by technical support, use the **show tech-support qos** command in privileged EXEC mode.

show tech-support qos [**switch** {*switch-number* | **active** | **all** | **standby**} | [**control-plane** | **interface** {*interface-name* | **all**}]]

Syntax Description

switch *switch-number*	(Optional) Displays QoS-related information for a specific switch.
active	(Optional) Displays QoS-related information for the active instance of the switch.
all	(Optional) Displays QoS-related information for all instances of the switch.
standby	(Optional) Displays QoS-related information for the standby instance of the switch.
control-plane	(Optional) Displays QoS-related information for the control-plane.
interface *interface-name*	(Optional) Displays QoS-related information for a specified interface.
all	(Optional) Displays QoS-related information for all interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support qos | redirect flash:** *filename*) in the local writable storage file system or remote file system.

The output of the **show tech-support qos** command displays a list of commands and their output. These commands differ based on the platform.

Examples

The following is sample output from the **show tech-support qos** command:

```
Device# show tech-support qos
.
.
```

```
.
------------------ show platform software fed switch 1 qos policy target brief
------------------


TCG summary for policy: system-cpp-policy

Loc Interface              IIF-ID           Dir tccg Child #m/p/q  State:(cfg,opr)
--- ---------------------- ---------------- --- ---- ----- ------- ---------------
?:255 Control Plane      0x00000001000001 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4da31c8
?:0 CoPP-Queue-0         0x0000000100000d OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4da41e8
?:0 CoPP-Queue-1         0x0000000100000e OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dbede8
?:0 CoPP-Queue-2         0x0000000100000f OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dc2df8
?:0 CoPP-Queue-3         0x00000001000010 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dc6e08
?:0 CoPP-Queue-4         0x00000001000011 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dcae18
?:0 CoPP-Queue-5         0x00000001000012 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dcee28
?:0 CoPP-Queue-6         0x00000001000013 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dd2e38
?:0 CoPP-Queue-7         0x00000001000014 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dd6e48
?:0 CoPP-Queue-8         0x00000001000015 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4ddae58
?:0 CoPP-Queue-9         0x00000001000016 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4ddee68
?:0 CoPP-Queue-10        0x00000001000017 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4de2e78
?:0 CoPP-Queue-11        0x00000001000018 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4de6e88
?:0 CoPP-Queue-12        0x00000001000019 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4deae98
?:0 CoPP-Queue-13        0x0000000100001a OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4deeea8
?:0 CoPP-Queue-14        0x0000000100001b OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4df2eb8
?:0 CoPP-Queue-15        0x0000000100001c OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4df6ec8
?:0 CoPP-Queue-16        0x0000000100001d OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dfaed8
?:0 CoPP-Queue-17        0x0000000100001e OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dfeee8
?:0 CoPP-Queue-18        0x0000000100001f OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e02ef8
?:0 CoPP-Queue-19        0x00000001000020 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e06f08
?:0 CoPP-Queue-20        0x00000001000021 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e0ae88
?:0 CoPP-Queue-21        0x00000001000022 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e0ee98
?:0 CoPP-Queue-22        0x00000001000023 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e12ea8
?:0 CoPP-Queue-23        0x00000001000024 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e16eb8
?:0 CoPP-Queue-24        0x00000001000025 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e1aec8
?:0 CoPP-Queue-25        0x00000001000026 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e1eed8
?:0 CoPP-Queue-26        0x00000001000027 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e22ee8
?:0 CoPP-Queue-27        0x00000001000028 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e26ef8
?:0 CoPP-Queue-28        0x00000001000029 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e2af08
?:0 CoPP-Queue-29        0x0000000100002a OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e2ef18
?:0 CoPP-Queue-30        0x0000000100002b OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e32f28
?:0 CoPP-Queue-31        0x0000000100002c OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e36f38

------------------ show platform software fed switch 1 qos policy summary ------------------


Policymap Summary: (counters)
  CGID     Clases Targets Child CfgErr InHw  OpErr Policy Name
---------- ------ ------- ----- ------ ----- ----- ------------------
15212688   22     33      0     0      33    0     system-cpp-policy
.
.
.
```

Output fields are self-explanatory.

trust device

To configure trust for supported devices connected to an interface, use the **trust device** command in interface configuration mode. Use the **no** form of this command to disable trust for the connected device.

trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}
no trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}

Syntax Description

cisco-phone	Configures a Cisco IP phone
cts	Configures a Cisco TelePresence System
ip-camera	Configures an IP Video Surveillance Camera (IPVSC)
media-player	Configures a Cisco Digital Media Player (DMP)

Command Default

Trust disabled

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **trust device** command on the following types of interfaces:

- **Auto**— auto-template interface
- **Capwap**—CAPWAP tunnel interface
- **GigabitEthernet**—Gigabit Ethernet IEEE 802
- **GroupVI**—Group virtual interface
- **Internal Interface**—Internal interface
- **Loopback**—Loopback interface
- **Null**—Null interface
- **Port-channel**—Ethernet Channel interface
- **TenGigabitEthernet--**10-Gigabit Ethernet
- **Tunnel**—Tunnel interface
- **Vlan**—Catalyst VLANs
- **range**—**interface range** command

Example

The following example configures trust for a Cisco IP phone in Interface GigabitEthernet 1/0/1:

```
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# trust device cisco-phone
```