QoS

This chapter contains the following QoS commands:

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	Assigns a name to the class map.
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 Release 15.0(2)EXCisco IOS Release 15.2(5)E	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 policy-map class configuration mode. These configuration commands are available:

- **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 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, see police, on page 32 and police aggregate, on page 34.
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see set, on page 40.
- **trust**—Defines a trust state for traffic classified with the **class** or the **class-map** command. For more information, see trust, on page 60.

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.

Examples

This example shows how to configure a default traffic class to a policy map:

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# match protocol ipv6
Device(config-cmap)# exit
Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# match protocol ip
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)# trust cos
Device(config-pmap-c)# exit
Device(config-pmap)# exit
```

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

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

```
Device# show policy-map pm3
  Policy Map pm3
    Class cm-3
      set dscp 4
    Class cm-4
      trust cos
    Class class-default
      set dscp 10
Device#
```

Related Commands

Command	Description
class-map, on page 4	Creates a class map to be used for matching packets to the class whose name you specify.
police, on page 32	Defines a policer for classified traffic.
policy map, on page 36	Defines a policer for classified traffic.
set, on page 40	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map, on page 53	Displays quality of service (QoS) policy maps.
trust, on page 60	Defines a trust state for the traffic classified through the **class** policy-map configuration command or the **class-map** global configuration command.

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

Syntax Description		
match-any	(Optional) Performs a logical-OR of the matching statements under this class map. One or more criteria must be matched.	
type	(Optional) Configures the CPL class map.	
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.	

Command Default

No class maps are defined.

Command Modes

Global configuration

Policy map configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

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. For more information, see the match (class-map configuration), on page 8 .
- **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.

Only one ACL can be configured in a class map. The ACL can have multiple access control entries (ACEs).

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.

Related Commands	Command	Description
	class, on page 2	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.
	match (class-map configuration), on page 8	Defines the match criteria to classify traffic.
	policy map, on page 36	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	show class-map, on page 42	Displays QoS class maps.

debug qos

To enable debugging of the quality of service (QoS) software, use the **debug qos** in privileged EXEC mode. Use the **no** form of this command to disable QoS debugging.

debug qos
{capability|command-installation-time|events|index|pre-classify|provision|service-policy|set|snmp|tunnel_marking}
no debug qos
{capability|command-installation-time|events|index|pre-classify|provision|service-policy|set|snmp|tunnel_marking}

Syntax Description

capability	Displays all QoS capability debug messages.
command-installation-time	Displays the amount of time the QoS command takes to become effective.
events	Displays QoS MQC events.
index	Displays class-based QoS MIB index persistency.
pre-classify	Displays QoS pre-classify events for VPN.
provision	Displays QoS provisions.
service-policy	Displays QoS service policies.
set	Displays QoS packet marking.
snmp	Displays class-based QoS configuration and statistics information.
tunnel_marking	Displays QoS packet tunnel marking.

Command Default   Debugging is disabled.

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   The **undebug qos** command is the same as the **no debug qos** command.

When you enable debugging on a switch stack, it is enabled only on the stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session** *switch-number* privileged EXEC command, then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* privileged EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

QoS

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.

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.

match {**access-group** *acl-index-or-name*|**ip** {**dscp** *dscp-list* |**precedence** *ip-precedence-list*}|**protocol** {**arp|cdp|http|ip|ipv6**}}
no match {**access-group** *acl-index-or-name*|**ip** {**dscp** *dscp-list* |**precedence** *ip-precedence-list*}|**protocol** {**arp|cdp|http|ip|ipv6**}}

Syntax Description		
	access-group *acl-index-or-name*	Specifies the number or name of an access control list (ACL). The range is from 1 to 2799.
	ip	Sets IP specific values. • **dscp** *dscp-list*—Lists 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. • **precedence** *ip-precedence-list*—Lists 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.
	protocol	Specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map. The following protocols are supported: **arp**,**cdp**, **http**, **ip**, and **ipv6**.

Command Default No match criteria are defined.

Command Modes Class-map configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

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

You cannot enter the **match access-group** *acl-index* command.

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.

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

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
```

Related Commands

Command	Description
class-map, on page 4	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map, on page 42	Displays quality of service (QoS) class maps.

mls qos

To enable quality of service (QoS) for the entire switch, use the **mls qos** command in global configuration mode. Use the **no** form of this command to reset all the QoS-related statistics and to disable the QoS features for the entire switch.

mls qos
no mls qos

Syntax Description	This command has no arguments or keywords.
Command Default	QoS is disabled. There is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).
	When QoS is enabled with the **mls qos** global configuration command and all other QoS settings are set to their defaults, traffic is classified as best effort (the DSCP and CoS value is set to 0) without any policing. No policy maps are configured. The default port trust state on all ports is untrusted. The default egress queue settings are in effect.
Command Modes	Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines	When the **mls qos** command is entered, QoS is enabled with the default parameters on all ports in the system.
	QoS must be globally enabled to use QoS classification, policing, marking or dropping, queueing, and traffic shaping features. You can create a policy map and attach it to a port before entering the **mls qos** command. QoS processing is disabled until you enter the **mls qos** command.
	When you enter the **no mls qos** command, policy maps and class maps that are used to configure QoS are not deleted from the configuration, but entries corresponding to policy maps are removed from the switch hardware to save system resources. To reenable QoS with the previous configurations, enter the **mls qos** command.
	Toggling the QoS status of the switch with this command modifies (reallocates) the sizes of the queues. During the queue size modification, the queue is temporarily shut down during the hardware reconfiguration, and the switch drops newly arrived packets for this queue.
Examples	This example shows how to enable QoS on the switch:

```
Device(config)# mls qos
```

You can verify your settings by entering the **show mls qos** privileged EXEC command.

Related Commands

Command	Description
show mls qos, on page 43	Displays QoS information.

mls qos aggregate-policer

To define policer parameters that can be shared by multiple classes within the same policy map, use the **mls qos aggregate-policer** command in global configuration mode. Use the **no** form of this command to delete an aggregate policer.

mls qos aggregate-policer *aggregate-policer-name rate-bps burst-byte* **exceed-action** {**drop**|**policed-dscp-transmit**}
no mls qos aggregate-policer *aggregate-policer-name rate-bps burst-byte* {**drop**|**policed-dscp-transmit**}

Syntax Description

aggregate-policer-name	The name of the aggregate policer as referenced by the **police aggregate** policy-map class configuration command.
rate-bps	The average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.
burst-byte	The normal burst size in bytes. The range is 8000 to 1000000.
exceed-action drop	Sets the traffic rate. If the rate is exceeded, the switch drops the packet.
exceed-action policed-dscp-transmit	Sets the traffic rate. If the rate is exceeded, the switch changes the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then sends the packet.

Command Default   No aggregate policers are defined.

Command Modes   Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

Define an aggregate policer if the policer is shared with multiple classes.

Policers for a port cannot be shared with other policers for another port; traffic from two different ports cannot be aggregated for policing purposes.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port (there is no guarantee that a port will be assigned to any policer).

You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps.

You cannot delete an aggregate policer if it is being used in a policy map. You must first use the **no police aggregate** *aggregate-policer-name* policy-map class configuration command to delete the aggregate policer from all policy maps before using the **no mls qos aggregate-policer** *aggregate-policer-name* command.

Policing uses a token-bucket algorithm. You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure how fast (the average rate) that the tokens are removed from the bucket by using the *rate-bps* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. For more information, see the software configuration guide for this release.

Examples

This example shows how to define the aggregate policer parameters and how to apply the policer to multiple classes in a policy map:

```
Device(config)# mls qos aggregate-policer agg_policer1 1000000 1000000 exceed-action drop
Device(config)# policy-map policy2
Device(config-pmap)# class class1
Device(config-pmap-c)# police aggregate agg_policer1
Device(config-pmap-c)# exit
Device(config-pmap)# class class2
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police aggregate agg_policer1
Device(config-pmap-c)# exit
Device(config-pmap)# class class3
Device(config-pmap-c)# trust dscp
Device(config-pmap-c)# police aggregate agg_policer2
Device(config-pmap-c)# exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

Related Commands

Command	Description
police aggregate, on page 34	Creates a policer that is shared by different classes.
show mls qos aggregate-policer, on page 44	Displays the quality of service (QoS) aggregate policer configuration.

mls qos cos

To define the default class of service (CoS) value of a port or to assign the default CoS to all incoming packets on the port, use the **mls qos cos** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

mls qos cos {*default-cos*|**override**}
no qos mls cos {*default-cos*|**override**}

Syntax Description	*default-cos* The default CoS value that is assigned to a port. If packets are untagged, the default CoS value becomes the packet CoS value. The CoS range is 0 to 7.
	override Overrides the CoS value of the incoming packets, and apply the default CoS value on the port to all incoming packets.

Command Default

The default CoS value for a port is 0.

CoS override is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

You can use the default value to assign a CoS and Differentiated Services Code Point (DSCP) value to all incoming packets that are untagged (if the incoming packet does not have a CoS value). You also can assign a default CoS and DSCP value to all incoming packets by using the **override** keyword.

Use the **override** keyword when all incoming packets on certain ports deserve higher or lower priority than packets entering from other ports. Even if a port is previously set to trust DSCP, CoS, or IP precedence, this command overrides the previously configured trust state, and all the incoming CoS values are assigned the default CoS value configured with the **mls qos cos** command. If an incoming packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.

Examples

This example shows how to configure the default port CoS to 4 on a port:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# mls qos trust cos
Device(config-if)# mls qos cos 4
```

This example shows how to assign all the packets entering a port to the default port CoS value of 4 on a port:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# mls qos cos 4
Device(config-if)# mls qos cos override
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface, on page 45	Displays quality of service (QoS) information.

mls qos dscp-mutation

To apply a Differentiated Services Code Point (DSCP)-to-DSCP-mutation map to a DSCP-trusted port, use the **mls qos dscp-mutation** command in interface configuration mode. Use the **no** form of this command to return the map to the default settings.

mls qos dscp-mutation *dscp-mutation-name*
no mls qos dscp-mutation *dscp-mutation-name*

Syntax Description	*dscp-mutation-name* The name of the DSCP-to-DSCP-mutation map. This map was previously defined with the **mls qos map dscp-mutation** global configuration command.

Command Default   The default DSCP-to-DSCP-mutation map is a null map, which maps incoming DSCPs to the same DSCP values.

Command Modes   Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   If two quality of service (QoS) domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate one set of DSCP values to match the definition of another domain. You apply the DSCP-to-DSCP-mutation map to the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

With ingress mutation, the new DSCP value overwrites the one in the packet, and QoS handles the packet with this new value. The switch sends the packet out the port with the new DSCP value.

You can configure multiple DSCP-to-DSCP-mutation maps on ingress ports.

You apply the map only to DSCP-trusted ports. If you apply the DSCP mutation map to an untrusted port, to CoS or IP-precedence trusted port, the command has no immediate effect until the port becomes DSCP-trusted.

Examples   This example shows how to define the DSCP-to-DSCP mutation map named *dscpmutation1* and to apply the map to a port:

```
Device(config)# mls qos map dscp-mutation dscpmutation1 10 11 12 13 to 30
Device(config)# interface gigabitethernet3/0/1
Device(config-if)# mls qos trust dscp
Device(config-if)# mls qos dscp-mutation dscpmutation1
```

This example shows how to remove the DSCP-to-DSCP mutation map name *dscpmutation1* from the port and to reset the map to the default:

```
Device(config-if)# no mls qos dscp-mutation dscpmutation1
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands

Command	Description
mls qos map, on page 18	Defines the DSCP-to-DSCP mutation map.
mls qos trust, on page 30	Configures the port trust state.
show mls qos maps, on page 49	Displays QoS mapping information.

mls qos map

To define the DSCP-to-DSCP-mutation map, use the **mls qos map** command in global configuration mode. Use the **no** form of this command to return to the default map.

mls qos map {**dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*}
no mls qos map {**dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*}

Syntax Description		
	dscp-mutation *dscp-mutation-name in-dscp* **to** *out-dscp*	Defines the DSCP-to-DSCP-mutation map.
		For *dscp-mutation-name*, enter the mutation map name.
		For *in-dscp*, enter up to eight DSCP values, with each value separated by a space, then enter the **to** keyword.
		For *out-dscp*, enter a single DSCP value.
		The range is 0 to 63.

Command Default

When this command is disabled, the default maps are set.

The default DSCP-to-DSCP-mutation map is a null map, which maps an incoming DSCP value to the same DSCP value.

The default policed-DSCP map is a null map, which maps an incoming DSCP value to the same DSCP value.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.2(6)E1	This command was introduced.

Usage Guidelines

All the maps are globally defined. The DSCP-to-DSCP-mutation map is applied to a specific port.

This example shows how to define the DSCP-to-DSCP-mutation map. All the entries that are not explicitly configured are not modified (remain as specified in the null map):

```
Device# configure terminal
Device(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 10
Device(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Device(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Device(config)# mls qos map dscp-mutation mutation1 0 31 32 33 34 to 30
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands

Command	Description
mls qos dscp-mutation, on page 16	Applies a DSCP-to-DSCP-mutation map to a DSCP-trusted port.
show mls qos maps, on page 49	Displays quality of service (QoS) mapping information.

mls qos queue-set output buffers

To allocate buffers to a queue set of four egress queues per port, use the **mls qos queue-set output buffers** command in global configuration mode. To return to the default setting, use the **no** form of this command.

mls qos queue-set output *qset-id* **buffers** *allocation1 ... allocation4*
no mls qos queue-set output *qset-id* **buffers**

Syntax Description		
	qset-id	Queue set ID. Each port belongs to a queue set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
	allocation1 ... allocation4	Buffer space allocation (percentage) for each queue (four values for queues 1 to 4).
		For *allocation1*, *allocation3*, and *allocation4*, the range is 0 to 99.
		For *allocation2*, the range is 1 to 100 (including the CPU buffer). Separate each value with a space.

Command Default

All allocation values are equally mapped among the four queues (25, 25, 25, 25). Each queue has $1/4^{th}$ of the buffer space.

Command Modes

Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

Specify the allocation values, and separate each with a space.

Allocate buffers according to the importance of the traffic. For example, give a large percentage of the buffer to the queue with the highest-priority traffic.

Note The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

To configure different classes of traffic with different characteristics, use this command with the **mls qos queue-set output** *qset-id* **threshold** global configuration command.

Examples

This example shows how to map a port to queue set *2*. It allocates 40 percent of the buffer space to egress queue 1 and 20 percent to egress queues 2, 3, and 4.

```
Device(config)# mls qos queue-set output 2 buffers 40 20 20 20
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface** [*interface-id* **buffers**] or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output threshold, on page 21	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
queue-set, on page 38	Maps a port to a queue set.
show mls qos interface, on page 45	Displays quality of service (QoS) information at the port level
show mls qos queue-set, on page 52	Displays egress queue settings for the queue set.

mls qos queue-set output threshold

To configure the weighted tail-drop (WTD) thresholds, to guarantee the availability of buffers, and to configure the maximum memory allocation to a queue set (four egress queues per port), use the **mls qos queue-set output threshold** command in global configuration mode. Use the **no** form of this command to return to the default setting.

mls qos queue-set output *qset-id* **threshold** [*queue-id*] *drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*
no mls qos queue-set output *qset-id* **threshold** [*queue-id*]

Syntax Description

qset-id	Queue set ID. Each port belongs to a queue set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
queue-id	(Optional) The queue in the queue set on which the command is performed. The range is 1 to 4.
drop-threshold1 drop-threshold2	Two WTD thresholds expressed as a percentage of the allocated memory of the queue. The range is 1 to 3200 percent.
reserved-threshold	The amount of memory to be guaranteed (reserved) for the queue and expressed as a percentage of the allocated memory. The range is 1 to 100 percent.
maximum-threshold	Queue in the full condition that is enabled to get more buffers than are reserved for it. This is the maximum memory the queue can have before the packets are dropped. The range is 1 to 3200 percent.

Command Default

When quality of service (QoS) is enabled, WTD is enabled.

For default egress queue WTD threshold values , see Table 1: Default Egress Queue WTD Threshold Settings, on page 21.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

Use the **mls qos queue-set output** *qset-id* **buffers** global configuration command to allocate a fixed number of buffers to the four queues in a queue set.

Table 1: Default Egress Queue WTD Threshold Settings

Feature	Queue 1	Queue 2	Queue 3	Queue 4
WTD drop threshold 1	100 percent	200 percent	100 percent	100 percent

Feature	Queue 1	Queue 2	Queue 3	Queue 4
WTD drop threshold 2	100 percent	200 percent	100 percent	100 percent
Reserved threshold	50 percent	100 percent	50 percent	50 percent
Maximum threshold	400 percent	400 percent	400 percent	400 percent

The drop-threshold percentages can exceed 100 percent and can be up to the maximum (if the maximum threshold exceeds 100 percent).

While buffer ranges allow individual queues in the queue set to use more of the common pool when available, the maximum user-configurable number of packets for each queue is still internally limited to 3200 percent, or 32 times the allocated number of buffers. One packet can use one 1 or more buffers.

Note   The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

The switch uses a buffer allocation scheme to reserve a minimum amount of buffers for each egress queue, to prevent any queue or port from consuming all the buffers and depriving other queues, and to decide whether to grant buffer space to a requesting queue. The switch decides whether the target queue has not consumed more buffers than its reserved amount (under-limit), whether it has consumed all of its maximum buffers (over-limit), and whether the common pool is empty (no free buffers) or not empty (free buffers). If the queue is not over-limit, the switch can allocate buffer space from the reserved pool or from the common pool (if it is not empty). If there are no free buffers in the common pool or if the queue is over-limit, the switch drops the frame.

Examples

This example shows how to map a port to queue set 2. It configures the drop thresholds for queue 2 to 40 and 60 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory this queue can have before packets are dropped:

```
Device(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **buffers** or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers, on page 19	Allocates buffers to a queue set.
queue-set, on page 38	Maps a port to a queue set.
show mls qos interface, on page 45	Displays quality of service (QoS) information at the port level.

Command	Description
show mls qos queue-set, on page 52	Displays egress queue settings for the queue-set.

mls qos rewrite ip dscp

To configure the switch to change or rewrite the Differentiated Services Code Point (DSCP) field of an incoming IP packet, use the **mls qos rewrite ip dscp** command in global configuration mode. Use the **no** form of this command to configure the switch to not modify or rewrite the DSCP field of the packet and to enable DSCP transparency.

mls qos rewrite ip dscp
no mls qos rewrite ip dscp

Syntax Description   This command has no arguments or keywords.

Command Default   DSCP transparency is disabled. The switch changes the DSCP field of the incoming IP packet.

Command Modes   Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   DSCP transparency affects only the DSCP field of a packet at the egress. If DSCP transparency is enabled by using the **no mls qos rewrite ip dscp** command, the switch does not modify the DSCP field in the incoming packet, and the DSCP field in the outgoing packet is the same as that in the incoming packet.

Note   Enabling DSCP transparency does not affect the port trust settings on IEEE 802.1Q tunneling ports.

By default, DSCP transparency is disabled. The switch modifies the DSCP field in an incoming packet, and the DSCP field in the outgoing packet is based on the quality of service (QoS) configuration, including the port trust setting, policing and marking, and the DSCP-to-DSCP mutation map.

Regardless of the DSCP transparency configuration, the switch modifies the internal DSCP value of the packet that the switch uses to generate a class of service (CoS) value representing the priority of the traffic. The switch also uses the internal DSCP value to select an egress queue and threshold.

For example, if QoS is enabled and an incoming packet has a DSCP value of 32, the switch might modify the internal DSCP value based on the policy-map configuration and change the internal DSCP value to 16. If DSCP transparency is enabled, the outgoing DSCP value is 32 (same as the incoming value). If DSCP transparency is disabled, the outgoing DSCP value is 16 because it is based on the internal DSCP value.

Examples   This example shows how to enable DSCP transparency and configure the switch to not change the DSCP value of the incoming IP packet:

```
Device(config)# mls qos
Device(config)# no mls qos rewrite ip dscp
```

This example shows how to disable DSCP transparency and configure the switch to change the DSCP value of the incoming IP packet:

```
Device(config)# mls qos
Device(config)# mls qos rewrite ip dscp
```

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

Related Commands	Command	Description
	mls qos, on page 10	Enables QoS globally.
	show mls qos, on page 43	Displays QoS information.
	**show running-config	include rewrite**	Displays the DSCP transparency setting.

mls qos srr-queue output cos-map

To map class of service (CoS) values to an egress queue or to map CoS values to a queue and to a threshold ID, use the **mls qos srr-queue output cos-map** command global configuration mode. Use the **no** form of this command to return to the default setting.

mls qos srr-queue output cos-map queue *queue-id* {*cos1 ... cos8* |**threshold** *threshold-id cos1 ... cos8* }
no mls qos srr-queue output cos-map

Syntax Description		
queue *queue-id*	Specifies a queue number.
	For *queue-id*, the range is 1 to 4.
cos1 ... cos8	CoS values that are mapped to an egress queue.
	For *cos1...cos8*, enter up to eight values, and separate each value with a space. The range is 0 to 7.
threshold *threshold-id cos1...cos8*	Maps CoS values to a queue threshold ID.
	For *threshold-id*, the range is 1 to 3.
	For *cos1...cos8*, enter up to eight values, and separate each value with a space. The range is 0 to 7.

Command Default

For default CoS output queue thresholds values, see .

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.

Note The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your quality of service (QoS) solution.

You can assign two weighted tail-drop (WTD) threshold percentages to an egress queue by using the **mls qos queue-set output** *qset-id* **threshold** global configuration command.

You can map each CoS value to a different queue and threshold combination, allowing the frame to follow different behavior.

Table 2: Default Cos Output Queue Threshold Map

CoS Value	0	1	2	3	4	5	6	7
Queue ID–Threshold ID	2–1	2–1	3–1	3–1	4–1	1–1	4–1	4–1

Examples

This example shows how to map a port to queue set 1. It maps CoS values 0 to 3 to egress queue 1 and to threshold ID 1. It configures the drop thresholds for queue 1 to 50 and 70 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Device(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Device(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# queue-set 1
```

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface** [*interface-id*] **buffers**, or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output threshold, on page 21	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
mls qos srr-queue output dscp-map, on page 28	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
queue-set, on page 38	Maps a port to a queue set.
show mls qos interface, on page 45	Displays quality of service (QoS) information at the port level
show mls qos maps, on page 49	Displays QoS mapping information.
show mls qos queue-set, on page 52	Displays egress queue settings for the queue-set.

mls qos srr-queue output dscp-map

To map Differentiated Services Code Point (DSCP) values to an egress queue or to map DSCP values to a queue and to a threshold ID, use the **mls qos srr-queue output dscp-map** command in global configuration mode. Use the **no** form of this command to return to the default setting.

mls qos srr-queue output dscp-map queue *queue-id* { *dscp1 ... dscp8* |**threshold** *threshold-id dscp1 ... dscp8* }
no mls qos srr-queue output dscp-map

Syntax Description		
	queue *queue-id*	Specifies a queue number.
		For *queue-id*, the range is 1 to 4.
	dscp1 ... dscp8	DSCP values that are mapped to an egress queue.
		For *dscp1...dscp8*, enter up to eight values, and separate each value with a space. The range is 0 to 63.
	threshold *threshold-id dscp1...dscp8*	Maps DSCP values to a queue threshold ID.
		For *threshold-id*, the range is 1 to 3.
		For *dscp1...dscp8*, enter up to eight values, and separate each value with a space. The range is 0 to 63.

Command Default   The default DSCP output queue thresholds are set.

Command Modes   Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.

For default DSCP output queue-threshold map values, see

Note   The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

You can assign two weighted tail-drop (WTD) threshold percentages to an egress queue by using the **mls qos queue-set output** *qset-id* **threshold** global configuration command.

You can map each DSCP value to a different queue and threshold combination, allowing the frame to follow different behavior.

You can map up to eight DSCP values per command.

Table 3: Default DSCP Output Queue Threshold Map

DSCP Value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Queue ID–Threshold ID	2–1	2–1	3–1	3–1	4–1	1–1	4–1	4–1

Examples

This example shows how to map a port to queue set 1. It maps DSCP values 0 to 3 to egress queue 1 and to threshold ID 1. It configures the drop thresholds for queue 1 to 50 and 70 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Device(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3
Device(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# queue-set 1
```

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface** [*interface-id*] **buffers** or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos srr-queue output cos-map, on page 26	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos queue-set output threshold, on page 21	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
queue-set, on page 38	Maps a port to a queue set.
show mls qos interface, on page 45	Displays quality of service (QoS) information at the port level
show mls qos maps, on page 49	Displays QoS mapping information.
show mls qos queue-set, on page 52	Displays egress queue settings for the queue set.

mls qos trust

To configure the port trust state, use the **mls qos trust** command in interface configuration mode. Use the **no** form of this command to return a port to its untrusted state.

mls qos trust [{**cos**|**device** {**cisco-phone**|**cts**|**ip-camera**|**media-player**}|**dscp**|**ip-precedence**}]
no mls qos trust [{**cos**|**device** {**cisco-phone**|**cts**|**ip-camera**|**media-player**}|**dscp**|**ip-precedence**}]

Syntax Description		
cos	(Optional) Classifies an ingress packet by using the packet CoS value. For an untagged packet, use the port default CoS value.	
device cisco-phone	(Optional) Classifies an ingress packet by trusting the CoS or DSCP value sent from the Cisco IP Phone (trusted boundary), depending on the trust setting.	
device {**cts** | **ip-camera** | **media-player**}	(Optional) Classifies an ingress packet by trusting the CoS or DSCP value for these video devices: • **cts**—Cisco TelePresence System • **ip-camera**—Cisco IP camera • **media-player**—Cisco digital media player For an untagged packet, use the port default CoS value.	
dscp	(Optional) Classifies an ingress packet by using the packet DSCP value (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS is used if the packet is tagged. For an untagged packet, the default port CoS value is used.	
ip-precedence	(Optional) Classifies an ingress packet by using the packet IP-precedence value (most significant 3 bits of 8-bit service-type field). For a non-IP packet, the packet CoS is used if the packet is tagged. For an untagged packet, the port default CoS value is used.	

Command Default   The port is not trusted. If no keyword is specified when you enter the command, the default is **dscp**.

Command Modes   Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   Packets entering a quality of service (QoS) domain are classified at the edge of the domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain. Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When a port is configured with trust DSCP or trust IP precedence and the incoming packet is a non-IP packet, the CoS-to-DSCP map is used to derive the corresponding DSCP value from the CoS value. The CoS can be the packet CoS for trunk ports or the port default CoS for nontrunk ports.

If the DSCP is trusted, the DSCP field of the IP packet is not modified. However, it is still possible that the CoS value of the packet is modified (according to DSCP-to-CoS map).

If the CoS is trusted, the CoS field of the packet is not modified, but the DSCP can be modified (according to CoS-to-DSCP map) if the packet is an IP packet.

The trusted boundary feature prevents security problems if users disconnect their PCs from networked Cisco IP Phones and connect them to the switch port to take advantage of trusted CoS or DSCP settings. You must globally enable the Cisco Discovery Protocol (CDP) on the switch and on the port connected to the IP phone. If the telephone is not detected, trusted boundary disables the trusted setting on the switch or routed port and prevents misuse of a high-priority queue.

If you configure the trust setting for DSCP or IP precedence, the DSCP or IP precedence values in the incoming packets are trusted. If you configure the **mls qos cos override** interface configuration command on the switch port connected to the IP phone, the switch overrides the CoS of the incoming voice and data packets and assigns the default CoS value to them.

For an inter-QoS domain boundary, you can configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different between the QoS domains.

Classification using a port trust state (for example, **mls qos trust** [**cos** | **dscp** | **ip-precedence**] and a policy map (for example, **service-policy input** *policy-map-name*) are mutually exclusive. The last one configured overwrites the previous configuration.

Related Commands   This example shows how to configure a port to trust the IP precedence field in the incoming packet:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# mls qos trust ip-precedence
```

This example shows how to specify that the Cisco IP Phone connected on a port is a trusted device:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# mls qos trust device cisco-phone
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

Command	Description
mls qos cos, on page 14	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
mls qos dscp-mutation, on page 16	Applies a DSCP-to DSCP-mutation map to a DSCP-trusted port.
mls qos map, on page 18	Defines the CoS-to-DSCP map, DSCP-to-CoS map, the DSCP-to-DSCP-mutation map, the IP-precedence-to-DSCP map, and the policed-DSCP map.
show mls qos interface, on page 45	Displays QoS information.

police

To define a policer for classified traffic, use the **police** command in policy-map class configuration mode. Use the **no** form of this command to remove an existing policer.

police *rate-bps* *burst-byte* [**exceed-action** [**drop** | **policed-dscp-transmit**]]
no police *rate-bps* *burst-byte* [**exceed-action** [**drop** | **policed-dscp-transmit**]]

Syntax Description	*rate-bps*	Specifies the average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.
	burst-byte	Specifies the normal burst size in bytes. The range is 8000 to 1000000.
	exceed-action drop	(Optional) Sets the traffic rate. If the rate is exceeded, the switch drops the packet .
	exceed-action policed-dscp-transmit	(Optional) Sets the traffic rate. If the rate is exceeded, the switch changes the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then sends the packet.
	aggregate	Chooses the aggregate policer for the current class.

Command Default   No policers are defined.

Command Modes   Policy-map class configuration

Command History	**Release**	**Modification**
	Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines   A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

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

Policing uses a token-bucket algorithm. You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure how quickly (the average rate) the tokens are removed from the bucket by using the *rate-bps* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. For more information, see the software configuration guide for this release.

Examples

This example shows how to configure a policer that drops packets if traffic exceeds 1 Mb/s average rate with a burst size of 20 KB. The DSCPs of incoming packets are trusted, and there is no packet modification.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# trust dscp
Device(config-pmap-c)# police 1000000 20000 exceed-action drop
Device(config-pmap-c)# exit
```

This example shows how to configure a policer, which marks down the DSCP values with the values defined in policed-DSCP map and sends the packet:

```
Device(config)# policy-map policy2
Device(config-pmap)# class class2
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

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

Related Commands

Command	Description
class, on page 2	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.
class-map, on page 4	Create a class map to be used for matching packets to the class whose name you specify with the **class** command.
mls qos map, on page 18 **policed-dscp**	Applies a policed-DSCP map to a DSCP-trusted port.
policy map, on page 36	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
set, on page 40	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map, on page 53	Displays QoS policy maps.

police aggregate

To apply an aggregate policer to multiple classes in the same policy map, use the **police aggregate** command in policy-map class configuration mode. Use the **no** form of this command to remove the specified policer.

police aggregate *aggregate-policer-name*
no police aggregate *aggregate-policer-name*

Syntax Description	*aggregate-policer-name*	The name of the aggregate policer.

Command Default   No aggregate policers are defined.

Command Modes   Policy-map class configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

You set aggregate policer parameters by using the **mls qos aggregate-policer** global configuration command. You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps.

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

You cannot configure aggregate policers in hierarchical policy maps.

Examples   This example shows how to define the aggregate policer parameters and to apply the policer to multiple classes in a policy map:

```
Device(config)# mls qos aggregate-policer agg_policer1 10000 1000000 exceed-action drop
Device(config)# policy-map policy2
Device(config-pmap)# class class1
Device(config-pmap-c)# police aggregate agg_policer1
Device(config-pmap-c)# exit
Device(config-pmap)# class class2
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police aggregate agg_policer1
Device(config-pmap-c)# exit
Device(config-pmap)# class class3
Device(config-pmap-c)# trust dscp
```

```
Device(config-pmap-c)# police aggregate agg_policer2
Device(config-pmap-c)# exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

	Command	Description
Related Commands	mls qos aggregate-policer, on page 12	Defines policer parameters, which can be shared by multiple classes within a policy map.
	show mls qos aggregate-policer, on page 44	Displays the quality of service (QoS) aggregate policer configuration.

policy map

To create or modify a policy map that can be attached to multiple physical ports 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	The name of the policy map.

Command Default

No policy maps are defined.

The default behavior is to set the Differentiated Services Code Point (DSCP) to 0 if the packet is an IP packet and to set the class of service (CoS) to 0 if the packet is tagged. No policing is performed.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	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.

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.

You can configure QoS only on physical ports. Configure the QoS settings, such as classification, queueing, and scheduling, and apply the policy map to a port. When configuring QoS on a physical port, you apply a nonhierarchical policy map to a port. A nonhierarchical policy map is the same as the port-based policy maps in the device.

Examples

This example shows how to create a policy map called *policy1*.

```
Device(config)# policy-map policy1
```

This example shows how to delete *policymap2*:

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

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

Related Commands	Command	Description
	class, on page 2	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration command) for the specified class-map name.
	class-map, on page 4	Creates a class map to be used for matching packets to the class whose name you specify.
	service-policy, on page 39	Applies a policy map to a physical port.
	show policy-map, on page 53	Displays QoS policy maps.

queue-set

To map a port to a queue set, use the **queue-set** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

queue-set *qset-id*
no queue-set *qset-id*

Syntax Description		
	qset-id	Queue-set ID. Each port belongs to a queue set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.

Command Default   The queue set ID is 1.

Command Modes   Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   For information about automatic generation of the queue-set ID with the **auto qos voip** command, see the "Usage Guidelines" section for the auto qos voip command.

Examples   This example shows how to map a port to queue-set 2:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **buffers** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers, on page 19	Allocates buffers to a queue set.
mls qos queue-set output threshold, on page 21	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
show mls qos interface, on page 45	Displays quality of service (QoS) information.

service-policy

To apply a policy map to the input of a physical port, 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*	Applies the specified policy map to the input of a physical port.
Command Default	No policy maps are attached to the port.	
Command Modes	Interface configuration	

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Though visible in the command-line help strings, the **output** keyword is not supported.

Policy maps can be configured on physical ports. 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. .

Classification using a port trust state (for example, **mls qos trust** [**cos** | **dscp** | **ip-precedence**] and a policy map (for example, **service-policy input** *policy-map-name*) are mutually exclusive. The last one configured overwrites the previous configuration.

Examples

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

```
Device(config)# interface gigabitethernet2/0/2
Device(config-if)# no service-policy input plcmap2
```

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

Related Commands

Command	Description
policy map, on page 36	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map, on page 53	Displays QoS policy maps.
show running-config	Displays the operating configuration.

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 {**dscp** *new-dscp* |**ip** {**dscp**|**precedence**}|**precedence** *precedence*}
no **set** {**dscp** *new-dscp* |**ip** {**dscp**|**precedence**}|**precedence** *precedence*}

Syntax Description		
dscp *new-dscp*	Sets the DSCP value in IPv4 and IPv6 packets.	
	The range is 0 to 63.	
ip {**dscp**	**precedence** }	Sets the IP values.	
	• **dscp**—Sets the IP DSCP value.	
	• **precedence**—Sets the IP precedence value.	
precedence *new-precedence*	Sets the precedence in IPv4 and IPv6 packets.	
	The range is 0 to 7.	

Command Default   No traffic classification is defined.

Command Modes   Policy-map class configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   If you have used the **set ip dscp** policy-map class configuration command, the device changes this command to **set dscp** in the device configuration. If you enter the **set ip dscp** policy-map class configuration command, this setting appears as **set dscp** in the device configuration.

You can use the **set ip precedence** policy-map class configuration command or the **set precedence** policy-map class configuration command. This setting appears as **set ip precedence** in the device configuration.

The **set** command is mutually exclusive with the **trust** policy-map class configuration command within the same policy map.

For the **set dscp** *new-dscp* or the **set ip precedence** *new-precedence* 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.

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-map 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.

Related Commands

Command	Description
class, on page 2	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.
police, on page 32	Defines a policer for classified traffic.
policy map, on page 36	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map, on page 53	Displays QoS policy maps.
trust, on page 60	Defines a trust state for traffic classified through the **class** policy-map configuration command or the **class-map** global configuration 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

This command is supported only on the LAN Base image.

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
```

Related Commands

Command	Description
class-map, on page 4	Creates a class map to be used for matching packets to the class whose name you specify.
match (class-map configuration), on page 8	Defines the match criteria to classify traffic.

show mls qos

To display global quality of service (QoS) configuration information, use the **show mls qos** command in EXEC mode.

show mls qos

Syntax Description	This command has no arguments or keywords.

Command Modes   User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Examples

This is an example of output from the **show mls qos** command when QoS is enabled and Differentiated Services Code Point (DSCP) transparency is disabled:

```
Device# show mls qos
QoS is enabled
QoS ip packet dscp rewrite is disabled
```

This is an example of output from the **show mls qos** command when QoS is enabled and DSCP transparency is enabled:

```
Device# show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

Related Commands

Command	Description
mls qos, on page 10	Enables QoS on the entire switch.

show mls qos aggregate-policer

To display the quality of service (QoS) aggregate policer configuration, use the **show mls qos aggregate-policer** command in EXEC mode.

show mls qos aggregate-policer [*aggregate-policer-name*]

Syntax Description	*aggregate-policer-name* (Optional) Displays the policer configuration for the specified name.

Command Modes   User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

This command is supported only on the LAN Base image.

Examples   This is an example of output from the **show mls qos aggregate-policer** command:

```
Device# show mls qos aggregate-policer policer1

aggregate-policer policer1 1000000 2000000 exceed-action drop
Not used by any policy map
```

Related Commands

Command	Description
mls qos aggregate-policer, on page 12	Defines policer parameters that can be shared by multiple classes within a policy map.

show mls qos interface

To display quality of service (QoS) information at the port level, use the **show mls qos interface** command in EXEC mode.

show mls qos interface [*interface-id*] [{**buffers**|**queueing**|**statistics**}]

Syntax Description	*interface-id*	(Optional) The QoS information for the specified port. Valid interfaces include physical ports.
	buffers	(Optional) Displays the buffer allocation among the queues.
	queueing	(Optional) Displays the queueing strategy (shared or shaped) and the weights corresponding to the queues.
	statistics	(Optional) Displays statistics for sent and received Differentiated Services Code Points (DSCPs) and class of service (CoS) values, the number of packets enqueued or dropped per egress queue, and the number of in-profile and out-of-profile packets for each policer.

Command Modes	User EXEC
	Privileged EXEC

Command History	**Release**	**Modification**
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   Though visible in the command-line help string, the **policers** keyword is not supported.

This command is supported only on the LAN Base image.

Examples   This is an example of output from the **show mls qos interface** *interface-id* command when port-based QoS is enabled:

```
Device# show mls qos interface gigabitethernet1/0/1
GigabitEthernet1/0/1
trust state: trust cos
trust mode: trust cos
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based
```

This is an example of output from the **show mls qos interface** *interface-id* command when port-based QoS is disabled:

```
Device# show mls qos interface  gigabitethernet1/0/1
GigabitEthernet1/0/1
QoS is disabled. When QoS is enabled, following settings will be applied
trust state: trust cos
trust mode: trust cos
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based
```

This is an example of output from the **show mls qos interface** *interface-id* **buffers** command:

```
Device# show mls qos interface gigabitethernet1/0/2 buffers
GigabitEthernet1/0/2
The port is mapped to qset : 1
The allocations between the queues are : 25 25 25 25
```

This is an example of output from the **show mls qos interface** *interface-id* **queueing** command. The egress expedite queue overrides the configured shaped round robin (SRR) weights.

```
Device# show mls qos interface gigabitethernet1/0/2 queueing
GigabitEthernet1/0/2
Egress Priority Queue :enabled
Shaped queue weights (absolute) :  25 0 0 0
Shared queue weights  :  25 25 25 25
The port bandwidth limit : 100  (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

This is an example of output from the **show mls qos interface** *interface-id* **statistics** command:

```
Device# show mls qos interface gigabitethernet1/0/1 statistics
GigabitEthernet1/0/1 (All statistics are in packets)

  dscp: incoming
-------------------------------

  0 -   4 :       15233             0             0             0             0
  5 -   9 :           0             0             0             0             0
 10 -  14 :           0             0             0             0             0
 15 -  19 :           0             0             0             0             0
 20 -  24 :           0             0             0             0             0
 25 -  29 :           0             0             0             0             0
 30 -  34 :           0             0             0             0             0
 35 -  39 :           0             0             0             0             0
 40 -  44 :           0             0             0             0             0
 45 -  49 :           0             0             0        406417             0
 50 -  54 :           0             0             0             0             0
 55 -  59 :           0             0             0             0             0
 60 -  64 :           0             0             0             0
  dscp: outgoing
-------------------------------

  0 -   4 :         337             0             0             0             0
  5 -   9 :           0             0             0             0             0
 10 -  14 :           0             0             0             0             0
 15 -  19 :           0             0             0             0             0
 20 -  24 :           0             0             0             0             0
 25 -  29 :           0             0             0             0             0
 30 -  34 :           0             0             0             0             0
 35 -  39 :           0             0             0             0             0
```

```
40 - 44 :              0             0             0             0             0
45 - 49 :              0             0             0         13866             0
50 - 54 :              0             0             0             0             0
55 - 59 :              0             0             0             0             0
60 - 64 :              0             0             0             0
 cos: incoming
-----------------------------

 0 -  4 :        1426270             0             0             0             0
 5 -  7 :              0             0             0
 cos: outgoing
-----------------------------

 0 -  4 :         131687            12             0             0          7478
 5 -  7 :           1993         25483        275213
 output queues enqueued:
queue:    threshold1    threshold2    threshold3
------------------------------------------------
queue 0:              0             0             0
queue 1:              0           341        441525
queue 2:              0             0             0
queue 3:              0             0             0

 output queues dropped:
queue:    threshold1    threshold2    threshold3
------------------------------------------------
queue 0:              0             0             0
queue 1:              0             0             0
queue 2:              0             0             0
queue 3:              0             0             0

Policer: Inprofile:          0 OutofProfile:            0
```

This table describes the fields in this display.

Table 4: show mls qos interface statistics Field Descriptions

Field		Description
DSCP	incoming	Number of packets received for each DSCP value.
	outgoing	Number of packets sent for each DSCP value.
CoS	incoming	Number of packets received for each CoS value.
	outgoing	Number of packets sent for each CoS value.
Output queues	enqueued	Number of packets in the egress queue.
	dropped	Number of packets in the egress queue that are dropped.
Policer	Inprofile	Number of in-profile packets for each policer.
	Outofprofile	Number of out-of-profile packets for each policer.

	Command	**Description**
Related Commands	mls qos queue-set output buffers, on page 19	Allocates buffers to a queue set.
	mls qos queue-set output threshold, on page 21	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
	mls qos srr-queue output cos-map, on page 26	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
	mls qos srr-queue output dscp-map, on page 28	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
	policy map, on page 36	Creates or modifies a policy map.
	queue-set, on page 38	Maps a port to a queue set.
	srr-queue bandwidth limit, on page 54	Limits the maximum output on a port.
	srr-queue bandwidth shape, on page 56	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
	srr-queue bandwidth share, on page 58	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

show mls qos maps

To display quality of service (QoS) mapping information, use the **show mls qos maps** command in EXEC mode.

show mls qos maps [{**cos-dscp|cos-output-q|dscp-cos|dscp-mutation** *dscp-mutation-name*|**dscp-output-q|ip-prec-dscp|policed-dscp**}]

Syntax Description	
cos-dscp	(Optional) Displays class of service (CoS)-to-DSCP map.
cos-output-q	(Optional) Displays the CoS output queue threshold map.
dscp-cos	(Optional) Displays DSCP-to-CoS map.
dscp-mutation *dscp-mutation-name*	(Optional) Displays the specified DSCP-to-DSCP-mutation map.
dscp-output-q	(Optional) Displays the DSCP output queue threshold map.
ip-prec-dscp	(Optional) Displays the IP-precedence-to-DSCP map.
policed-dscp	(Optional) Displays the policed-DSCP map.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

During classification, QoS uses the mapping tables to represent the priority of the traffic and to derive a corresponding class of service (CoS) or Differentiated Services Code Point (DSCP) value from the received CoS, DSCP, or IP precedence value.

The policed-DSCP, DSCP-to-CoS, and the DSCP-to-DSCP-mutation maps appear as a matrix. The d1 column specifies the most-significant digit in the DSCP. The d2 row specifies the least-significant digit in the DSCP. The intersection of the d1 and d2 values provides the policed-DSCP, the CoS, or the mutated-DSCP value. For example, in the DSCP-to-CoS map, a DSCP value of 43 corresponds to a CoS value of 5.

The DSCP output queue threshold maps appear as a matrix. The d1 column specifies the most-significant digit of the DSCP number. The d2 row specifies the least-significant digit in the DSCP number. The intersection of the d1 and the d2 values provides the queue ID and threshold ID. For example, in the DSCP output queue threshold map, a DSCP value of 43 corresponds to queue 1 and threshold 3 (01-03).

The CoS output queue threshold maps show the CoS value in the top row and the corresponding queue ID and threshold ID in the second row. For example, in the CoS output queue threshold map, a CoS value of 5 corresponds to queue 1 and threshold 3 (1-3).

Examples

This is an example of output from the **show mls qos maps** command:

```
Device# show mls qos maps
  Policed-dscp map:
    d1 :  d2 0   1   2   3   4   5   6   7   8   9
    ---------------------------------------
     0 :     00  01  02  03  04  05  06  07  08  09
     1 :     10  11  12  13  14  15  16  17  18  19
     2 :     20  21  22  23  24  25  26  27  28  29
     3 :     30  31  32  33  34  35  36  37  38  39
     4 :     40  41  42  43  44  45  46  47  48  49
     5 :     50  51  52  53  54  55  56  57  58  59
     6 :     60  61  62  63

  Dscp-cos map:
    d1 :  d2 0   1   2   3   4   5   6   7   8   9
    ---------------------------------------
     0 :     00  00  00  00  00  00  00  00  01  01
     1 :     01  01  01  01  01  01  02  02  02  02
     2 :     02  02  02  02  03  03  03  03  03  03
     3 :     03  03  04  04  04  04  04  04  04  04
     4 :     05  05  05  05  05  05  05  05  06  06
     5 :     06  06  06  06  06  06  07  07  07  07
     6 :     07  07  07  07

  Cos-dscp map:
        cos:  0   1   2   3   4   5   6   7
    -------------------------------
       dscp:  0   8  16  24  32  46  48  56

  IpPrecedence-dscp map:
     ipprec:  0   1   2   3   4   5   6   7
    -------------------------------
       dscp:  0   8  16  24  32  40  48  56

  Dscp-outputq-threshold map:
    d1 :d2    0       1       2       3       4       5       6       7       8       9
    ------------------------------------------------------------------
     0 :    03-03  03-03  03-03  03-03  03-03  03-03  03-03  03-03  04-01  04-01
     1 :    04-02  04-01  04-02  04-01  04-02  04-01  02-01  02-01  02-01  02-01
     2 :    02-01  02-01  02-01  02-01  02-02  03-01  02-01  02-01  02-01  02-01
     3 :    02-01  02-01  01-03  01-03  02-01  02-01  02-01  02-01  02-01  02-01
     4 :    01-03  01-03  01-03  01-03  01-03  01-03  01-03  01-03  02-03  02-03
     5 :    02-03  02-03  02-03  02-03  02-03  02-03  02-03  02-03  02-03  02-03
     6 :    02-03  02-03  02-03  02-03

  Cos-outputq-threshold map:
            cos:  0   1   2   3   4   5   6   7
            ---------------------------------
  queue-threshold: 3-3 4-3 2-1 2-2 1-3 1-3 2-3 2-3


  Dscp-dscp mutation map:
  Default DSCP Mutation Map:
    d1 :  d2 0   1   2   3   4   5   6   7   8   9
    ---------------------------------------
     0 :     00  01  02  03  04  05  06  07  08  09
     1 :     10  11  12  13  14  15  16  17  18  19
     2 :     20  21  22  23  24  25  26  27  28  29
     3 :     30  31  32  33  34  35  36  37  38  39
     4 :     40  41  42  43  44  45  46  47  48  49
     5 :     50  51  52  53  54  55  56  57  58  59
     6 :     60  61  62  63
```

Related Commands

Command	Description
mls qos map, on page 18	Defines the CoS-to-DSCP map, DSCP-to-CoS map, DSCP-to-DSCP-mutation map, IP-precedence-to-DSCP map, and the policed-DSCP map.
mls qos srr-queue output cos-map, on page 26	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map, on page 28	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.

show mls qos queue-set

To display quality of service (QoS) settings for the egress queues, use the **show mls qos queue-set** command in EXEC mode.

show mls qos queue-set [*gset-id*]

Syntax Description	*qset-id* (Optional) Queue set ID. Each port belongs to a queue set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Examples

This is an example of output from the **show mls qos queue-set** command:

```
Device# show mls qos queue-set
Queueset: 1
Queue   :       1       2       3       4
---------------------------------------------
buffers  :      25      25      25      25
threshold1:     100     200     100     100
threshold2:     100     200     100     100
reserved :      50      50      50      50
maximum  :      400     400     400     400
Queueset: 2
Queue   :       1       2       3       4
---------------------------------------------
buffers  :      25      25      25      25
threshold1:     100     200     100     100
threshold2:     100     200     100     100
reserved :      50      50      50      50
maximum  :      400     400     400     400
```

Related Commands

Command	Description
mls qos queue-set output buffers, on page 19	Allocates buffers to the queue set.
mls qos queue-set output threshold, on page 21	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation of the queue set.

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*]

Syntax Description	*policy-map-name* (Optional) The policy map name.

Command Modes
User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

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 **session**,**type**,**control-plane**, and **interface** keywords are not supported; statistics shown in the display should be ignored.

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

```
Device# show policy-map
Policy Map videowizard_policy2
  class  videowizard_10-10-10-10
    set dscp 34
    police 100000000 2000000 exceed-action drop

 Policy Map mypolicy
  class  dscp5
    set dscp 6
```

Related Commands

Command	Description
policy map, on page 36	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.

srr-queue bandwidth limit

To limit the maximum output on a port, use the **srr-queue bandwidth limit** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth limit *weight1*
no srr-queue bandwidth limit

Syntax Description

weight1	The port speed limit in percentage terms. The range is 10 to 90.

Command Default

The port is not rate limited and is set to 100 percent.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

If you configure this command to 80 percent, the port is idle 20 percent of the time. The line rate drops to 80 percent of the connected speed. These values are not exact because the hardware adjusts the line rate in increments of six.

Examples

This example shows how to limit a port to 800 Mb/s:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# srr-queue bandwidth limit 80
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **queueing** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers, on page 19	Allocates buffers to the queue set.
mls qos srr-queue output dscp-map, on page 28	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold, on page 21	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation for the queue set.
queue-set, on page 38	Maps a port to a queue set.
show mls qos interface, on page 45	Displays QoS information.
srr-queue bandwidth shape, on page 56	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.

Command	Description
srr-queue bandwidth share, on page 58	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth shape

To assign the shaped weights and to enable bandwidth shaping on the four egress queues mapped to a port, use the **srr-queue bandwidth shape** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth shape *weight1 weight2 weight3 weight4*
no srr-queue bandwidth shape

Syntax Description	

weight1 weight2 weight3 weight4	The weights that specify the percentage of the port that is shaped. The inverse ratio (1/*weight*) specifies the shaping bandwidth for this queue. Separate each value with a space. The range is 0 to 65535.

Command Default   Weight1 is set to 25; weight2, weight3, and weight4 are set to 0, and these queues are in shared mode.

Command Modes   Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   In shaped mode, the queues are guaranteed a percentage of the bandwidth, and they are rate-limited to that amount. Shaped traffic does not use more than the allocated bandwidth even if the link is idle. Use shaping to smooth bursty traffic or to provide a smoother output over time.

The shaped mode overrides the shared mode.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue come into effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.

Note   The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Examples   This example shows how to configure the queues for the same port for both shaping and sharing. Queues 2, 3, and 4 operate in the shared mode, because the weight ratios for these queues are set to 0. The bandwidth weight for queue 1 is 1/8, which is 12.5 percent. Queue 1 is guaranteed this bandwidth and limited to it; it does not extend its slot to the other queues even if the other queues have no traffic and are idle. Queues 2, 3, and 4 are in shared mode, and the setting for queue 1 is ignored. The bandwidth ratio allocated for the queues in shared mode is 4/(4+4+4), which is 33 percent:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# srr-queue bandwidth shape 8 0 0 0
Device(config-if)# srr-queue bandwidth share 4 4 4 4
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **queueing** privileged EXEC command.

Related Commands	Command	Description
	mls qos queue-set output buffers, on page 19	Allocates buffers to a queue set.
	mls qos srr-queue output dscp-map, on page 28	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
	mls qos queue-set output threshold, on page 21	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
	queue-set, on page 38	Maps a port to a queue set.
	show mls qos interface, on page 45	Displays QoS information.
	srr-queue bandwidth share, on page 58	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth share

To assign the shared weights and to enable bandwidth sharing on the four egress queues mapped to a port, use the **srr-queue bandwidth share** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth share *weight1 weight2 weight3 weight4*
no srr-queue bandwidth share

Syntax Description	*weight1 weight2 weight3 weight4*	The ratios of *weight1*, *weight2*, *weight3*, and *weight4* specify the ratio of the frequency in which the SRR scheduler dequeues packets. Separate each value with a space. The range is 1 to 255.

Command Default Equal bandwidth is allocated to each queue (Equal bandwidth for weight1, weight2, weight3, and weight4).

Command Modes Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines The ratio of the weights is the ratio of frequency in which the shaped round-robin (SRR) scheduler dequeues packets from each queue.

The absolute value of each weight is meaningless, and only the ratio of parameters is used.

In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue empties and does not require a share of the link, the remaining queues can expand into the unused bandwidth and share it among themselves.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in SRR shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue take effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.

Note The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Examples This example shows how to configure the weight ratio of the SRR scheduler running on an egress port. Four queues are used. The bandwidth ratio allocated for each queue in shared mode is 1/(1+2+3+4), 2/(1+2+3+4), 3/(1+2+3+4), and 4/(1+2+3+4), which is 10 percent, 20 percent, 30 percent, and 40 percent for queues 1, 2, 3, and 4. This means that queue 4 has four times the bandwidth of queue 1, twice the bandwidth of queue 2, and one-and-a-third times the bandwidth of queue 3.

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# srr-queue bandwidth share 1 2 3 4
```

You can verify your settings by entering the **show mls qos interface** [*interface-id* **queueing**] privileged EXEC command.

	Command	Description
Related Commands	mls qos queue-set output buffers, on page 19	Allocates buffers to a queue set.
	mls qos queue-set output threshold, on page 21	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
	mls qos srr-queue output dscp-map, on page 28	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
	queue-set, on page 38	Maps a port to a queue set.
	show mls qos interface, on page 45	Displays quality of service (QoS) information.
	srr-queue bandwidth shape, on page 56	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.

trust

To define a trust state for traffic classified through the **class** policy-map configuration or the **class-map** global configuration command, use the **trust** command in policy-map class configuration mode. Use the **no** form of this command to return to the default setting.

trust [{**cos|dscp|ip-precedence**}]
no trust [{**cos|dscp|ip-precedence**}]

Syntax Description

cos	(Optional) Classifies an ingress packet by using the packet class of service (CoS) value. For an untagged packet, the port default CoS value is used.
dscp	(Optional) Classifies an ingress packet by using the packet Differentiated Services Code Point (DSCP) values (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP.
ip-precedence	(Optional) Classifies an ingress packet by using the packet IP-precedence value (most significant 3 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the port default CoS value is used to map CoS to DSCP.

Command Default   The action is not trusted. If no keyword is specified when the command is entered, the default is **dscp**.

Command Modes   Policy-map class configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines   Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from other traffic. For example, incoming traffic with certain DSCP values can be trusted. You can configure a class map to match and trust the DSCP values in the incoming traffic.

Trust values set with this command supersede trust values set with the **mls qos trust** interface configuration command.

The **trust** command is mutually exclusive with **set** policy-map class configuration command within the same policy map.

If you specify **trust cos**, QoS uses the received or default port CoS value and the CoS-to-DSCP map to generate a DSCP value for the packet.

If you specify **trust dscp**, QoS uses the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP value for the packet is derived from the CoS-to-DSCP map.

If you specify **trust ip-precedence**, QoS uses the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP

packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP for the packet is derived from the CoS-to-DSCP map.

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 define a port trust state to trust incoming DSCP values for traffic classified with a default class:

```
Device(config)# policy-map policy1
Device(config-pmap)# class class-default
Device(config-pmap-c)# trust dscp
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

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

Related Commands

Command	Description
class, on page 2	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration command) for the specified class-map name.
police, on page 32	Defines a policer for classified traffic.
policy map, on page 36	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
set, on page 40	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map, on page 53	Displays QoS policy maps.

trust