

Chapter 27

Quality of Service (QoS)

What is Quality of Service?	27-3
QoS Operations	27-3
Packet Flow through the Switch	27-4
Packet Flow for Accelerated IPv6 Traffic	27-8
QoS and the Switching Fabric	27-11
Storm Protection	27-12
Filtering Actions	27-13
QoS Entities	27-15
Classifiers	27-15
Flow Groups	27-15
Traffic Classes	27-16
QoS Policies	27-18
RED Curves	27-19
Port Groups	27-21
QoS Processes	27-23
Premarking	27-23
Bandwidth Metering	27-24
Re-Marking	27-27
Replacing Priorities on Egress	27-29
Scheduling Queues	27-31
Configuring QoS on the Switch	27-32
Rules for QoS Configuration	27-32
Overview of Procedure	27-32
Configuring QoS for Accelerated IPv6 Traffic	27-34
DiffServ Domains	27-36
Layer 2 Priority-Based QoS	27-39
Configuration Examples	27-40
Command Reference	27-42
add qos flowgroup	27-42
add qos policy	27-43
add qos portgroup port	27-44
add qos trafficclass	27-45
create qos flowgroup	27-46
create qos policy	27-48
create qos portgroup	27-53
create qos red	27-54
create qos trafficclass	27-55
delete qos flowgroup	27-61
delete qos policy	27-62
delete qos portgroup port	27-63
delete qos trafficclass	27-64

destroy qos flowgroup	27-65
destroy qos policy	27-66
destroy qos portgroup	27-66
destroy qos red	27-67
destroy qos trafficclass	27-68
disable qos debug	27-69
enable qos debug	27-69
purge qos	27-70
reset qos accelerator counters	27-70
reset qos port counters	27-71
reset qos portgroup counters	27-72
set qos accelerator policy	27-73
set qos defaultpriority	27-73
set qos dscpmap	27-74
set qos fabric queue	27-76
set qos fabric queuemap	27-77
set qos flowgroup	27-78
set qos policy	27-80
set qos port	27-85
set qos port egressqueue	27-87
set qos portgroup	27-89
set qos prio2queuemap	27-90
set qos red	27-90
set qos trafficclass	27-93
show qos accelerator counters	27-98
show qos defaultpriority	27-100
show qos dscpmap	27-101
show qos fabric	27-103
show qos flowgroup	27-104
show qos policy	27-106
show qos port	27-109
show qos port counters	27-112
show qos portgroup	27-114
show qos portgroup counters	27-115
show qos prio2queuemap	27-117
show qos red	27-118
show qos trafficclass	27-122

What is Quality of Service?

Quality of Service (QoS) is a term that encompasses both Layer 2 and Layer 3 in the OSI model and refers to the ability to intelligently manage network traffic to provide stable and predictable end-to-end network performance. The concept of QoS is a departure from the original networking protocols that treat all traffic on the Internet or within a LAN the same. Without QoS, every different traffic type is equally likely to be dropped when a link becomes oversubscribed. With QoS, certain types of traffic can be given preferential treatment. QoS is important to control congestion.

Business benefits

Quality of Service mechanisms allow:

- traditional voice and data carriers to effectively compete against aggressive competition from wireless, satellite, and cable providers through the ability to integrate and deliver voice, video, and data services over the existing copper infrastructure
- network service providers to sell different levels of service to customers, based on what customers require, and be confident in their ability to guarantee the reliable delivery of these services
- enterprise and educational organisations to actively manage and provide many services across one network, for example live video streaming and standard data services, with preferential treatment given for mission-critical traffic
- network administrators to manage network congestion as network traffic levels increase and time-critical applications, such as streaming media, become more widely in demand by customers and organisations

QoS stages

Configuring Quality of Service involves two separate stages that are described in different chapters of this Software Reference. The following table explains the stages and where to find information.

Stage	Description	Where to look
1	Classifying traffic into flows, according to a wide range of criteria. Classification is performed by the switch's packet classifier.	Chapter 26, Generic Packet Classifier
2	Approaches, methods, and commands for acting on traffic flows.	this chapter

QoS Operations

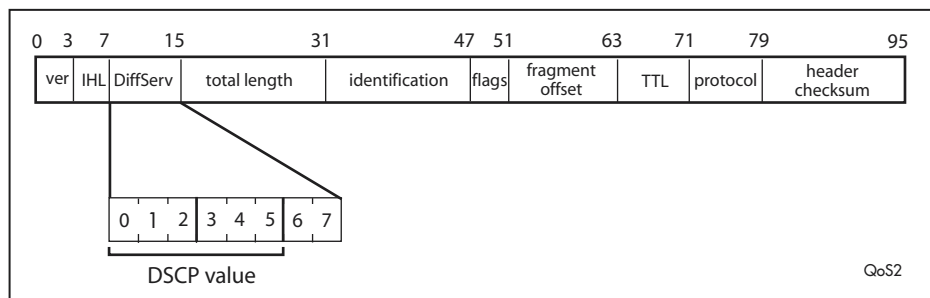
Quality of Service is typically based on how the switch does the following:

- assigns priority to incoming frames if they do not already carry priority information
- correlates prioritised frames with traffic classes, or maps frames to traffic classes based on other criteria
- correlates traffic classes with egress queues, or maps prioritised frames to egress queues
- provides minimum and maximum bandwidth guarantees for traffic classes, egress queues, and/or ports
- schedules frames in egress queues for transmission (for example, empty queues in strict priority or sample each queue)

- re-labels the priority of outgoing frames
- determines which frames to drop or re-queue if the network becomes congested
- reserves memory for switching/routing or QoS operation (for example, reserving buffers for egress queues or buffers to store packets with particular characteristics)

QoS features comprise a tool set for performing a range of QoS applications. These applications include configuring a Differentiated Services (DiffServ) domain. Routers within a DiffServ domain process traffic on the basis of the DSCP (DiffServ Code Point) value in the IP header's Differentiated Services (DS) field ([Figure 27-1](#)).

Figure 27-1: The DSCP bits of the DS field in the IPv4 header



Note that the Differentiated Services field supersedes the IPv4 Type of Service (TOS) field and the IPv6 Traffic Class field. For more information about DiffServ, see [“DiffServ Domains” on page 27-36](#) and RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

Packet Flow through the Switch

[Figure 27-2](#) and [Figure 27-3](#) on [page 27-6](#) show the flow of a packet through the switch's QoS engine. For reference, [Figure 27-2](#) includes points where the switch determines whether the packet is to be bridged (Layer 2 switched) or routed (Layer 3 switched). For a description of the numbered stages, refer to [Table 27-1 on page 27-6](#).

Figure 27-2: Packet flow through the QoS engine

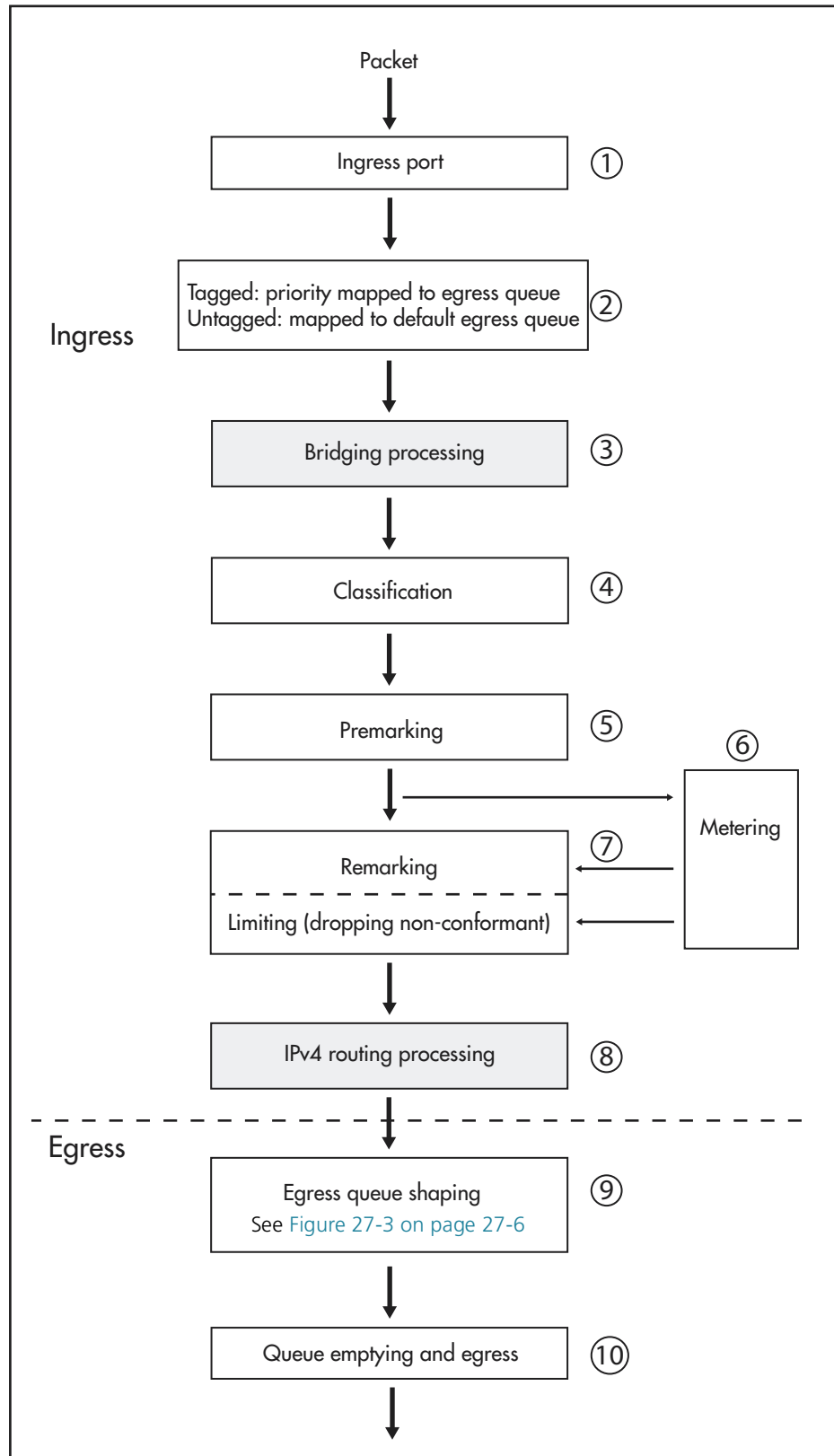


Figure 27-3: Details of egress queue shaping from Figure 27-2 on page 27-5

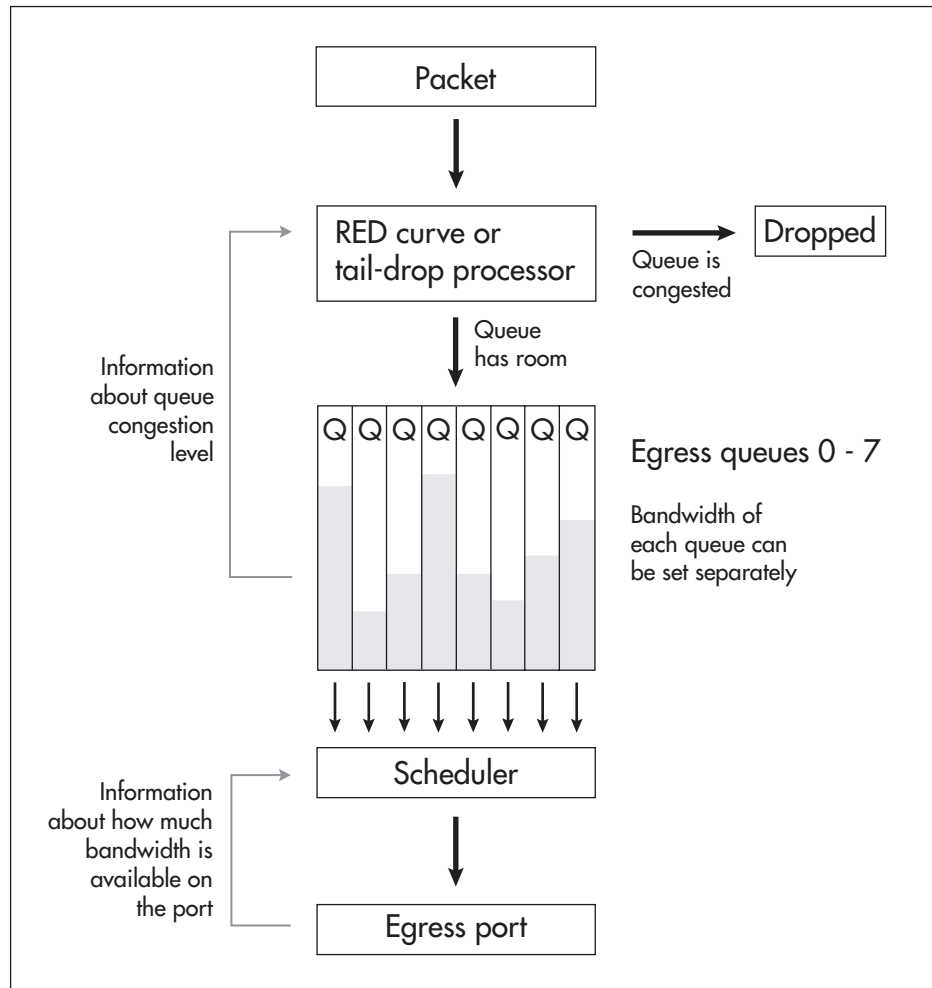


Table 27-1: Stages in QoS packet processing

Stage	Description	For more information see
1	The packet arrives at the ingress port.	"Switch Ports" on page 7-5 of Chapter 7, Switching.
2	For tagged packets, the switch maps the packet's initial VLAN tag User Priority value to an egress queue. For untagged packets, the switch assigns the packet to the default queue.	"To enable Layer 2 QoS" on page 27-39.
3	The switch determines whether the packet is to be bridged (Layer 2 switched) or routed (Layer 3 switched). If it is to be bridged, the switch determines its destination port or ports.	"The Layer 2 Switching Process" on page 7-34 of Chapter 7, Switching.
4	The switch classifies the packet. Classification sorts traffic into data flows.	Chapter 26, Generic Packet Classifier.
5	If you configure <i>premarking</i> , the switch replaces one or both of the packet's initial DSCP or VLAN tag User Priority values, or assigns the packet to a bandwidth class or an egress queue.	"Premarking" on page 27-23.

Table 27-1: Stages in QoS packet processing (cont.)

Stage	Description	For more information see
6	If you configure <i>metering</i> , the switch measures how much bandwidth the packet uses. From this, it determines whether the packet conforms to the bandwidth specifications of the data flow to which the packet belongs.	“Bandwidth Metering” on page 27-24.
7	If you configure <i>remarking</i> , the switch re-marks the packet as a result of the metering. Like premarking, re-marking involves changing one or both of the packet's DSCP or VLAN tag User Priority values, or assigning the packet to a bandwidth class or an egress queue. If you configure dropping bandwidth class 3, the switch discards the packet if it does not conform to the bandwidth specifications of the data flow.	“Re-Marking” on page 27-27, and the dropbwclass3 parameter of the create qos trafficclass command on page 27-55.
8	The switch determines whether the packet is to be routed (Layer 3 switched) and if so, its destination port or ports.	Chapter 13, Internet Protocol (IP) for information about IP.
9	The packet is transmitted over the switching fabric. As the packet egresses the switching fabric, the fabric queue scheduler empties the queues according to the default or configured scheme.	“QoS and the Switching Fabric” on page 27-11. The scheduler parameter of the set qos fabric queue command on page 27-76.
10	The switch determines whether the appropriate egress queue has room for the packet. If the queue has room, the switch puts the packet in that queue. If the queue is congested, the switch may discard the packet instead, according to the default tail drop scheme or the configured RED curve or tail drop scheme.	“RED Curves” on page 27-19, “Tail-drop discarding scheme” on page 27-21, and the set qos port egressqueue command on page 27-87. A diagram of this stage in Figure 27-3 on page 27-6.
11	The egress queue scheduler empties the queues according to the default or configured scheme, and at a rate that does not exceed the bandwidth available at the egress port. The packet leaves the egress port.	The scheduler parameter of the set qos port egressqueue command on page 27-87. The egresslimit parameter of the set switch port command on page 7-106 of Chapter 7, Switching to limit the port's bandwidth. A diagram of this stage in Figure 27-3 on page 27-6.

Important If you apply QoS to traffic that crosses switch instance boundaries, you may see a reduction in QoS performance during congested conditions. A *switch instance* refers to a single switch chip.

Packet Flow for Accelerated IPv6 Traffic

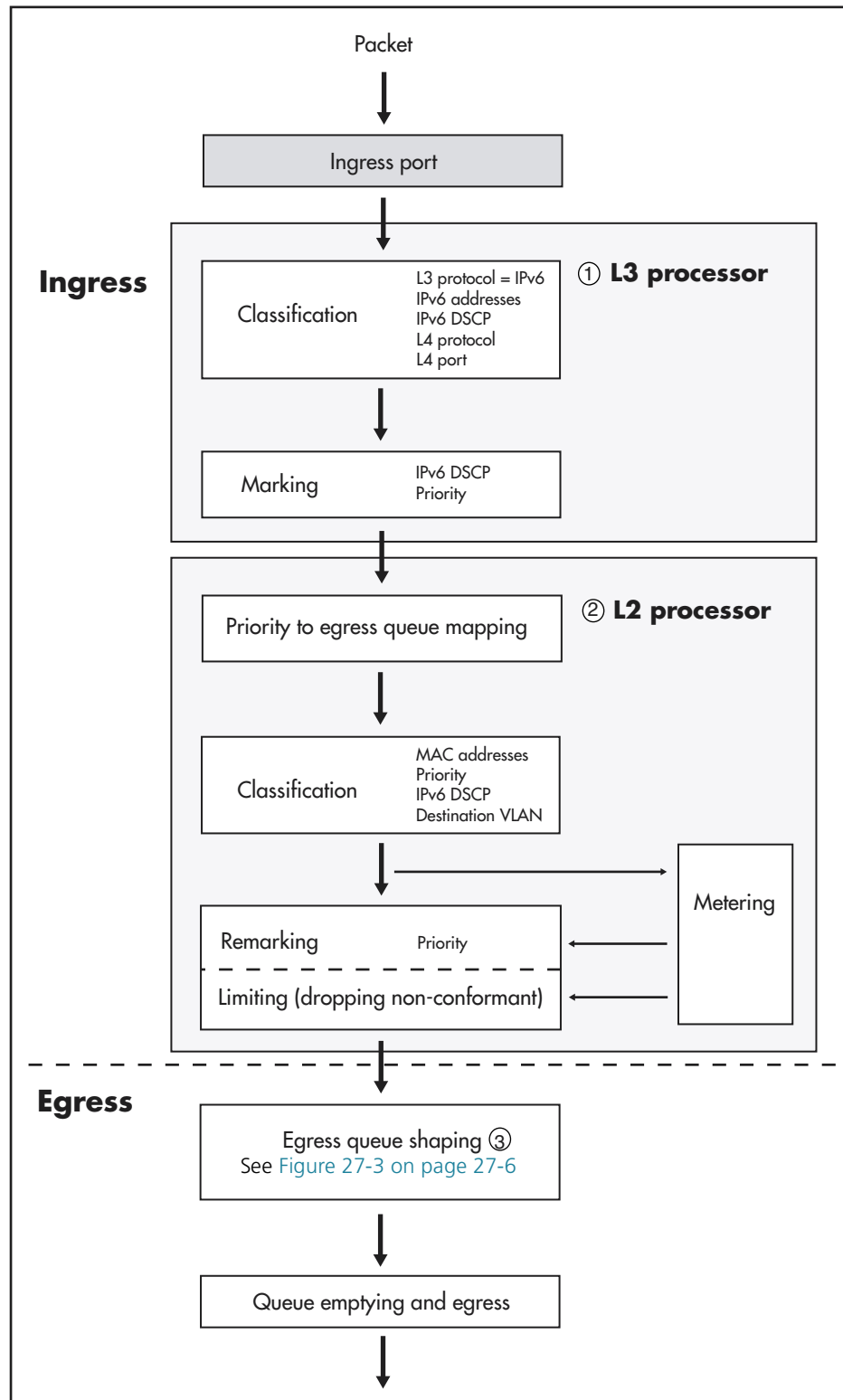
You can install accelerator cards on AT-8948 and AT-9924T/4SP switches. This lets you do the following:

- deliver IPv6 services in real-time that are sensitive to delay and packet loss, such as voice and video
- offer different levels of service to customers, and guarantee minimum and maximum data rates for both IPv4 and IPv6
- meet SLA requirements and enforce compliance with SLAs
- maximise network resources
- prioritise mission-critical traffic, increasing network reliability

An AT-ACC01 network processor accelerator card expedites routed IPv6 unicast and multicast packets on AT-8948 and AT-9924T/4SP switches. When the switch receives an IPv6 packet to route, it sends the packet to the accelerator card. The card processes the packet, makes alterations, and sends it out the correct switch port. For more information about IPv6 and accelerated IPv6 traffic, see [Chapter 23, Internet Protocol version 6 \(IPv6\)](#).

[Figure 27-4 on page 27-9](#) and [Figure 27-3 on page 27-6](#) detail the flow of a packet through the QoS engine on the accelerator card and the switch. For a description of the numbered stages, refer to [Table 27-1](#)

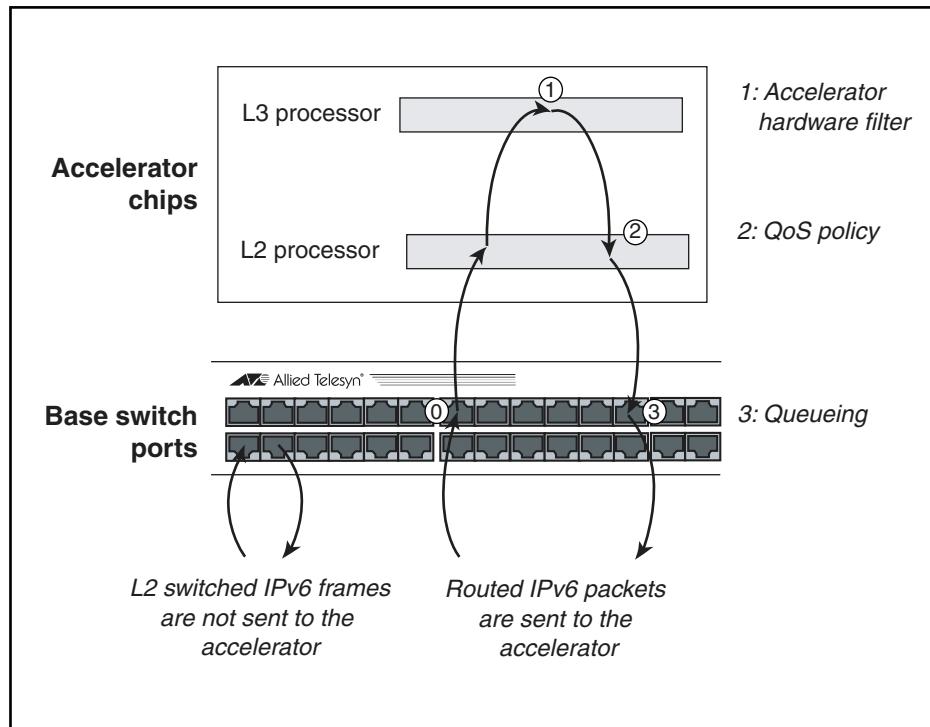
Figure 27-4: Packet flow through the IPv6 accelerator card processors



QoS functionality is performed on accelerated IPv6 traffic at the following processing points:

- Layer 3 processor on the accelerator card (position 1 in Figure 27-5)
- Layer 2 processor on the accelerator card (position 2 in Figure 27-5)
- Egress port on the switch (position 3 in Figure 27-5)

Figure 27-5: QoS processing points on a switch with an accelerator card



Note that metering and bandwidth control are applied separately to Layer 2 switched packets and Layer 3 accelerated packets. This is because IPv6 packets that are Layer 2 switched are not sent to the accelerator card.

Stages in the following table correlate to processing points in [Figure 27-5](#).

Table 27-2: Stages in packet processing for accelerated IPv6 traffic

Stage	Description	For more information see
0	The packet arrives at the ingress port.	"Switch Ports" on page 7-5 of Chapter 7, Switching.
1	The switch sends each IPv6 packet that it is routing to the accelerator card. The Layer 3 processor on the card classifies the packet to sort it into a data flow. You can configure the processor to classify traffic according to a number of Layer 3 and 4 characteristics. Valid options are shown in Figure 27-4 .	Chapter 26, Generic Packet Classifier .
	If you configure <i>marking</i> , the Layer 3 processor replaces the packet's IPv6 DSCP value or VLAN tag User Priority.	"Classifier-Based Filters with Accelerated IPv6 Traffic" on page 7-41 of Chapter 7, Switching.

Table 27-2: Stages in packet processing for accelerated IPv6 traffic (cont.)

Stage	Description	For more information see
2	The Layer 3 processor sends the packet to the Layer 2 processor on the card. The Layer 2 processor maps the packet's current VLAN tag User Priority value to an egress queue.	show qos prio2queuemap command on page 27-117.
	The Layer 2 processor classifies the packet to sort it into a data flow. You can configure the processor to classify traffic according to a number of Layer 2 characteristics or IPv6 DSCP. Valid options are shown in Figure 27-4 .	Chapter 26, Generic Packet Classifier .
	If you configure <i>metering</i> , the Layer 2 processor measures how much bandwidth the packet uses. From this, it determines whether the packet conforms to the bandwidth specifications of the data flow to which the packet belongs.	"Bandwidth Metering" on page 27-24 .
	If you configure <i>remarking</i> , the Layer 2 processor replaces the packet's VLAN tag User Priority. If you configure <i>dropping</i> bandwidth class 3, the Layer 2 processor discards the packet if it does not conform to the bandwidth specifications of the data flow.	"Re-Marking" on page 27-27 , and the dropbwclass3 parameter of the create qos trafficclass command on page 27-55 .
3	The switch determines whether the appropriate egress queue has room for the packet. If the queue has room, the switch puts the packet in it. If the queue is congested, the switch may discard the packet instead, according to the default tail drop scheme or the configured RED curve or tail drop scheme. This processing stage is the same for IPv6 packets (both Layer 2 switched or accelerated) and non-IPv6 packets. For a diagram of this stage, see Figure 27-3 on page 27-6 .	"RED Curves" on page 27-19 , "Tail-drop discarding scheme" on page 27-21 , and the set qos port egressqueue command on page 27-87 .
	The Egress Queue Scheduler empties the queues according to the default or configured scheme, at a rate that does not exceed the bandwidth available at the egress port. The packet leaves out the egress port.	The scheduler parameter of the set qos port egressqueue command on page 27-87 .
	This processing stage is the same for IPv6 (both Layer 2 switched or accelerated) and non-IPv6 packets.	The egresslimit parameter of the set switch port command on page 7-106 of Chapter 7, Switching , to limit the port's bandwidth. A diagram of this stage in Figure 27-3 on page 27-6 .

QoS and the Switching Fabric

Ports on the x900-24X switch belong to one of four switch instances: two on the main board and one on each expansion module. Switch instances exchange packets over a switching fabric. The switching fabric understands the priorities assigned to each packet and performs QoS queuing.

The switching fabric is different from the switch instance in that the fabric has four queues, whereas each switch port in a switch instance has eight egress queues. These two types of queues must be mapped to each other. To specify which fabric queues should exchange packets with the eight egress queues on each switch port, use the command:

```
set qos fabric queuemap=q0,q1,q2,q3,q4,q5,q6,q7
```

The integers *q0* to *q7* indicate the fabric queue that corresponds to an egress queue.

You can also configure the switching fabric to use different scheduling methods for each of the four fabric queues. This controls the way that fabric queues share the available bandwidth during congested times. To set a scheduling method for the fabric queues, use the command:

```
set qos fabric queue={queue-list|all}
[scheduler={strict|wrr}] [wrrweight=1..30]
```

For details about scheduling methods, see [“Scheduling Queues” on page 27-31](#).

To display information about settings for the switching fabric, use the command:

```
show qos fabric
```

Storm Protection

Storm protection uses QoS mechanisms to classify on traffic likely to cause a packet storm (broadcast and multicast). With a per-port storm protection mechanism, any traffic over the configured limit is discarded. However, with QoS storm protection, several actions are possible when a storm is detected:

- You can disable the port physically.
- You can disable the port logically.
- You can disable the port for a particular VLAN.

Enhanced mode must be enabled with the [set switch enhancedmode command on page 7-103 of Chapter 7, Switching](#) before you can configure storm protection. When a storm is detected on a port, a message is automatically recorded in the log, and you can configure an SNMP trap to signal that a port has been disabled. When a storm is detected on a trunk or port group, the entire trunk or port group is disabled.

The following table explains the basic concepts involved with storm protection.

Concept	Description
Window	The frequency at which traffic is measured to determine whether storm protection should be activated.
Rate	The amount of traffic per second that must be exceeded before the switch takes the configured action.
Action	What the switch does when it detects a storm on a port.
Timeout	The length of time the port remains disabled after a port has been disabled due to a packet storm.

To create a policy and enable storm protection on its default traffic class (DTC) processes, use the command:

```
create qos policy=id-list [dtcstormstatus={enable|disable}]
[dtcstormwindow={window-size|none}]
[dtcstormrate={rate|none}]
[dtcstormaction={linkdown|portdisable}]
[dtcstormtimeout={timeout-length|none}]
[other-parameters]
```

To change storm protection parameters for the DTC of a policy, use the command:

```
set qos policy=id-list [dtcstormstatus={enable|disable}]
[dtcstormwindow={window-size|none}]
[dtcstormrate={rate|none}]
[dtcstormaction={linkdown|portdisable}]
[dtcstormtimeout={timeout-length|none}]
[other-parameters]
```

To see information about storm protection enabled on the DTC of a policy, use the command:

```
show qos policy [= {id|all}]
```

To enable storm protection on a traffic class when you create one, use the command:

```
create qos trafficclass=trafficclass-list
[stormstatus={enable|disable}]
[stormwindow={window-size|none}] [stormrate={rate|none}]
[stormaction={linkdown|portdisable|vlandisable}]
[stormtimeout={timeout-length|none}]
[other-parameters]
```

To change storm protection parameters for a traffic class, use the command:

```
set qos trafficclass=trafficclass-list
[stormstatus={enable|disable}]
[stormwindow={window-size|none}]
[stormrate={rate|none}]
[stormaction={linkdown|portdisable|vlandisable}]
[stormtimeout={timeout-length|none}]
[other-parameters]
```

To see information about storm protection enabled on a traffic class, use the command:

```
show qos trafficclass [= {id|all}]
```

Filtering Actions

Options in **create** and **set** commands redirect traffic that has been classified into flow groups and traffic classes. The following types of filtering are possible:

- forward normally
- discard
- send to a preconfigured mirror port
- send to a port on a VLAN
- none

Possible combinations are shown in the following table.

	Forward	Discard	SendMirror	SendVlanPort
Forward		N	Y	N
Discard	N		N	N
SendMirror	Y	N		Y
SendVlanPort	N	N	Y	

An action set on a flow group takes precedence over one set on a traffic class. For more information and configuration examples, see *How To Configure Filtering Actions on QoS Flow Groups and Traffic Classes* at www.alliedtelesis.co.uk/en-gb/solutions/techdocs.asp?area=howto. This How To note is also in the Resource Center on your Documentation & Tools CD.

To redirect classified traffic at the flow group level, use one of the commands:

```
create qos flowgroup=id-list
  action={none|forward|forward,sendmirror|discard|
  sendmirror|sendmirror,sendvlanport|sendvlanport}
  [vlan=vlan-id] [port=port] [other-options]

set qos flowgroup=id-list
  action={none|forward|forward,sendmirror|discard|
  sendmirror|sendmirror,sendvlanport|sendvlanport}
  [vlan=vlan-id] [port=port] [other-options]
```

By setting a flow group action to **none**, traffic classified into it is treated the same as the action for the flow group's associated traffic class.

To redirect classified traffic at the traffic class level, use one of the commands:

```
create qos trafficclass=id-list
  action={forward|forward,sendmirror|discard|sendmirror|
  sendmirror,sendvlanport|sendvlanport} [vlan=vlan-id]
  [port=port] [other-options]

set qos trafficclass=id-list
  action={forward|forward,sendmirror|discard|sendmirror|
  sendmirror,sendvlanport|sendvlanport} [vlan=vlan-id]
  [port=port] [other-options]
```

The actions have the same effect as the flow group actions except that **action=none** is not valid.

To redirect unclassified traffic, which is then processed by the default traffic class (DTC), use one of the commands:

```
create qos policy=id-list
  dtcaction={forward|forward,sendmirror|discard|sendmirror|
  sendmirror,sendvlanport|sendvlanport} [vlan=vlan]
  [port=port] [other-options]

set qos policy=id-list
  dtcaction={forward|forward,sendmirror|discard|sendmirror|
  sendmirror,sendvlanport|sendvlanport} [vlan=vlan]
  [port=port] [other-options]
```

The DTC actions have the same effect as the flow group actions except that **dtcaction=none** is not valid.

QoS Entities

This section describes the following entities:

- [Classifiers](#)
- [Flow Groups](#)
- [Traffic Classes](#)
- [QoS Policies](#)
- [RED Curves](#)
- [Port Groups](#)

Classifiers

Classifiers identify a particular traffic flow and range from general to specific. To create a classifier, use the command:

```
create classifier
```

For details about how to configure classifiers, see [Chapter 26, Generic Packet Classifier](#).

To assign classifiers to a flow group, use the command:

```
add qos flowgroup=flowgroup-id classifier=classifier-list
```

To delete one or more classifiers from a flow group, use the command

```
delete qos flowgroup=flowgroup-id  
classifier={classifier-list|all}
```

Flow Groups

Flow groups let you collect similar traffic together. They consist of a small set of QoS parameters and a group of classifiers. You achieve "per flow" QoS by classifying traffic into flow groups and then performing QoS on that group. Flow groups enable more precise control than what the traffic class specifies. For example, you can specify that traffic be forwarded, discarded, sent from a port on a specific VLAN, and sent to a configured mirror port. For more information, see ["Configuration Examples" on page 27-40](#).

You can add a flow group to only one traffic class. However, a traffic class can have many flow groups. Traffic is matched in order of flow group identifier, beginning from the lowest ID. A maximum of 1024 flow groups are supported, numbered from 0 to 1023.

Controls at the flow group level provide a QoS hierarchy. Non-default flow group settings are always used. But when no setting is specified for a flow group, it uses settings for the traffic class to which it belongs. For example, you can use a traffic class to limit the bandwidth available to web and FTP traffic combined. Within that traffic class, you can create two different flow groups with different priorities in order to give web traffic a higher priority than FTP. Web traffic would then be given preferential access to bandwidth, but would be limited to the bandwidth limit of the traffic class.

To create a flow group, use the command:

```
create qos flowgroup=flowgroup-list [action={none|forward|
forward,sendmirror|discard|discard,sendmirror|sendmirror|
sendmirror,sendvlanport|sendvlanport}]
[description=description] [markvalue={dscp-value|none}]
[port=port] [premarking={usemarkvalue|usedscp|none}]
[vlan=vlan-id]
```

To modify the properties of a flow group, use the command:

```
set qos flowgroup=flowgroup-list [action={none|forward|
forward,sendmirror|discard|discard,sendmirror|sendmirror|
sendmirror,sendvlanport|sendvlanport}]
[description=description] [markvalue={dscp-value|none}]
[port=port] [premarking={usemarkvalue|usedscp|none}]
[vlan=vlan-id]
```

To assign flow groups to a traffic class, use the command:

```
add qos trafficclass=trafficclass-id flowgroup=flowgroup-list
```

To delete a flow group from a traffic class, use the command:

```
delete qos trafficclass=trafficclass-id
flowgroup={flowgroup-list|all}
```

To display configuration information for one or more flow groups, use the command:

```
show qos flowgroup[={id|all}]
```

Traffic Classes

Traffic classes are the central component of QoS and provide most of the controls in QoS. They consist of a set of QoS parameters and a group of *flow groups*. A maximum of 1024 traffic classes are supported, numbered from 0 to 1023. A traffic class can be assigned to only one policy, and other policies cannot use it. Traffic is matched in order of traffic class identifier, beginning from the lowest numbered traffic class. Note that you must apply the traffic class's policy to a port before the switch can check that the maximum bandwidth is available to this traffic class.

You can explicitly redirect traffic—forward, discard, send it out a port on a specific VLAN, and send to a preconfigured mirror port. For more information, see [“Configuration Examples” on page 27-40](#).

To create a traffic class, use the command:

```
create qos trafficclass=id-list [action={forward|
forward,sendmirror|discard|discard,sendmirror|sendmirror|
sendmirror,sendvlanport|sendvlanport}]
[description=description] [dropbwclass3={off|no|false|on|
yes|true}] [ignorebwclass3={off|no|false|on|yes|true}]
[markvalue={dscp-value|none}] [maxbandwidth={bandwidth|
none}] [maxburstsize=burstsize] [minbandwidth={bandwidth|
none}] [minburstsize=burstsize] [port=port]
[premarking={usemarkvalue|usedscp|none}]
[remarking={usedscpmap|bwclass|none}] [vlan=vlan-id]
[other-parameters]
```


To modify the properties of a traffic class, use the command:

```
set qos trafficclass=id-list [action={forward|
forward,sendmirror|discard|discard,sendmirror|sendmirror|
sendmirror,sendvlanport|sendvlanport}]
[description=description] [dropbwclass3={off|no|false|on|
yes|true}] [ignorebwclass3={off|no|false|on|yes|true}]
[markvalue={dscp-value|none}] [maxbandwidth={bandwidth|
none}] [maxburstsize=burstsize] [minbandwidth={bandwidth|
none}] [minburstsize=burstsize] [port=port]
[premarking={usemarkvalue|usedscp|none}]
[remarking={usedscpmap|bwclass|none}] [vlan=vlan-id]
[other-parameters]
```

To assign traffic classes to a policy, use the command:

```
add qos policy=id trafficclass=trafficclass-list
```

To delete a traffic class from a policy, use the command:

```
delete qos policy=id trafficclass={trafficclass-list|all}
```

To display configuration information for one or more traffic classes, use the command:

```
show qos trafficclass [= {id|all}]
```

Default traffic class

Each QoS policy contains a *default traffic class* (DTC). The policy's DTC provides a catch-all for traffic that does not match one of the traffic classes you assign to that policy.

The DTC supports the same actions and premarking, metering, and dropping functionality as a regular traffic class. To specify the properties of the default traffic class, use the **create qos policy** and **set qos policy** commands.

Note that each policy's default traffic class reduces by one the number of traffic classes that you can create.

Monitoring traffic classes

Information from counters helps you determine if your QoS configuration is working as intended. For example, you can discover which traffic classes are the busiest, and where most of the packets are dropped. If the traffic distribution across classes is not what you intended, you can rearrange the properties of the classes and monitor your configuration until it operates as desired.

For each category of counter, you can view counters relating to a particular entity, for example a particular traffic class, by specifying its ID. The following procedure explains how to enable counters for traffic classes, including default traffic classes.

1. Enable counters for traffic classes by using the command:

```
set switch enhancedmode=qoscounters
```

Note that when you enable counters, the maximum number of traffic classes is reduced.

To disable counters, use the command:

```
set switch enhancedmode=none
```

2. Restart the switch by using one of the following commands:

```
reset switch
restart reboot
```

3. View traffic classes attached to ports via policies by using the command:

```
show qos port counters trafficclass[={trafficclass-id|
default|all}]
```

View traffic class counters for a policy attached to an accelerator card on AT-8948 and AT-9924T/4SP switches by using the command:

```
show qos accelerator counters trafficclass
[={trafficclass-list|default|all}]
```

4. Reset counters by using the command:

```
reset qos port counters trafficclass[={trafficclass-list|
default|all}]
```

Reset traffic class counters for a policy attached to an accelerator card on AT-8948 and AT-9924T/4SP switches by using the command:

```
reset qos accelerator counters
trafficclass[={trafficclass-list|default|all}]
```

QoS Policies

QoS policies consist of a collection of user-defined traffic classes and the default traffic class. QoS controls are applied to traffic ingressing ports. Therefore, to control a particular type of traffic, an appropriate policy must be attached to each port that type of traffic ingresses.

Figure 27-6 on page 27-33 shows a model for building a policy out of traffic classes, flow groups, and classifiers.

A maximum of 256 policies are supported on AT-8948 models and are numbered from 0 to 255. On AT-9924T/4SP, AT-9924T, and AT-9924SP models, a maximum of 512 policies are supported, numbered from 0 to 511. A maximum of 512 policies are supported on x900-24X switches, numbered from 0 to 511. You can assign a policy to more than one port, but a port can have only one policy.

For AT-9900 switches, you can attach a QoS policy to a port trunk group only when all members of the trunk belong to the same switch instance. A *switch instance* refers to a single switch chip. The switch contains two switch instances, which consist of ports 1-12 and ports 13-24.

For x900-24X switches, you can attach a QoS policy to a port trunk group only when all members of the trunk belong to the same switch instance. A *switch instance* refers to a single switch chip. The switch contains the following switch instances: ports 1-12, ports 13-24, and all ports that belong to a single expansion module.

To create a policy and specify the default traffic class properties, use the command:

```
create qos policy=id-list [description=description]
[dtcaction={forward|forward,sendmirror|discard|
discard,sendmirror|sendmirror|sendmirror,sendvlanport|
sendvlanport}] [dtcdropbwclass3={off|no|false|on|yes|
true}] [dtcignorebwclass={off|no|false|on|yes|true}]
[dtcmaxbandwidth={bandwidth|none}]
[dtcmaxburstsize=burstsize] [dtcminbandwidth={bandwidth|
none}] [dtcminburstsize=burstsize]
[dtcpremarking={usemarkvalue|usedscp|none}]
[dtcremarking={usedscpmmap|bwclass|none}]
[markvalue={dscp-value|none}] [port=port] [vlan=vlan-id]
[other-parameters]
```

To modify the properties of a policy or the default traffic class, use the command:

```
set qos policy=id-list [description=description]
[dtcaction={forward|forward,sendmirror|discard|
discard,sendmirror|sendmirror|sendmirror,sendvlanport|
sendvlanport}] [dtcdropbwclass3={off|no|false|on|yes|
true}] [dtcignorebwclass={off|no|false|on|yes|true}]
[dtcmaxbandwidth={bandwidth|none}]
[dtcmaxburstsize=burstsize] [dtcminbandwidth={bandwidth|
none}] [dtcminburstsize=burstsize]
[dtcpremarking={usemarkvalue|usedscp|none}]
[dtcremarking={usedscpmap|bwclass|none}]
[markvalue={dscp-value|none}] [port=port] [vlan=vlan-id]
[other-parameters]
```

To assign a policy to a port or ports, use the command:

```
set qos port={port-id|all} [policy={id|none}]
[defaultqueue=queue-number] [forcedefqueue={yes|no}]
[red={red-id|none}]
```

Note that error checking of parameters and parameter values for the policy is done when the policy is set on a port.

To destroy a policy, use the command:

```
destroy qos policy={id-list|all}
```

To display configuration information for a policy, use the command:

```
show qos policy[={id|all}]
```

RED Curves

Random Early Detection/Discard (RED) is a congestion avoidance mechanism that allows the switch to drop packets randomly before the egress queue exceeds the allocated maximum queue length. It is aware of bandwidth classes; therefore, it can drop less conformant packets when some congestion occurs, and can drop more conformant packets as congestion becomes more severe.

Each RED curve set consists of three curves, one for each bandwidth class. RED curves are typically designed so that packets in bandwidth class 3 start being dropped when the average queue length reaches a reasonably low threshold. Packets in bandwidth class 2 start being dropped at a higher average threshold. Conforming packets, which are in bandwidth class 1, are dropped at the highest threshold.

Using RED curves stops the switch from dropping bursts of packets and therefore breaks the global synchronisation of TCP flows. This maximises link utilisation for TCP flows. RED also makes non-conformant flows drop packets earlier than they otherwise would. This can be an advantage if the switch has both non-conformant and almost-conformant UDP flows. It stops non-conformant flows from filling the egress queues, which makes it possible for almost-conformant flows to queue packets during bursts.

A total of four global, user-definable sets of RED curves are supported. Depending on the switch, one or two RED curve sets (RED=1) exist by default at startup. You cannot create or destroy them but you can configure them. You can create and configure up to three more RED curve sets. Parameters for RED curve sets are set to the defaults.

RED curve functionality is implemented on egress ports. Each RED curve set has eight RED curves, one for each egress queue. There are eight egress queues per port. Each RED curve has three thresholds, one for each bandwidth class. For more information on bandwidth classes, see [“Bandwidth conformance classes” on page 27-25](#).

The following table describes parameters that define a RED curve.

Parameter	Description
start	Average length of the egress queue in bytes below which packets are accepted.
stop	Average length of the egress queue in bytes above which all packets are discarded.
drop	Drop probability at the egress queue length specified by the stop value.

The queue length for RED probability calculations is measured in numbers of bytes. Since the maximum length for an egress queue is set in terms of frames, the relationship between the egress queue and the queue length for RED probability calculations varies, depending on the particular mix of traffic at any time. The range of the user-defined RED curve parameters is not restricted in consideration of this. If the length of the egress queue is not correctly taken into account, some configurations may not result in the expected RED control behaviour.

To create a RED curve set, use the command:

```
create qos red=red-id [DESCRIPTION=description]
```

To set properties of a specific RED curve set for an egress queue, use the command:

```
set qos red=red-id [averaging=averaging-factor]
[description=description] [queue=queue-list]
[start1=start] [stop1=stop] [drop1=probability]
[start2=start] [stop2=stop] [drop2=probability]
[start3=start] [stop3=stop] [drop3=probability]
```

The **averaging** parameter specifies the weight from 0 to 15 to use in the time-based averaging calculation of queue length for the RED curve algorithm. If 0 is specified, the average queue length follows the actual queue length exactly. A larger **averaging** value applies a longer time constant to the calculation. This improves the performance of TCP sessions around the **stop** values by helping to avoid synchronous dropping of frames from all sessions on the queue. The default is 9.

The **queue** parameter specifies which queues in the set have their settings updated by the specified values. If this parameter is not specified, all egress queues are updated with new values. There is no default.

The **start**, **stop**, and **drop** parameters set the thresholds for each of the three bandwidth classes. Note that the RED algorithm calculates a running average queue length that the Start and Stop values use. Because they are averages, Start and Stop must be less than 100% of the maximum queue length.

The **start1**, **stop1**, and **drop1** parameters specify the RED settings for frames associated with bandwidth class 1.

The **start2**, **stop2**, and **drop2** parameters specify the RED settings for frames associated with bandwidth class 2.

The **start3**, **stop3**, and **drop3** parameters specify the RED settings for frames associated with bandwidth class 3.

To destroy a single RED curve set or all sets, use the command:

```
destroy qos red={red-idlist|all}
```

You must configure a port on the switch to implement RED curve functionality. You can configure each egress port to use any of the four global RED curve sets. To specify that a port or ports use a specific RED curve set, use the command:

```
set qos port={port-id|all} red=red-id [other-parameters]
```

To display configuration information about a RED curve set or all RED curve sets, use the command:

```
show qos red[={red-id|all}] [queue=queue-list]
```

Tail-drop discarding scheme

Tail-drop refers to when packets are discarded from the logical tail of an egress queue because there is no more space in the queue.

You can configure an egress port to use a three tail-drop discarding scheme using a subset of the parameters for the default RED curve set (RED=1). The tail-drop discarding scheme uses the **stop1**, **stop2**, and **stop3** values for each queue in the default RED curve set. If a queue has a length greater than **stop3** then no frames with bandwidth class 3 are added to the queue, they are dropped.

To specify that a port use the tail-drop discarding scheme, use the command:

```
set qos port={port-id|all} red=none [other-parameters]
```

Port Groups

A port group is a set of ports you have collected together so that QoS can process them as a single entity. Typically, you create port groups and then assign a policy to a group. When you do this, only one instance of the policy is created. Traffic arriving via members of the port group is then processed by that policy. If port groups are not used, the policy's configuration is copied and duplicated on multiple policies in hardware.

The distinction between multiple, different instances of a policy separately attached to each port, and a single instance attached collectively to ports is especially important for metering. *Metering* marks packets with a bandwidth class number that indicates whether the packet is within specific bandwidth limits. Downstream QoS processes then determine how to handle the packets, depending on their respective bandwidth class. For individual ports, the metering process separately measures the data rate coming into each port. However, with port groups, metering collectively measures the total data rate coming into members of the group.

A single port scenario is suitable for multiple unit situations, such as hotels, where each port connects to a separate end-user, and you want to separately meter data for each end-user. However, port groups are appropriate for enterprises where all ports on a switch are connected to a LAN owned by one customer. The goal is to measure the combined traffic arriving at the switch over ports to which specific policies are assigned.

To create one or more port groups or remove a group, use the commands:

```
create qos portgroup=group-list [port=port-list]
[description=description]
```

```
destroy qos portgroup=group-list
```

To add ports or remove them from a port group, use the commands:

```
add qos portgroup port=port-list  
delete qos portgroup port=port-list
```

To attach a policy to a port group or remove the current policy, use the command:

```
set qos portgroup=group-list [policy={policy-list|none}]  
[description=description]
```

To enable QoS counters, use the command:

```
set switch enhancedmode=qoscounters
```

To reset traffic class counters for a port group, use the command:

```
reset qos portgroup counters trafficclass[={trafficclass-list|  
all}]
```

To display information about port groups, use the commands:

```
show qos portgroup[={group-list|all}]  
show qos portgroup counters trafficclass[={trafficclass-list|  
default|all}]  
show qos port[={port-list|all}] [egressqueue=queue-list]
```

QoS Processes

This section describes the following processes:

- [Premarking](#)
- [Bandwidth Metering](#)
- [Re-Marking](#)
- [Replacing Priorities on Egress](#)
- [Scheduling Queues](#)

Premarking

Premarking occurs before bandwidth metering is applied to a traffic class. Premarking lets you select new values for the DiffServ Code Point (DSCP), bandwidth class, egress queue, and VLAN Tag User Priority of a flow group or traffic class. These new values are based on either the DSCP values of the constituents of the flow group or traffic class, or by using a nominated mark-value to index a preset, user-defined DSCP mapping table.

Setting the DSCPMAP table

One of the options for premarking is the DSCP mapping table. For each DSCP value, the table contains new values that the switch assigns for the following:

- bandwidth class
- DSCP
- egress queue
- VLAN Tag User Priority

To change the table's entries for a particular DSCP, use the command:

```
set qos dscpmap=premarking dscp=dscp-list
[newbwclass=bandwidth-class] [newdscp=dscp-value]
[newpriority=vlan-priority] [newqueue=queue-number]
```

The initial value for **newdscp** is the value specified in the DSCP parameter. The initial value for **newbwclass** is 1. The initial value is 0 for **newpriority** and **newqueue**. If you specify any of these parameters, you must also supply a value; there is no default.

Applying premarking to a flow group or traffic class

To specify premarking, use the commands:

```
create qos flowgroup=flowgroup-list
[markvalue={dscp-value|none}]
premarking={usemarkvalue|usedscp|none} [other-parameters]

set qos flowgroup=flowgroup-list
[markvalue={dscp-value|none}]
premarking={usemarkvalue|usedscp|none} [other-parameters]

create qos trafficclass=id-list [markvalue={dscp-value|none}]
premarking={usemarkvalue|usedscp|none} [other-parameters]

set qos trafficclass=id-list [markvalue={dscp-value|none}]
premarking={usemarkvalue|usedscp|none} [other-parameters]
```

Important If **premarking** is specified for a flow group, these settings override the premarking settings specified for a traffic class.

If **premarking=usedscp** is specified, the QoS settings for the traffic flow are selected from the DSCPMAP table using the DSCP value in the matching data frames and a bandwidth class value of 1.

If **premarking=usemarkvalue** is specified, the QoS settings for the traffic flow are selected from the DSCPMAP table using **markvalue** and a bandwidth class of 1. The **markvalue** parameter specifies an explicit value to use as an index into the DSCPMAP table when the **premarking** parameter is set to **usemarkvalue**. The **markvalue** must be set to a valid DSCP to allow this action.

If **premarking=none** is specified for the **create qos flowgroup** or **set qos flowgroup** command, the traffic flow is passed to the traffic class stage.

If **premarking=none** is specified for the **create qos trafficclass** or **set qos trafficclass** command, the traffic flow is passed to the metering stage.

The default for the **premarking** and **markvalue** parameters is **none**.

Unclassified traffic

You can set the default traffic class for any policy so that it premarks unclassified traffic using a DSCPMAP setting for which the new bandwidth class is 2. This forces the default traffic class into a lower forwarding preference group for all egress queues, ensuring that “legal” classified traffic is processed first. The default traffic class may also be mapped to a lower priority queue, or the queue may be placed in a lower priority arbitration group.

To specify that the default traffic class is premarked before traffic class bandwidth metering is applied, use the commands:

```
create qos policy=id-list dtcpremarking={usemarkvalue|
usedscp|none} [markvalue={dscp-value|none}]
[other-parameters]

set qos policy=id-list dtcpremarking={usemarkvalue|usedscp|
none} [markvalue={dscp-value|none}] [other-parameters]
```

Bandwidth Metering

Metering lets you specify the limits of the bandwidth allocation meter that measures the bandwidth that a traffic class uses.

You can select either a single-rate bandwidth allocation meter, or twin-rate bandwidth allocation meter. Twin-rate lets you manage traffic flow with greater sophistication.

Based on the conformance of the traffic class to limits set with the bandwidth allocation meter, you can specify that traffic be dropped, and/or that the QoS properties of the traffic flow be remarked.

The meter resolution varies according to the specific rate limits set. To ensure that the meter operates as closely as possible to the specified limits, an adaptive meter rate calculation algorithm is used. The metering process supports a variable, user-defined tolerance to bursts of traffic (burstsize), in excess of the defined limits.

Bandwidth conformance classes

The bandwidth allocation meters employ a three-level bandwidth conformance class, or bandwidth class, classification scheme against which traffic is measured. The following table shows the service level for each bandwidth class marker.

Bandwidth Class Marker	Service Level
Bandwidth class 1	Best conformance; best access to available bandwidth; highest performance
Bandwidth class 2	Discretionary access to bandwidth
Bandwidth class 3	Lowest conformance; over acceptable limits, lowest performance

The bandwidth class marker provides a preferential service level for conforming traffic, while permitting the flexible treatment of marginal or non-conforming traffic during the re-marking, congestion control, and egress stages.

How bandwidth and burstsize are specified

Bandwidth is specified in kilobits per second (kbps) from 0 to 16000000 kbps. You can specify this value in kbps, Mbps, or Gbps. If no unit is specified, the value is read as kbps. If Mbps or Gbps is specified, the value may contain a decimal fraction, for example, 1.25 Mbps.

Burstsize is a value from 0 to 16777216 bytes. This value may be specified in bytes, kbytes or Mbytes (in uppercase or lowercase). If no unit is specified, the value is read as bytes. If Mbytes is specified, the value may contain a decimal fraction, for example, 1.25 Mbytes.

Single-rate bandwidth allocation meter

A single-rate bandwidth allocation meter has one bandwidth threshold and two burstsize levels. The following table describes properties of a single-rate bandwidth allocation meter.

Bandwidth Class Marker	Service Level
Bandwidth class 1	Under maximum rate and under minimum burstsize.
Bandwidth class 2	Bursting between minimum and maximum burstsize.
Bandwidth class 3	Over maximum rate and over maximum burstsize.

Specifying properties for single-rate bandwidth metering

To create and modify the single-rate bandwidth metering properties for a traffic class, use the commands:

```
create qos trafficclass=id-list [dropbwclass3={yes|no}]
    maxbandwidth={bandwidth|none} maxburstsize=burstsize
    minburstsize=burstsize [other-parameters]

set qos trafficclass=id-list [dropbwclass3={yes|no}]
    maxbandwidth={bandwidth|none} maxburstsize=burstsize
    minburstsize=burstsize [other-parameters]
```

The **dropbwclass3** parameter specifies whether frames exceeding the traffic class **maxbandwidth** setting are dropped. Setting this parameter to **yes** indicates that data received on this traffic class at a rate higher than the combined **maxbandwidth** and **maxburstsize** settings allow is dropped immediately. Setting this parameter to **no** marks non-conforming traffic as bandwidth class 3 and allows non-conforming traffic to be selected for dropping by the RED curve settings, which have a more TCP-friendly algorithm. The default is **no**.

The **maxbandwidth** parameter specifies the bandwidth available to the traffic class. This parameter determines the maximum data rate for bandwidth class 1 and 2. The default is **none**.

The **maxburstsize** parameter specifies the burst tolerance for **maxbandwidth**. The **maxburstsize** parameter determines the maximum amount of data permitted above **maxbandwidth** for the traffic class before frames are remarked to bandwidth class 3, or frames are dropped depending on the setting of **dropbwclass3**. The **maxburstsize** should be as least as large as the largest size packet to be metered on the aggregate flow. The default is 0.

The **minburstsize** parameter determines the maximum amount of data permitted above **maxbandwidth** for the traffic class before re-marking to bandwidth class 2 occurs. The default is 0.

To create and modify the single-rate bandwidth metering properties for the default traffic class, use the commands:

```
create qos policy=id-list [dtdropbwclass3={yes|no}]
    dtcmaxbandwidth={bandwidth|none}
    dtcmaxburstsize=burstsize
    dtcminburstsize=burstsize [other-parameters]

set qos policy=id-list [dtdropbwclass3={yes|no}]
    dtcmaxbandwidth={bandwidth|none}
    dtcmaxburstsize=burstsize
    dtcminburstsize=burstsize [other-parameters]
```

Twin-rate bandwidth allocation meter

A twin-rate bandwidth allocation meter has a minimum bandwidth threshold and a maximum bandwidth threshold, and one level of burst per minimum and maximum threshold. The following table describes properties of a twin-rate bandwidth allocation meter.

Bandwidth Class Marker	Service Level
Bandwidth class 1	Under minimum rate and under minimum burstsize.
Bandwidth class 2	Over minimum rate and burstsize and under maximum rate and burstsize.
Bandwidth class 3	Over maximum rate and maximum burstsize.

Specifying properties for twin-rate bandwidth metering

To create and modify the twin-rate bandwidth metering properties for a traffic class, use the commands:

```
create qos trafficclass=id-list [dropbwclass3={yes|no}]
    maxbandwidth={bandwidth|none} maxburstsize=burstsize
    minbandwidth={bandwidth|none} minburstsize=burstsize
    [other-parameters]

set qos trafficclass=id-list [dropbwclass3={yes|no}]
    maxbandwidth={bandwidth|none} maxburstsize=burstsize
    minbandwidth={bandwidth|none} minburstsize=burstsize
    [other-parameters]
```

The **dropbwclass3** parameter specifies whether frames exceeding the traffic class **maxbandwidth** setting are dropped. Setting this parameter to **yes** indicates that data received on this traffic class at a rate higher than the combined **maxbandwidth** and **maxburstsize** settings allow is dropped immediately. Setting this parameter to **no** marks non-conforming traffic as bandwidth class 3 and allows non-conforming traffic to be selected for dropping by the RED curve settings, which have a more TCP-friendly algorithm. The default is **no**.

The **maxbandwidth** parameter specifies the maximum bandwidth available to the traffic class. This parameter determines the maximum data rate for bandwidth class 2. The default maximum bandwidth is **none**.

The **maxburstsize** parameter specifies the burst tolerance for **maxbandwidth**. The **maxburstsize** parameter determines the maximum amount of data permitted above **maxbandwidth** for the traffic class before re-marking to bandwidth class 3 occurs, or frames are dropped depending on the setting of **dropbwclass3**. The **maxburstsize** should be as least as large as the largest size packet to be metered on the aggregate flow. The default is 0.

The **minbandwidth** parameter specifies the minimum bandwidth reserved for the traffic class. This parameter determines the maximum rate of data in bandwidth class 1. The default is **none**.

The **minburstsize** parameter specifies the burst tolerance for **minbandwidth**. The **minburstsize** parameter determines the maximum amount of data permitted above **minbandwidth** for the traffic class before re-marking to bandwidth class 2 occurs. The default is 0.

To create and modify the twin-rate bandwidth metering properties for the default traffic class, use the commands:

```
create qos policy=id-list [dtdropbwclass3={yes|no}]
    dtcmaxbandwidth={bandwidth|none}
    dtcmaxburstsize=burstsize
    dtcminbandwidth={bandwidth|none}
    dtcminburstsize=burstsize [other-parameters]

set qos policy=id-list [dtdropbwclass3={yes|no}]
    dtcmaxbandwidth={bandwidth|none}
    dtcmaxburstsize=burstsize
    dtcminbandwidth={bandwidth|none}
    dtcminburstsize=burstsize [other-parameters]
```

Re-Marking

Re-marking specifies the action to take on the traffic flow after the metering stage. During metering, a temporary value of bandwidth class is assigned to the traffic flow that is used to determine its per-hop behaviour. During re-marking, you can specify that frames be re-marked based on the bandwidth limit conformance calculation after metering.

Specifying properties

To create and modify the re-marking properties for a traffic class, use the commands:

```
create qos trafficclass=id-list remarking={usedscpmap|
    bwclass|none} [other-parameters]

set qos trafficclass=id-list remarking={usedscpmap|bwclass|
    none} [other-parameters]
```

To create and modify the re-marking properties for the default traffic class, use the commands:

```
create qos policy=id-list dtcremarking={usedscpmap|bwclass|
    none} [other-parameters]

set qos policy=id-list dtcremarking={usedscpmap|bwclass|none}
    [other-parameters]
```

If **usedscpmap** is specified, the temporary value of bandwidth class is used with the DiffServ Code Point (DSCP) of the frame as an index into the re-marking DSCPMAP table. The DSCPMAP table then assigns the actual, new values for bandwidth class, DSCP, egress queue and VLAN Tag User Priority (see [Setting the DSCPMAP table](#) below).

If **bwclass** is specified, the temporary bandwidth class becomes the new bandwidth class for the flow. If **none** is specified, no re-marking occurs, which is the default.

Setting the DSCPMAP table

One of the options for re-marking is a DSCP mapping table. For each temporary bandwidth class and DSCP value, the table contains new values that the switch assigns for:

- bandwidth class
- DSCP
- egress queue
- VLAN Tag user priority

Using the DSCP mapping table lets you specify the per-hop re-marking actions for each frame according to the frame's previous DSCP and bandwidth class. The following table is an example of the beginning of a DSCP mapping table.

BWCLASS DSCP	Class 1	Class 2	Class 3
0	NEWBWCLASS NEWDSCP NEWPRIORITY NEWQUEUE	NEWBWCLASS NEWDSCP NEWPRIORITY NEWQUEUE	NEWBWCLASS NEWDSCP NEWPRIORITY NEWQUEUE
1	NEWBWCLASS NEWDSCP NEWPRIORITY NEWQUEUE	NEWBWCLASS NEWDSCP NEWPRIORITY NEWQUEUE	NEWBWCLASS NEWDSCP NEWPRIORITY NEWQUEUE

To change table entries for a particular DSCP and bandwidth class, use the command:

```
set qos dscpmap=remarking dscp=dscp-list bwclass=bwclass-list
[newbwclass=bandwidth-class] [newdscp=dscp-value]
[newpriority=vlan-priority] [newqueue=queuenumber]
```

The initial value for **newdscp** is the value specified in the **dscp** parameter. The initial value for **newbwclass** is the value specified in the **bwclass** parameter. The initial value is 0 for **newpriority** and **newqueue**. If you specify any of these parameters, you must also supply a value; there is no default. The following table shows a conceptual example of part of a DSCPMAP table, including initial values.

BWCLASS DSCP	Class 1	Class 2	Class 3
0	NEWBWCLASS=1 NEWDSCP=0 NEWPRIORITY=0 NEWQUEUE=0	NEWBWCLASS=2 NEWDSCP=0 NEWPRIORITY=0 NEWQUEUE=0	NEWBWCLASS=3 NEWDSCP=0 NEWPRIORITY=0 NEWQUEUE=0

BWCLASS \ DSCP	Class 1	Class 2	Class 3
1	NEWBWCLASS=1 NEWDSCP=1 NEWPRIORITY=0 NEWQUEUE=0	NEWBWCLASS=2 NEWDSCP=1 NEWPRIORITY=0 NEWQUEUE=0	NEWBWCLASS=3 NEWDSCP=1 NEWPRIORITY=0 NEWQUEUE=0

Replacing Priorities on Egress

If the switch determines priority on the basis of the traffic class or flow group priority, this priority determines the egress queue where a packet is sent when it egresses this switch. By default, it has no effect on how the rest of the network processes the packet. To permanently change the packet's priority, you must replace one of the following priority fields in the packet header:

- DSCP value of the IP header's Differentiated Services field
- User Priority field of the VLAN tag header

DSCP value Replacing the DSCP value of the IPv4 or IPv6 header's Differentiated Services field on egress may be required as part of the configuration of an edge switch in a DiffServ domain. For information on using the QoS policy model and the DSCP value to configure a DiffServ domain, see ["DiffServ Domains" on page 27-36](#).

To replace the DSCP value of a packet, use the commands:

```
create qos trafficclass=id-list remarking=usedscmap
[other-parameters]

set qos trafficclass=id-list remarking=usedscmap
[other-parameters]
```

The **remarking** parameter specifies the action to take after the metering stage.

The **usedscmap** option specifies that the temporary value of bandwidth conformance class is used (in conjunction with the DSCP of the frame) as an index into the DSCPMAP mapping table, which then assigns the actual, new values for bandwidth class, DSCP, egress queue and VLAN Tag User Priority.

To set the properties of the DSCP mapping table, use the command:

```
show qos dscmap[={premarking|remarking}] dscp=dscp-list
bwclass=bwclass-list [newdscp=dscp-value]
[newbwclass=bandwidth-class] [newqueue=queuenumber]
[newpriority=vlan-priority]
```

For each DSCP value in the DSCP mapping table there are three sets of QoS parameter values, one per bandwidth class. This lets you specify the per-hop re-marking actions for each frame according to the frame's previous DSCP and bandwidth class.

Note that you can also give a particular DSCP to packets that come from the switch's CPU by using the command:

```
set ip dscpooverride={none|0..63}
```

For more information, see the [set ip dscpooverride command on page 13-116 of Chapter 13, Internet Protocol \(IP\)](#).

VLAN tag priority field

Replacing the User Priority field of the VLAN tag header relabels VLAN-tagged traffic so that the next switch can process traffic appropriately. Replacing the User Priority field is most useful outside DiffServ domains. You can specify that the VLAN Tag Priority field be replaced for tagged frames at ingress and be set for untagged frames at egress.

To specify that the VLAN Tag Priority field of tagged frames be replaced, use the commands:

```
create qos trafficclass=id-list remarking={usedscmap|
    bwclass|none} [other-parameters]

set qos trafficclass=id-list remarking={usedscmap|bwclass|
    none} [other-parameters]
```

The **usedscmap** option specifies that the temporary value of bandwidth conformance class is used (in conjunction with the DSCP of the frame) as an index into DSCPMAP, which then assigns the actual, new values for bandwidth class, DSCP, egress queue and VLAN Tag User Priority.

If **bwclass** is specified, the temporary bandwidth class becomes the new bandwidth class for the flow. The default is **none**.

To set the VLAN Tag Priority field assigned at egress for frames that were untagged at ingress, use the command:

```
set qos defaultpriority=q0,q1,q2,q3,q4,q5,q6,q7
```

The integers *q0* to *q7* represent the VLAN Tag User Priority corresponding to an internal Class of Service queue. All eight values are required. The first value, *q0*, represents the VLAN Tag User Priority corresponding to an internal Class of Service queue of 0, and similarly values *q1* to *q7* represent the VLAN Tag User Priority corresponding to an internal Class of Service queue of 1 to 7. The default set of values is 1,2,0,3,4,5,6,7. This is the reverse of the default **prio2queuemap** setting.

Frames that do not have a User Priority value assigned by any other QoS mechanism have a value assigned this way.

Note that you can also give a particular 802.1p priority to packets that come from the switch's CPU by using the command:

```
set switch cputxpriority={none|0..7}
```

See the **set switch cputxpriorityoverride** command on page 7-101 of Chapter 7, [Switching](#) for more information.

Scheduling Queues

You must configure how the switch determines the order in which to empty queues, and what proportion of the bandwidth is allowed for packets from each queue. Egress queues must be scheduled on x900-48FE and AT-9900 switches, as explained in the following table. Both egress and fabric queues must be scheduled for x900-24X switches, as explained below.

Method	Description	Disadvantage
Strict priority	<p>Higher priority queues are emptied before packets are transmitted from queues with lower priorities.</p> <p>For example, queues with priority 7 must be totally empty before packets are sent from the queue with priority 6.</p> <p>The schedule defaults to strict priority for egress queues, and also for fabric queues on x900-24X switches.</p> <p>We suggest you put latency and jitter-sensitive traffic, such as VoIP, into a strict priority traffic class.</p>	<p>High priority traffic may use all the available bandwidth, forcing the switch to drop all medium and low priority traffic.</p> <p>To prevent this problem, put a bandwidth limit on the high priority traffic.</p>
Weighted round robin (WRR)	<p>Queues share bandwidth based on specific weightings set by the user thereby letting the switch transmit packets from all queues during high congestion.</p> <p>If you change the schedule on x900-24X switches to WRR for most of the egress queues, we suggest you also change the schedule for fabric queues so that QoS handles traffic consistently.</p> <p>You can configure the weightings to ensure that more packets per second are sent from queues that are more sensitive to packet drop, than from less sensitive or lower priority ones.</p>	<p>Large packets get more than their fair share of the bandwidth.</p>

Limiting bandwidth on queues

The scheduler is not the only mechanism that controls how egress queues are emptied. You can also set a maximum data rate on individual queues with the **maxbandwidth** parameter in the command:

```
set qos port egressqueue=queue-list maxbandwidth=bandwidth
```

Setting a bandwidth limit on a whole port and setting a bandwidth limit on an individual queue control two different aspects of egress scheduling. The limit on the port sets the rate at which the port "pulls" packets from the egress queues. Whereas the limit on the queue sets the rate at which it lets packets be pulled from it.

Queues can resist a pull when they reach their bandwidth limit. This suggests that this limit competes somewhat with the scheduler. For example, if the top priority queue reaches its bandwidth limit, then packets must be emitted from the next priority queue, even if the top priority queue is not empty.

Configuring QoS on the Switch

This section outlines the following:

- [Rules for QoS Configuration](#)
- [Overview of Procedure](#)
- [Configuring QoS for Accelerated IPv6 Traffic](#)

Rules for QoS Configuration

We recommend the following:

- A classifier may be assigned to many flow groups, and can work successfully in many different policies. However, use a classifier once per policy.
- Do not use a single classifier in different flows that end up, via traffic classes, assigned to the same policy.
- A flow group may have many classifiers.
- A flow group should be assigned to only one traffic class, but a traffic class can have many flow groups.
- A traffic class should be assigned to only one policy, but a policy can have many traffic classes.
- A policy may be assigned to many ports; however, a port should have only one policy.

Overview of Procedure

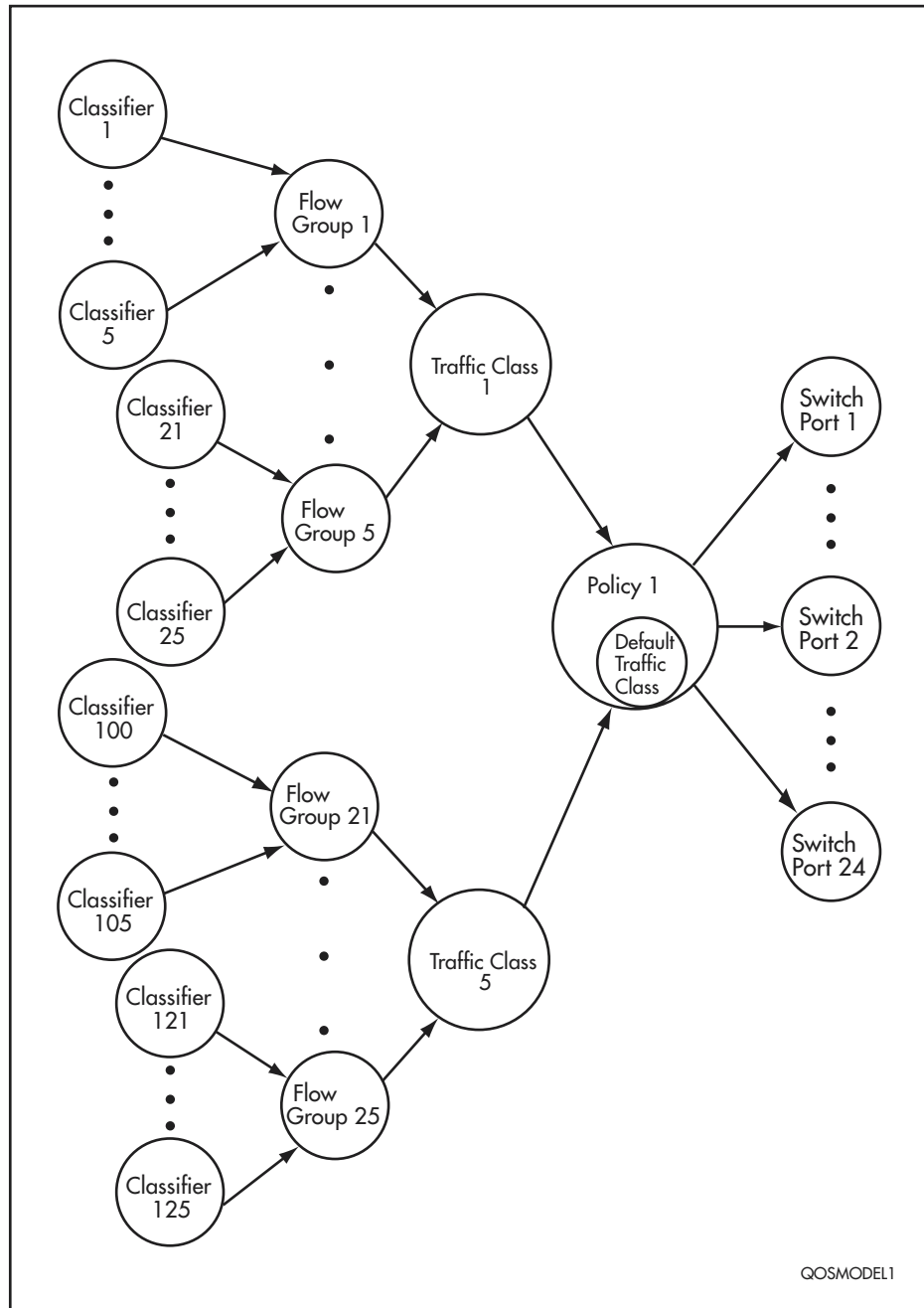
Within the QoS model, flow groups are assigned to a traffic class, traffic classes are assigned to a policy, and the policy is attached to one or more ports.

The following tasks are listed in a conceptually logical order; however, the QoS policy must be attached to a port before the switch can check it for errors. To simplify error diagnosis, plan your configuration on paper first, and then enter it into the switch in reverse order, starting with policies.

1. Create *classifiers* to sort packets into traffic flows. For detailed information about classifiers, see [Chapter 26, Generic Packet Classifier](#).
2. Create *flow groups* and add classifiers to them. Flow groups are groups of classifiers that group together similar traffic flows. Using premarking functionality, you can select new values for the traffic's DiffServ Code Point (DSCP), bandwidth class, internal queue, and VLAN Tag User Priority.
3. Create *traffic classes* and add flow groups to them. Traffic classes are groups of flow groups and are central to QoS. You can apply the same premarking functionality as described in the previous step; apply bandwidth metering limits against which the bandwidth used by a traffic class is measured; specify that frames exceeding the maximum bandwidth limit for a traffic class are immediately dropped; specify that after metering frames that carry an "over limit" bandwidth class marker are dropped immediately; specify that after metering frames are remarked according to their bandwidth limit conformance calculation.
4. Create *policies* and add traffic classes to them. Policies are groups of traffic classes and the default traffic class. The default traffic class is the catch-all for traffic that does not match one of the traffic classes you assign to a policy. A policy defines a complete QoS solution for a port or group of ports.
5. Associate policies with ports.

Packets received on a port are sorted into various traffic flows, according to the QoS policy that applies to the port. The switch then allocates resources to direct this traffic according to the bandwidth or priority settings in the QoS policy. Each policy is built from traffic classes, flow groups, and classifiers (Figure 27-6).

Figure 27-6: QoS model



Configuring QoS for Accelerated IPv6 Traffic

The following procedure applies to switches with accelerator cards, such as AT-8948s. It explains all the possible QoS controls that you can configure on accelerated IPv6 traffic. Whether you need each individual control depends on your particular application.

1. **Classify the IPv6 traffic at the accelerator card Layer 3 processor** (position 1 in [Figure 27-5](#)).

Create the required classifiers by using the command:

```
create classifier=rule-id [ethformat={ethii-tagged|any}]
[ipdaddr={any|ipv6-add/prefix-length}] [ipsaddr={any|
ipv6-add/prefix-length}] [ipdscp={0..63|any}]
[ipprotocol={tcp|udp|icmp|ipprotocolnum|any}]
[protocol=ipv6] [tcpdport={portid|any}]
[tcpsport={portid|any}] [udpport={portid|any}]
[udpsport={portid|any}]
```

For more information see [Chapter 26, Generic Packet Classifier](#).

2. **Filter the traffic at the Layer 3 processor** (position 1 in [Figure 27-5](#)).

You can configure an IPv6 accelerator hardware-based filter to mark matching traffic with a new DSCP and/or VLAN tag User Priority.

To create the filter, use the command:

```
add switch accelerator hwfilter=filter-id
classifier=rule-id action=mark [newipdscp=0..63]
[newpriority=0..7]
```

For example, if you classify on source IPv6 address, the accelerator filters allow you to:

- Apply a particular priority to all traffic from certain IPv6 addresses. The accelerator card then assigns the traffic to an egress queue on the basis of that priority.
- Apply a particular DSCP to all traffic from certain IPv6 addresses. At the next stage of QoS processing you can then classify traffic by that DSCP and apply bandwidth and queuing control to matching traffic.

For more information about filters see [“Classifier-Based Filters with Accelerated IPv6 Traffic” on page 7-41 of Chapter 7, Switching](#).

3. **Assign the traffic to an egress queue according to its current priority** (position 2 in [Figure 27-5](#)).

To specify the mapping between the packet's current VLAN tag User Priority value and an egress queue, use the command:

```
set qos prio2queuemap=p0,p1,p2,p3,p4,p5,p6,p7
```

The **prior2queuemap** parameter specifies a comma-separated list of eight values, all of which must be present. The first value, p0, represents the queue priority corresponding to a current VLAN tag User Priority of 0. Similarly values p1 to p7 represent the queue priority corresponding to a current VLAN tag User Priority of 1 to 7. The defaults are 2,0,1,3,4,5,6,7 as recommended in IEEE Standard 802.1q (1998) section 8.7.3.

4. **Classify the IPv6 traffic at the Layer 2 processor** (position 2 in [Figure 27-5](#)).

Create the required classifiers by using the command:

```
create classifier=rule-id ethformat=ethii-tagged
protocol=ipv6 [ipdscp={dscplist|any}]
[ipprotocol={tcp|udp|icmp|ipprotocolnum|any}]
[macdaddr={macadd|any}] [macsaddr={macadd|any}]
[mactype={l2ucast|l2mcast|any}]
[vlan={vlanname|..4094|any}] [vlanpriority=0..7]
```

Note that the `vlan` parameter refers to the *destination* VLAN for accelerated IPv6 packets. For more information about the classifier, see [Chapter 26, Generic Packet Classifier](#).

5. Create a QoS policy to meter traffic or discard it on the basis of its conformance.

Only commands to create traffic classes and policies are listed in this step in the interest of brevity. To modify an existing traffic class or policy, use the `set` commands instead of `create` commands. To configure the policy, you must also create flow groups and assemble the policy in full. See [“Overview of Procedure” on page 27-32](#) for more information.

You can configure a QoS policy to take traffic that matches the classifiers and meter it to determine how well it conforms with the bandwidth specifications. Metering assigns traffic to a bandwidth class depending on conformance (bwclass 1 = green, fully conformant; bwclass 2 = yellow, partially conformant; bwclass 3 = red, non-conformant). You can configure metering as part of the traffic class and the default traffic class by using the commands:

For a single-rate bandwidth meter:

```
create qos trafficclass=id-list maxbandwidth={bandwidth|
none} maxburstsize=burstsize minburstsize=burstsize
[other-parameters]

create qos policy=id-list dtcmaxbandwidth={bandwidth|none}
dtcmaxburstsize=burstsize
dtcminburstsize=burstsize [other-parameters]
```

For a twin-rate bandwidth meter:

```
create qos trafficclass=id-list maxbandwidth={bandwidth|
none} maxburstsize=burstsize minbandwidth={bandwidth|
none} minburstsize=burstsize [other-parameters]

create qos policy=id-list dtcmaxbandwidth={bandwidth|none}
dtcmaxburstsize=burstsize
dtcminbandwidth={bandwidth|none}
dtcminburstsize=burstsize [other-parameters]
```

See [“Bandwidth Metering” on page 27-24](#) for information about these commands and options.

Once traffic has been metered, you can also configure the traffic class and policy to discard traffic that does not conform. Use the commands:

```
create qos trafficclass=id-list dropbwclass3=yes
[other-parameters]

create qos policy=id-list dtcdropbwclass3=yes
[other-parameters]
```

6. Apply the QoS policy to the Layer 2 processor (position 2 in [Figure 27-5](#)).

To apply the policy to the accelerated traffic, use the command:

```
set qos accelerator policy=id
```

To check which policy is applied to the accelerator card, use the command:

```
show qos policy
```

7. Configure the egress queuing behaviour (position 3 in [Figure 27-5](#)).

At the egress port, you can apply the full range of traffic shaping and policing functions that are available on the switch. Relevant commands include:

```
create qos red=red-id [description=description]

set qos red=red-id [averaging=averaging-factor]
[description=description] [queue=queue-list]
[start1=start] [stop1=stop] [drop1=probability]
[start2=start] [stop2=stop] [drop2=probability]
[start3=start] [stop3=stop] [drop3=probability]

set qos port={port-id|all} [defaultqueue=queue-number]
[forcedefqueue={yes|no}] [red={red-id|none}]

set qos port={port-id|all} egressqueue=queue-list
[length=queue-length] [maxbandwidth=bandwidth|none]
[scheduler={strict|wrr1|wrr2}]
[wrrweight=queue-weight]
```

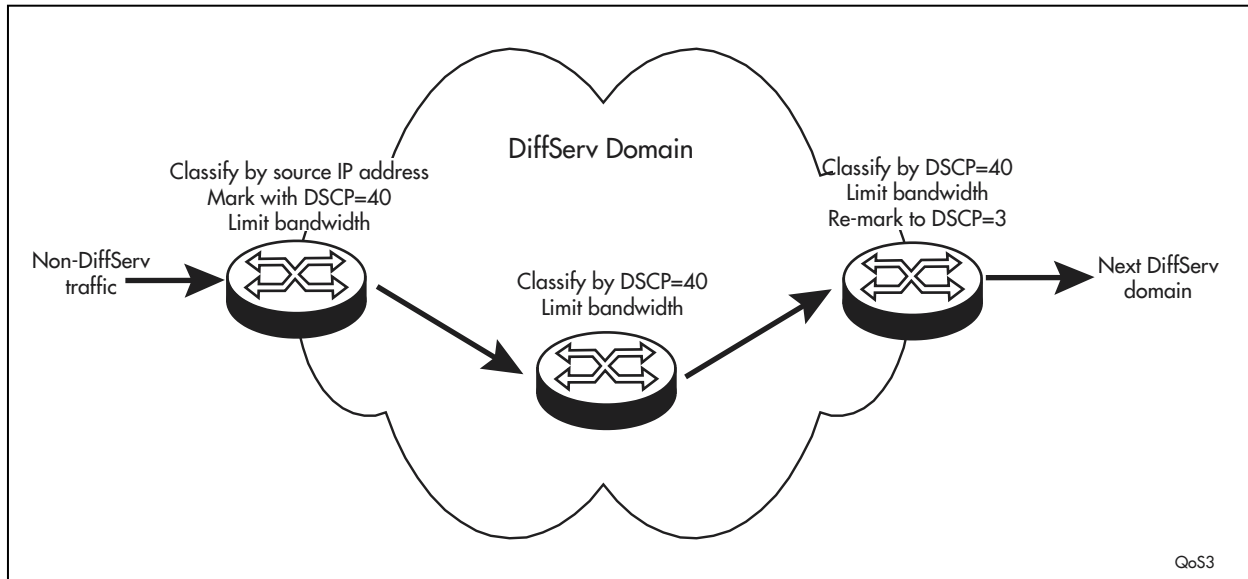
DiffServ Domains

Differentiated Services (DiffServ) is a method of dividing IP traffic into classes of service without requiring that every switch in a network remember detailed information about traffic flows.

DiffServ operates within a *DiffServ domain*, which is a network or subnet managed as a single QoS unit. Packets are classified according to user-specified criteria at the edge of the network, divided into classes, and assigned the required class of service. Packets are then marked with a Differentiated Services Code Point (DSCP) tag to indicate the class of service to which they belong. The DSCP value is written into the Differentiated Services field of the IP header. Routers within the network then use this DSCP value to classify packets and assign QoS appropriately. When a packet leaves the DiffServ domain, the DSCP value can be replaced with a value appropriate for the next DiffServ domain.

A simple example of the process for limiting the amount of bandwidth used by traffic from a particular IP address is shown in [Figure 27-7 on page 27-37](#). In the domain shown, this bandwidth limit is supplied by the class of service represented by a DSCP value of 40. In the next DiffServ domain, this traffic is assigned to the class of service represented by a DSCP value of 3.

Figure 27-7: Example of a DiffServ domain



To use the QoS tool set to configure a DiffServ domain:

1. Classify the packets coming into the domain at edge switches, according to the required characteristics. For available options, see the [create classifier command on page 26-4 of Chapter 26, Generic Packet Classifier](#).

Assign the classifiers to flow groups and the flow groups to traffic classes, with a different traffic class for each DiffServ code point grouping within the DiffServ domain.

Give each traffic class the priority, RED curve and/or bandwidth limiting controls that are required for that type of packet within this part of the domain.

Assign a DSCP value to each traffic class, to be written into the Differentiated Services field of the packet header by using the **markvalue** parameter of the [create qos trafficclass command on page 27-55](#) or [set qos trafficclass command on page 27-93](#).

2. On switches and routers within the DiffServe domain, classify packets according to the DSCP values that were assigned to traffic classes on the edge switches.

Assign the classifiers to flow groups and the flow groups to traffic classes, with a different traffic class for each DiffServ code point grouping within the DiffServ domain.

Give each traffic class the priority, RED curve and/or bandwidth limiting controls that are required for that type of packet within this part of the domain. These QoS controls need not be the same for each switch.

3. As packets leave the DiffServ domain, classify them according to the DSCP values.

Assign the classifiers to flow groups and the flow groups to traffic classes, with a different traffic class for each DiffServ code point grouping within the DiffServ domain.

Give each traffic class the priority, RED curve and/or bandwidth limiting controls required for transmission of that type of packet to its next destination, in accordance with any Service Level Agreement (SLA) with the providers of that destination.

If necessary, assign a different DSCP value to each traffic class, to be written into the Differentiated Services field of the packet header, to match the DiffServ requirements of the destination network.

To enable DiffServ QoS

The switch processes traffic for Quality Of Service according to guidelines in RFC 2475, *An Architecture for Differentiated Services*. DSCP-based classification, marking, and meter-based re-marking are supported.

1. Create classifiers, flow groups, traffic classes, and policies.

To create the QoS elements and specify the functionality of these elements, use the following commands:

```
create classifier
create qos flowgroup=flowgroup-list [other-parameters]
create qos trafficclass=id-list [other-parameters]
create qos policy=id-list [other-parameters]
```

The default traffic class values are specified with the **create qos policy** command.

2. Set the properties of the DSCP-based QoS marking tables.

If premarking or re-marking functionality is specified in the **create qos flowgroup**, **create qos trafficclass**, or **create qos policy** commands, you must set the properties of the DSCP-based QoS marking tables with the command:

```
set qos dscpmap[={premarking|remarking}] dscp=dscp-list
bwclass=bwclass-list [newdscp=dscp-value]
[newbwclass=bandwidth-class] [newqueue=queuenumber]
[newpriority=vlan-priority]
```

3. Add classifiers to a flow group, add flow groups to a traffic class, and add traffic classes to a policy.

To logically link QoS elements, use the following commands:

```
add qos flowgroup=flowgroup-id classifier=classifier-list
add qos trafficclass=trafficclass-id
flowgroup=flowgroup-list
add qos policy=id trafficclass=trafficclass-list
```

Note that if premarking is specified with the **create qos flowgroup** command, this overrides premarking specified with the **create qos trafficclass** command.

4. For congestion control set the RED curve values.

To create RED curve sets and then set the properties of these RED curve sets, use the following commands:

```
create qos red=red-id [description=description]
set qos red=red-id [averaging=averaging-factor]
[description=description] [queue=queue-list]
[start1=start] [stop1=stop] [drop1=probability]
[start2=start] [stop2=stop] [drop2=probability]
[start3=start] [stop3=stop] [drop3=probability]
```

A RED curve set is assigned to a port with the **set qos port** command.

5. Set the egress queue parameters for a port.

To update the parameters for all or specific egress queues on a port, use the command:

```
set qos port={port-id|all} egressqueue=queue-list [other-parameters]
```

This command is used to rate limit and/or force congestion control of normally uncontested traffic.

6. Assign the policy to a port.

To assign a policy to one or more ports, use the command:

```
set qos port={port-id|all} [policy={id|none}]
[defaultqueue=queue-number] [forcedefqueue={yes|no}]
[red={red-id|none}]
```

Note that a port can have only one QoS policy assigned to it.

7. Set the maximum bandwidth available to a port.

By default, the maximum bandwidth is available to a port. To restrict the maximum bandwidth available to a port, use the command:

```
set switch port={port-id|all}
egresslimit={bandwidth|default} [other-parameters]
```

The **egresslimit** parameter specifies the maximum bandwidth available to the port in multiples of approximately 650 kbps. This parameter does not set the exact bandwidth of the port. Rather, the parameter is a measurement of the rate at which data leaves internal queues before it is transmitted onto the line. Header and trailer information encapsulated in the frame are not included in the calculation. The size of the frame impacts upon the actual data transmission rate that the port can transmit onto the line. Therefore, the larger the frame size, the closer the actual percentage of bandwidth on line gets to the bandwidth set.

For more information, see the [set switch port command on page 7-106 of Chapter 7, Switching](#).

Layer 2 Priority-Based QoS

The switch supports QoS on Layer 2 parameters for non-DiffServ compatible traffic. The selection of an egress queue based on the Layer 2 VLAN Tag Priority Field is supported for frames that are tagged at ingress, or by selecting a default queue per port for untagged frames. Meter re-marking of Layer 2 priority on the basis of the selected egress queue and metering bandwidth conformance class is supported. Frames that are untagged at ingress and do not have their priority set during the marking or re-marking stages, have the egress VLAN Tag Priority value selected from a user definable mapping of egress queue values to priority values.

To enable Layer 2 QoS

The following steps enable Layer 2 priority-based QoS functionality.

1. Set the initial queue assignment for tagged frames.

To set the mapping of incoming VLAN Tag User Priorities to the internal service queues for ingressing packets that include a VLAN tag header, use the command:

```
set qos prio2queuemap=p0,p1,p2,p3,p4,p5,p6,p7
```

The integers *p0* to *p7* indicate the queue priority corresponding to an incoming VLAN Tag User Priority. All eight values are required. The first value, *p0*, represents the queue priority corresponding to an incoming VLAN Tag User Priority of 0, and similarly values *p1* to *p7* represent the queue priority corresponding to an incoming VLAN Tag User Priority of 1 to 7. The defaults are 2,0,1,3,4,5,6,7 as recommended in IEEE Standard 802.1q (1998) section 8.7.3.

2. Set the default queue for untagged frames ingressing a specified port.

To set the default queue for untagged frames ingressing a specified port or ports and which have no VLAN Tag User Priority value, use the command:

```
set qos port={port-id|all} defaultqueue=queue-number
[other-parameters]
```

If the default queue is not reassigned by premarking and/or re-marking, this is the egress queue number.

3. Specify that all frames be forced to the default queue.

To specify that all frames, tagged and untagged ones, ingressing a specific port be forced to the default queue, use the command:

```
set qos port={port-id|all} forcedefqueue={yes|no}
[other-parameters]
```

4. Set the VLAN Tag Priority field assigned at egress.

To set the VLAN Tag Priority field assigned at egress for frames that were untagged at ingress (frames that had a queue assigned with the **defaultqueue** parameter in the **set qos port** command), use the command:

```
set qos defaultpriority=q0,q1,q2,q3,q4,q5,q6,q7
```

The integers $p0$ to $p7$ represent the VLAN Tag User Priority corresponding to an to an internal Class of Service queue. All eight values are required. The first value, $q0$, represents the VLAN Tag User Priority corresponding to an internal Class of Service queue of 0, and similarly values $q1$ to $q7$ represent the VLAN Tag User Priority corresponding to an internal Class of Service queue of 1 to 7. The default set of values is 1,2,0,3,4,5,6,7. This is the reverse of the default **prio2queuemap** setting.

Frames that do not have a User Priority value assigned by any other QoS mechanism have a value assigned this way.

Configuration Examples

Examples in this section show how to configure the following:

- **Storm protection per-port**
- **Storm protection per-port per-VLAN**

The following documents describe more solutions, and are available from the Resource Center on your Documentation and Tools CD-ROM or from www.alliedtelesis.co.uk/en-gb/solutions/techdocs.asp?area=howto.

- *How To Configure QoS on the AT-8948 and AT-9900 series switches*
- *How To Configure Filtering Actions on QoS Flow Groups and Traffic Classes*

Storm protection per-port This example protects the switch against broadcast and multicast storms by disabling ports where a storm is detected.

```
# Create QoS entities and configure storm protection against bursts above
# 10kbps and monitor traffic 10 times a second
create qos policy=1
create qos trafficclass=1 stormstatus=enable stormrate=10kbps stormwindow=100
create qos flowgroup=1

# Monitor broadcast and multicast traffic
create classifier=1 mactype=l2bcast
create classifier=2 mactype=l2mcast

# Attach all QoS entities together
add qos flowgroup=1 class=1-2
add qos trafficclass=1 flowgroup=1
add qos policy=1 trafficclass=1

# Apply storm protection policy to ports 1-10
set qos port=1-10 policy=1
```

Storm protection per-port per-VLAN This example protects the switch against broadcast and multicast storms on a per-port, per-VLAN basis. The port is disabled only for the VLAN where the storm was detected. This lets other VLANs continue to use the port uninterrupted.

```
# Create vlan 2 and add all ports as tagged members
create vlan=vlan2 vid=2
add vlan=2 port=all frame=tagged

# Create QoS entities and configure storm protection against bursts of 10kbps,
# monitor traffic 10 times a second, and disable the port for the VLAN on which the
# storm was detected
cre qos policy=1
cre qos tr=1-2 storms=ena stormr=10kbps stormw=100 storma=vlandisable
cre qos flowgroup=1-2

# Monitor broadcast and multicast traffic on VLANs 1 and 2
cre classifier=1 mactype=l2bcast vlan=1
cre classifier=2 mactype=l2mcast vlan=1
cre classifier=3 mactype=l2bcast vlan=2
cre classifier=4 mactype=l2mcast vlan=2

# Attach all QoS entities together
add qos flowgroup=1 classifier=1-2
add qos flowgroup=2 classifier=3-4
add qos trafficclass=1 flowgroup=1
add qos trafficclass=2 flowgroup=2
add qos policy=1 trafficclass=1-2

# Apply storm protection policy to all ports
set qos port=all policy=1
```

Command Reference

This section describes the commands available to configure and manage the QoS functions on the switch.

The shortest valid command is denoted by capital letters in the Syntax section. See [“Conventions” on page -xlix of , About this Software Reference](#) in the front of this manual for details of the conventions used to describe command syntax. See [Appendix A, Messages](#), for a complete list of messages and their meanings.

add qos flowgroup

Syntax `ADD QOS FLOWgroup=flowgroup-id CLASSifier=classifier-list`

Description This command adds one or more classifiers to a QoS flow group.

Parameter	Description
Flowgroup	Existing flow group to which you want to add a classifier. The <i>flowgroup-id</i> is an integer from 0 to 1023. Default: no default
CLASSifier	Existing classifier to add to the flow group. A <i>classifier-list</i> consists of: an integer from 1 to 9999 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges Default: no default

Examples To add classifiers 2, 3, 4, 5 and 6 to flow group 42 use the command:

```
add qos fl=42 class=2-6
```

Related Commands

- [create classifier](#)
- [create qos flowgroup](#)
- [delete qos flowgroup](#)
- [destroy qos flowgroup](#)
- [set qos flowgroup](#)
- [show qos flowgroup](#)

add qos policy

Syntax `ADD QOS POLIcy=id TRAfficclass=trafficclass-list`

Description This command adds traffic classes to a policy. Packets are first matched against the traffic flow groups of the first traffic class, then the second traffic class and so on. Therefore, the order in which traffic classes appear in the list affects the QoS behaviour of the policy. A default traffic class is automatically created at the end of the list, and does not need to be configured.

Parameter	Description
POLIcy	Existing policy to which you want to add a traffic class. The <i>id</i> is an integer from 0 to 255. Default: no default
TRAfficclass	Existing traffic class to be added to the traffic class. A traffic class can be added to only one policy. A <i>trafficclass-list</i> consists of: an integer from 0 to 1023 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges Default: no default

Examples To add the traffic classes 1, 2, 3, 4 and 8 to policy 8, use the command:

```
add qos poli=8 tr=1-4,8
```

Related Commands

- [create qos policy](#)
- [delete qos policy](#)
- [destroy qos policy](#)
- [set qos policy](#)
- [set qos port](#)
- [show qos policy](#)

add qos portgroup port

Syntax ADD QOS PORTGroup=*group-list* PORT=*port-list*

Description This command adds ports to an existing port group. A policy can then be attached to the port group.

Parameter	Description
PORTgroup	Port group to which you want to add a port. The <i>group-list</i> consists of: <ul style="list-style-type: none">one or more port groupsa range specified with a hyphen, such as 1-4a comma-separated list of numbers and/or rangesan integer from 1 to 32 Default: no default
PORT	Port to add to the port group. Ports cannot belong to a trunk group or another port group, and must all belong to the same switch instance. The <i>port-list</i> consists of: <ul style="list-style-type: none">one or more portsa range specified with a hyphen, such as 1-4a comma-separated list of numbers and/or ranges Default: no default

Examples To add ports 6 to 9 to port group 1, use the command:

```
add qos portg=1 po=6-9
```

Related Commands

- [create qos portgroup](#)
- [delete qos portgroup port](#)
- [destroy qos portgroup](#)
- [set qos portgroup](#)
- [show qos portgroup](#)

add qos trafficclass

Syntax ADD QOS TRafficclass=*trafficclass-id*
FLowgroup=*flowgroup-list*

Description This command adds one or more QoS data flows to a traffic class.

Parameter	Description
TRafficclass	Existing traffic class to which you want to add a flow group. The <i>trafficclass-id</i> is an integer from 0 to 1023. Default: no default
Flowgroup	Existing flow to be added to the traffic class. A flow group can belong to only one traffic class. The <i>flowgroup-list</i> consists of: an integer from 0 to 1023 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges Default: no default

Examples To add flows 1, 2, 3, 4 and 9 to the traffic class 42, use the command:

```
add qos tr=42 fl=1-4,9
```

Related Commands [create qos trafficclass](#)
[delete qos trafficclass](#)
[destroy qos trafficclass](#)
[set qos trafficclass](#)
[show qos trafficclass](#)

create qos flowgroup

Syntax CREate QOS FLOWgroup=*flowgroup-list* [Action={NONE|FORward|FORward,SENDMirror|DIScard|SENDMirror|SENDMirror,SENDVlanport|SENDVlanport}] [DESCRiption=*description*] [MArkvalue={*dscp-value*|NONE}] [PORt=*port*] [PREMarking={USEMarkvalue|USEDscp|NONE}] [VLAN=*vlan-id*]

Description This command creates one or more QoS flow groups with the given identifiers. None of the specified flow groups should already exist.

Parameter	Description										
Flowgroup	Flow group you want to create. The <i>flowgroup-list</i> consists of: an integer from 0 to 1023 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges Default: no default										
Action	Action to be performed on traffic belonging to the flow group. Default: none <table> <tr> <td>NONE</td><td>The action is overridden with the setting of the flow group's traffic class.</td></tr> <tr> <td>FORward</td><td>Normally forwards traffic.</td></tr> <tr> <td>DIScard</td><td>Drops traffic.</td></tr> <tr> <td>SENDVlanport</td><td>Traffic goes to the VLAN specified by the vlan parameter and the port specified by the port parameter. Both vlan and port must also be specified. The VLAN must exist and the port must be a member of that VLAN. The switch determines whether the port is tagged or untagged for that VLAN and sends traffic accordingly.</td></tr> <tr> <td>SENDMirror</td><td>Traffic goes to the preconfigured mirror port. This option lets you mirror packets classified on any port. It is more flexible than standard mirroring, which only monitors traffic on a single port. You can also forward mirrored traffic normally, discard it, or send it to a particular port and VLAN.</td></tr> </table>	NONE	The action is overridden with the setting of the flow group's traffic class.	FORward	Normally forwards traffic.	DIScard	Drops traffic.	SENDVlanport	Traffic goes to the VLAN specified by the vlan parameter and the port specified by the port parameter. Both vlan and port must also be specified. The VLAN must exist and the port must be a member of that VLAN. The switch determines whether the port is tagged or untagged for that VLAN and sends traffic accordingly.	SENDMirror	Traffic goes to the preconfigured mirror port. This option lets you mirror packets classified on any port. It is more flexible than standard mirroring, which only monitors traffic on a single port. You can also forward mirrored traffic normally, discard it, or send it to a particular port and VLAN.
NONE	The action is overridden with the setting of the flow group's traffic class.										
FORward	Normally forwards traffic.										
DIScard	Drops traffic.										
SENDVlanport	Traffic goes to the VLAN specified by the vlan parameter and the port specified by the port parameter. Both vlan and port must also be specified. The VLAN must exist and the port must be a member of that VLAN. The switch determines whether the port is tagged or untagged for that VLAN and sends traffic accordingly.										
SENDMirror	Traffic goes to the preconfigured mirror port. This option lets you mirror packets classified on any port. It is more flexible than standard mirroring, which only monitors traffic on a single port. You can also forward mirrored traffic normally, discard it, or send it to a particular port and VLAN.										
DESCRiption	Description of the flow group to be created. The <i>description</i> consists of: a string 1 to 15 characters long any printable characters double quotes if it contains spaces Default: no default										
MArkvalue	Value to use as an index into the DSCP MAP table when the premarking parameter is set to usemarkvalue . Default: none <table> <tr> <td><i>dscp-value</i></td><td>Integer from 0 to 63 for a valid DSCP.</td></tr> <tr> <td>NONE</td><td>Premarking is not used by setting the markvalue parameter although it can still be set with premarking=usedscp.</td></tr> </table>	<i>dscp-value</i>	Integer from 0 to 63 for a valid DSCP.	NONE	Premarking is not used by setting the markvalue parameter although it can still be set with premarking=usedscp .						
<i>dscp-value</i>	Integer from 0 to 63 for a valid DSCP.										
NONE	Premarking is not used by setting the markvalue parameter although it can still be set with premarking=usedscp .										

Parameter (cont.)	Description (cont.)
Port	Port where traffic is sent when action=sendvlanport . The port must belong to the VLAN specified by the vlan parameter
PREMarking	<p>Action to take on the flow group before traffic class bandwidth metering is applied. Values for premarking and markvalue in a flow group override the setting for the traffic class.</p> <p>Default: none</p>
USEMarkvalue	Settings for the flow are selected from the DSCP MAP table using markvalue and a bandwidth class of 1
USEDscp	Settings for the flow are selected from the DSCP MAP table using the DSCP value in the matching data frames and a bandwidth class value of 1.
NONE	The flow is passed to the traffic class stage.
VLAN	Where traffic is sent when action=sendvlanport . Traffic is sent out the port specified by the port parameter, so the VLAN must contain this port. The <i>vlan-id</i> is an integer from 1 to 4094.

Examples To create QoS flow group number 50 with a description of *myFlowGroup*, and set it to premark all member (classifier-matching) frames with the DSCP MAP values for a DSCP value of 32, and to send this traffic to the mirror port, use the command:

```
cre qos fl=50 desc=myFlowGroup prem=usem ma=32
    action=sendmirror
```

Related Commands

- [add qos flowgroup](#)
- [delete qos flowgroup](#)
- [destroy qos flowgroup](#)
- [set qos dscpmap](#)
- [set qos flowgroup](#)
- [show qos dscpmap](#)
- [show qos flowgroup](#)

create qos policy

Syntax CREate QOS POLIcy=*id-list* [DESCRiption=*description*]
 [DTCAction={FORward|FORward, SENDMirror|DIScard|
 SENDMirror|SENDMirror, SENDVlanport|SENDVlanport}]]
 [DTCDRopbwclass3={OFF|NO|False|ON|YES|True}]]
 [DTCIgnorebwclass={OFF|NO|False|ON|YES|True}]]
 [DTCMAXBAndwidth={*bandwidth*|NONE}]]
 [DTCMAXBUrstsiz=*burstsize*]
 [DTCMINBAndwidth={*bandwidth*|NONE}]]
 [DTCMINBUrstsiz=*burstsize*]
 [DTCPRemarking={USEMarkvalue|USEDscp|NONE}]]
 [DTCREmarking={USEDSCPMap|BWClass|NONE}]]
 [DTCSTORMStatus={ENable|DISable}]]
 [DTCSTORMWindow={*window size*|NONE}]]
 [DTCSTORMRate={Rate|NONE}]]
 [DTCSTORMAction={LINKDown|PORTdisable}]]
 [DTCSTORMTimeout={*timeout length*|NONE}]]
 [Markvalue={*dscp-value*|NONE}]]
 [Port=*port*] [VLAN=*vlan-id*]

Description This command creates one or more new QoS policies, and lets you enable storm protection. For more information about bandwidth metering, see [“Bandwidth conformance classes” on page 27-25](#).

You can also specify settings for the default traffic class (DTC) with this command. The default traffic class processes unclassified traffic on the policy's port.

Parameter	Description
POLlcy	<p>The <i>id-list</i> is a specific policy to create that consists of:</p> <ul style="list-style-type: none"> an integer from 0 to 255 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges <p>Default: no default</p>
DESCRiption	<p>Text that describes the policy being created and consists of:</p> <ul style="list-style-type: none"> a string 1 to 15 characters long any printable character <p>If <i>description</i> contains spaces, it must be in double quotes.</p> <p>Default: no default</p>

Parameter (cont.)	Description (cont.)
DTCAction	<p>Action to be performed on traffic that is processed by the default traffic class.</p> <p>Default: forward</p>
FORward	Forwarded normally.
DIScard	Dropped.
SENDVlanport	<p>Sends traffic to the VLAN specified by the vlan parameter and the port specified by the port parameter. Both vlan and port must also be specified. The VLAN must exist and the specified port must be a member of that VLAN.</p> <p>The switch determines whether the port is tagged or untagged for that VLAN, and sends traffic with the correct tag if the port is tagged. If the port is untagged for the specified VLAN, the frame is sent untagged.</p>
SENDMirror	<p>Sends traffic to the preconfigured mirror port. This option lets you mirror packets classified on any port. It is more flexible than standard mirroring, which only monitors traffic on a single port. You can also forward mirrored traffic normally, discard it, or send it to a particular port and VLAN.</p>
DTCDropbwclass3	<p>Whether to drop frames exceeding the default traffic class dtcmaxbandwidth setting.</p> <p>Default: no</p>
YES	Data is dropped immediately if the rate is higher than the combined dtcmaxbandwidth and dtcmaxburstsize settings.
NO	Marks non-conforming traffic as bandwidth class 3 and allows this traffic to be selected for dropping by the RED curve settings, which have a more TCP-friendly algorithm.
DTCIgnorebwclass	<p>Whether the metering stage acknowledges any previous bandwidth class assigned to flows processed by the default traffic class.</p> <p>Default: no</p>
YES	<p>If bandwidth processing (dtcminbandwidth, dtcmaxbandwidth) is active on this traffic class, the metering function ignores any bandwidth class previously assigned to the flow in the premarking stage and sets the meter bandwidth class according to the meter conformance level of the flow.</p>
NO	<p>The meter bandwidth class is temporary unless the bwclass or usedscpmap option is entered for the dtcremarking parameter.</p>

Parameter (cont.)	Description (cont.)
DTCMAXBandwidth	<p>Maximum bandwidth available to the default traffic class. Maximum data rate for bandwidth class 2. If the traffic class is on a policy that is attached to a switch port, the resultant bandwidth must be valid for that port.</p> <p>Default: none</p> <hr/> <p><i>bandwidth</i> Value from 0 to 16 000 000 kbps. This value may be specified in kbps, Mbps or Gbps (in uppercase or lowercase). If no unit is specified, it is read as kbps. If Mbps or Gbps is specified, the value may contain a decimal fraction, for example, 1.25 Mbps.</p> <hr/> <p>NONE No maximum.</p>
DTCMAXBurstsize	<p>Specifies the burst tolerance for the dtcmaxbandwidth parameter. The dtcmaxburstsize parameter determines the maximum amount of data permitted above dtcmaxbandwidth for the traffic class before re-marking to bandwidth class 3 occurs, or frames are dropped depending on the setting of the dtcdropbwclass3 parameter.</p> <p><i>Burstsize</i> is a value from 0 to 16 777 216 bytes. This value may be specified in bytes, kbytes, or Mbytes (in uppercase or lowercase). If no unit is specified, it is read as bytes. If Mbytes is specified, the value may contain a decimal fraction, for example, 1.25 Mbytes. This parameter should always be as large as the largest size packet to be metered on the aggregate flow.</p> <p>Default: 0</p>
DTCMINBandwidth	<p>Specifies the minimum bandwidth reserved for the traffic class. This parameter determines the maximum rate of data in bandwidth class 1.</p> <p>Default: none</p> <hr/> <p><i>bandwidth</i> Value from 0 to 16 000 000 kbps. This value may be specified in kbps, Mbps or Gbps (in uppercase or lowercase). If no unit is specified, it is read as kbps. If Mbps or Gbps is specified, the value may contain a decimal fraction, for example, 1.25 Mbps.</p> <hr/> <p>NONE No minimum.</p>
DTCMINBurstsize	<p>Specifies the burst tolerance for dtcminbandwidth, or for dtcmaxbandwidth when dtcminbandwidth is none. This parameter determines the maximum amount of data permitted above dtcminbandwidth for the traffic class before re-marking to bandwidth class 2 occurs.</p> <p><i>Burstsize</i> is a value from 0 to 16 777 216 bytes. This value may be specified in bytes, kbytes, or Mbytes (in uppercase or lowercase). If no unit is specified, it is read as bytes. If Mbytes is specified, the value may contain a decimal fraction, for example, 1.25 Mbytes. If this parameter is not specified for class 2, its value must be less than the value of dtcmaxburstsize.</p> <p>Default: 0</p>

Parameter (cont.)	Description (cont.)
DTCPRemarking	Specifies the QoS action to take on the default traffic class before bandwidth metering is applied. Default: none
	USEMarkvalue Settings for the flow are selected from the DSCP MAP table using markvalue and a bandwidth class of 1.
	USEDscp Settings for the flow are selected from the DSCP MAP table using the DSCP value in the matching data frames and a bandwidth class value of 1.
	NONE The flow is passed to the metering stage.
DTCREmarking	Specifies the action to take after the metering stage. The metering stage assigns a temporary value of bandwidth class to the flow that is used to determine its per-hop behaviour. Default: none
	USEDSCPMap The temporary value is used (in conjunction with the DSCP of the frame) as an index into DSCP MAP, which then assigns the actual, new values for bandwidth class, DSCP, egress queue, and VLAN Tag User Priority.
	BWClass The temporary bandwidth class becomes the new bandwidth class for the flow.
	NONE No action.
DTCSTORMStatus	Whether storm protection is enabled for the default traffic class. Default: disabled
DTCSTORMWindow	Time between the polling of traffic class counters that checks whether storm protection should be activated. Required when storm protection is enabled. Default: none
	<i>windowsize</i> Number of milliseconds from 100 to 60 000.
	NONE Storm protection is inactive.
DTCSTORMRate	Storm protection is activated when this rate of traffic is exceeded. Required when storm protection is enabled. If the value of dtcstormwindow is less than one second, the rate is averaged over the last second. Default: none
	Rate Bits per second from 1Kbps to 10Gbps, specified in Kbps, Mbps or Gbps. If you do not specify a unit, it uses Kbps. If you specify Mbps or Gbps, the rate may contain a decimal fraction with up to 3 decimal places, for example, 1.25 Mbps.
	NONE Storm protection is inactive.
DTCSTORMAction	Action QoS takes when a storm is detected on a port. Default: portdisable
	LINKDown Operationally disables ports to which the policy is attached.
	PORTdisable Administratively disables ports to which the policy is attached.

Parameter (cont.)	Description (cont.)
DTCSTORMTimeout	Length of time the port remains disabled after a storm is detected. Default: none
<i>timeoutlength</i>	Duration in seconds from 1 to 86400.
NONE	The port remains disabled until you enable it again with the enable switch port command on page 7-94 of Chapter 7, Switching.
MArkvalue	Specifies an explicit value to use as an index into the DSCPMAP table when the dtcpremarking parameter is usemarkvalue . Default: none
<i>dscp-value</i>	An integer from 0 to 63.
NONE	No special index.
Port	Port where unclassified traffic is sent when dtcaction is sendvlanport . The port must belong to the VLAN specified by the vlan parameter.
VLAN	VLAN where unclassified traffic is sent when dtcaction is sendvlanport . Traffic is sent over the port specified by the port parameter so the VLAN must contain that port. <i>Vlan-id</i> is an integer from 1 to 4094.

Examples The following example:

- creates QoS Policy 1 with a description of *myPolicy*
- sets the default traffic class premark, all otherwise unclassified traffic
- DSCPMAP values indicated for a DSCP value of 0
- has no bandwidth class 1 reserve
- has a maximum bandwidth class 2 limit of 10Mbps with 64kbyte burst tolerance and set to drop frames in bandwidth class 3
- includes premetering bandwidth class allocation
- remarks after metering based on DSCPMAP settings
- sends resulting traffic to the mirror port

```
cre qos poli=1 desc=myPolicy dtcdr=yes dtcig=no
    dtcmaxba=10mbps dtcmaxbu=64kbyte dtcre=usedscpm dtcpr=usem
    ma=0 dtca=sendmirror
```

The following command enables storm protection as follows:

- creates QoS Policy 1 with a description of *stormprotection*
- enables storm protection on the policy
- checks traffic every 200 milliseconds
- if the rate has exceeded 50kbps, activates storm protection
- when activated, storm protection operationally disables the port for 60 seconds

```
cre qos poli=1 desc=stormprotection dtcstorms=ena
    dtcstormw=200 dtcstormr=50kbps dtcstorma=linkd
    dtcstormt=60
```

Related Commands

- [add qos policy](#)
- [delete qos policy](#)
- [destroy qos policy](#)
- [set qos policy](#)
- [set qos port](#)
- [show qos policy](#)

create qos portgroup

Syntax `CREate QOS PORTGroup=group-list [Port=port-list]
[DESCription=description]`

Description This command creates a port group so that a policy can be attached to it. A *switch instance* refers to a single switch chip; port groups cannot span multiple switch instances.

Parameter	Description
PORTgroup	Port group that you want to create. The <i>group-list</i> consists of: <ul style="list-style-type: none">one or more port groupsa range specified with a hyphen, such as 1-4a comma-separated list of numbers and/or rangesan integer from 1 to 32 Default: no default
Port	Port to add to this port group. The <i>port-list</i> consists of: <ul style="list-style-type: none">one or more portsa range specified with a hyphen, such as 1-4a comma-separated list of numbers and/or ranges Default: no default
DESCription	Description of the port group. Default: no default

Examples To create port group 1, name it “uplink”, and assign port 3 and ports 5 to 10 to *uplink*, use the command:

```
cre qos portg=1 po=3,5-10 desc=uplink
```

Related Commands

- [add qos portgroup port](#)
- [delete qos portgroup port](#)
- [destroy qos portgroup](#)
- [set qos portgroup](#)
- [show qos portgroup](#)

create qos red

Syntax CREate QOS RED=*red-id* [DESCRiption=*description*]

Description This command creates a set of RED curves and sets all of their parameters to the defaults. RED1 exists at startup and therefore cannot be created or destroyed.

Parameter	Description
RED	RED curve set that you want to create. The <i>red-id</i> is an integer from 2 to 4. Default: no default
DESCRiption	Description of the RED curve set being created that consists of: a string 1 to 15 characters long any printable character If <i>description</i> contains spaces, it must be in double quotes. Default: no default

Examples To create RED curve 2 and label it *Red2*, use the command:

```
cre qos red=2 desc=Red2
```

Related Commands [destroy qos red](#)
[set qos red](#)
[show qos red](#)

create qos trafficclass

Syntax CREate QOS TRafficclass=*trafficclass-list*
 [DESCRiption=*description*] [ACTion={FORward|
 FORward, SENDMirror|DIScard|SENDMirror|
 SENDMirror, SENDVlanport|SENDVlanport}}]
 [DROPBwclass3={OFF|NO|False|ON|YES|True}}]
 [IGNorebwclass3={OFF|NO|False|ON|YES|True}}]
 [Markvalue={*dscp-value*|NONE}}] [MAXbandwidth={*bandwidth*|
 NONE}}] [MAXBUrstsize=*burstsize*]
 [MINbandwidth={*bandwidth*|NONE}}]
 [MINBUrstsize=*burstsize*] [PORt=*port*]
 [PREMarking={USEMarkvalue|USEDscp|NONE}}]
 [REMarking={USEDSCPMap|BWClass|NONE}}]
 [STORMStatus={ENable|DISable}}]
 [STORMWindow={*windowsize*|NONE}}]
 [STORMRate={Rate|NONE}}]
 [STORMAction={LINKDown|Portdisable|VLANDisable}}]
 [STORMTimeout={*timeoutlength*|NONE}}]
 [VLAN=*vlan-id*]

Description This command creates one or more new traffic classes, and lets you enable storm protection. For more information about bandwidth metering, see [“Bandwidth conformance classes” on page 27-25](#).

Parameter	Description
TRafficclass	<p>The <i>trafficclass-list</i> is the traffic class you want to create that consists of:</p> <ul style="list-style-type: none"> an integer from 0 to 1023 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges <p>Default: no default</p>
DESCRiption	<p>Text that describes the traffic class being created and consists of:</p> <ul style="list-style-type: none"> a string 1 to 15 characters long any printable character <p>If <i>description</i> contains spaces, it must be in double quotes.</p> <p>Default: no default</p>

Parameter (cont.)	Description (cont.)
ACtion	Action to be performed on traffic belonging to this traffic class. Default: forward
	FORward Forwarded normally.
	DIScard Dropped.
	SENDVlanport Sends traffic to the VLAN specified by the vlan parameter and the port specified by the port parameter. Both vlan and port must also be specified. The VLAN must exist and the specified port must be a member of that VLAN. The switch determines whether the port is tagged or untagged for that VLAN, and sends traffic with the correct tag if the port is tagged. If the port is untagged for the specified VLAN, the frame is sent untagged.
	SENDMirror Sends traffic to the preconfigured mirror port. This option lets you mirror packets classified on any port. It is more flexible than standard mirroring, which only monitors traffic on a single port. You can also forward mirrored traffic normally, discard it, or send it to a particular port and VLAN.
DROPBwclass3	Whether to drop frames exceeding the traffic class maxbandwidth setting. Default: no
	YES Data is dropped immediately if the rate is higher than the combined maxbandwidth and maxburstsize settings.
	NO Marks non-conforming traffic as bandwidth class 3 and allows this traffic to be selected for dropping by the RED curve settings, which have a more TCP-friendly algorithm.
IGNorebwclass	Whether the metering stage acknowledges any previous bandwidth class assigned to flows processed by the default traffic class. Default: no
	YES If bandwidth processing (minbandwidth , maxbandwidth) is active on this traffic class, the metering function ignores any bandwidth class previously assigned to the flow in the premarking stage and sets the meter bandwidth class according to the meter conformance level of the flow.
	NO The meter bandwidth class is temporary unless the bwclass or usedscpmap option is entered for the remarking parameter.
MArkvalue	Specifies an explicit value to use as an index into the DSCP MAP table when the premarking parameter is usemarkvalue . Default: none
	<i>dscp-value</i> An integer from 0 to 63.
	NONE No special index.

Parameter (cont.)	Description (cont.)
MAXBAndwidth	<p>Maximum bandwidth available to the traffic class. Maximum data rate for bandwidth class 2. If the traffic class is on a policy that is attached to a switch port, the resultant bandwidth must be valid for that port.</p> <p>Default: none</p> <hr/> <p><i>bandwidth</i> Value from 0 to 16 000 000 kbps. This value may be specified in kbps, Mbps or Gbps (in uppercase or lowercase). If no unit is specified, it is read as kbps. If Mbps or Gbps is specified, the value may contain a decimal fraction, for example, 1.25 Mbps.</p> <hr/> <p>NONE No maximum.</p>
MAXBUrsize	<p>Specifies the burst tolerance for the maxbandwidth parameter. The maxburstsize parameter determines the maximum amount of data permitted above maxbandwidth for the traffic class before re-marking to bandwidth class 3 occurs, or frames are dropped depending on the setting of the dropbwclass3 parameter.</p> <p><i>Burstsize</i> is a value from 0 to 16 777 216 bytes. This value may be specified in bytes, kbytes, or Mbytes (in uppercase or lowercase). If no unit is specified, it is read as bytes. If Mbytes is specified, the value may contain a decimal fraction, for example, 1.25 Mbytes. This parameter should always be as large as the largest size packet to be metered on the aggregate flow.</p> <p>Default: 0</p>
MINBAndwidth	<p>Specifies the minimum bandwidth reserved for the traffic class. This parameter determines the maximum rate of data in bandwidth class 1.</p> <p>Default: none</p> <hr/> <p><i>bandwidth</i> Value from 0 to 16 000 000 kbps. This value may be specified in kbps, Mbps or Gbps (in uppercase or lowercase). If no unit is specified, it is read as kbps. If Mbps or Gbps is specified, the value may contain a decimal fraction, for example, 1.25 Mbps.</p> <hr/> <p>NONE No minimum.</p>
MINBUrsize	<p>Specifies the burst tolerance for minbandwidth, or for maxbandwidth when minbandwidth is none. This parameter determines the maximum amount of data permitted above minbandwidth for the traffic class before re-marking to bandwidth class 2 occurs.</p> <p><i>Burstsize</i> is a value from 0 to 16 777 216 bytes. This value may be specified in bytes, kbytes, or Mbytes (in uppercase or lowercase). If no unit is specified, it is read as bytes. If Mbytes is specified, the value may contain a decimal fraction, for example, 1.25 Mbytes. If this parameter is not specified for class 2, its value must be less than the value of maxburstsize.</p> <p>Default: 0</p>
Port	<p>Port where unclassified traffic is sent when action is sendvlanport. The port must belong to the VLAN specified by the vlan parameter.</p>

Parameter (cont.)	Description (cont.)
PRemarking	Specifies the QoS action to take on the traffic class before bandwidth metering is applied. Default: none
	USEMarkvalue Settings for the flow are selected from the DSCP MAP table using markvalue and a bandwidth class of 1.
	USEDscp Settings for the flow are selected from the DSCP MAP table using the DSCP value in the matching data frames and a bandwidth class value of 1.
	NONE The flow is passed to the metering stage.
REmarking	Specifies the action to take after the metering stage. The metering stage assigns a temporary value of bandwidth class to the flow that is used to determine its per-hop behaviour. Default: none
	USEDSCPMap The temporary value is used (in conjunction with the DSCP of the frame) as an index into DSCP MAP, which then assigns the actual, new values for bandwidth class, DSCP, egress queue, and VLAN Tag User Priority.
	BWClass The temporary bandwidth class becomes the new bandwidth class for the flow.
	NONE No action.
STORMStatus	Whether storm protection is enabled for the default traffic class. Default: disabled
STORMWindow	Time between the polling of traffic class counters that checks whether storm protection should be activated. Required when storm protection is enabled. Default: none
	<i>window size</i> Number of milliseconds from 100 to 60 000.
	NONE Storm protection is inactive.
STORMRate	Storm protection is activated when this rate of traffic is exceeded. Required when storm protection is enabled. If the value of stormwindow is less than one second, the rate is averaged over the last second. Default: none
	Rate Bits per second from 1Kbps to 10Gbps, specified in Kbps, Mbps or Gbps. If you do not specify a unit, it uses Kbps. If you specify Mbps or Gbps, the rate may contain a decimal fraction with up to 3 decimal places, for example, 1.25 Mbps.
	NONE Storm protection is inactive.

Parameter (cont.)	Description (cont.)
STORMAction	Action QoS takes when a storm is detected on a port. Default: portdisable
LINKDown	Operationally disables ports to which the traffic class is attached.
POrtdisable	Administratively disables ports to which the traffic class is attached.
VLANdisable	Administratively disables ports to which the traffic class is attached for the VLAN on which the classifier is matching.
STORMTimeout	Length of time the port remains disabled after a storm is detected. Default: none
timeoutlength	Duration in seconds from 1 to 86400.
NONE	The port remains disabled until you enable it again with the enable switch port command on page 7-94 or the enable switch port vlan command on page 7-95 of Chapter 7, Switching.
VLAN	VLAN where unclassified traffic is sent when action is sendvlanport . Traffic is sent over the port specified by the port parameter so the VLAN must contain that port. <i>Vlan-id</i> is an integer from 1 to 4094.

Examples The following command:

- creates QoS traffic class number 10 with a description of *myTrafficClass*
- sets the traffic class to premark all member flows (not previously marked by their flow group) according to the DSCPMAP values indicated by a DSCP value of 10
- has a bandwidth class 1 bandwidth reserve of 1Mbps with 64kbytes burst tolerance
- sets a maximum bandwidth class 2 limit of 2Mbps with 64kbyte burst tolerance
- sets it to drop frames in bandwidth class 3
- ignores premetering bandwidth class allocation
- has a meter-based re-marking based on DSCPMAP settings
- sends this traffic to the mirror port

```
cre qos tr=10 desc=myTrafficClass prem=usem ma=10 min=1mb
minbu=64kb max=2mb maxbu=64kb dropb=yes ign=yes
rem=usedscpm action=sendmirror
```

The following command enables storm protection as follows:

- creates QoS traffic class 1 with a description of *stormprotection*
- enables storm protection on the traffic class
- checks traffic every 200 milliseconds
- if the rate exceeds 50kbps, then activates storm protection
- when activated, storm protection operationally disables the port for 60 seconds

```
cre qos tr=1 desc=stormprotection storms=ena stormw=200
stormr=50kbps storma=linkd stormt=60
```

Related Commands

- add qos trafficclass
- delete qos trafficclass
- destroy qos trafficclass
- set qos trafficclass
- show qos trafficclass

delete qos flowgroup

Syntax `DELEte QOS FLOWgroup=flowgroup-id
CLASSifier={classifier-list|ALL}`

Description This command deletes all classifiers from a flow group or specific ones.

Parameter	Description
Flowgroup	Flow group from which you want to delete a classifier. The <i>flowgroup-id</i> consists of an integer from 0 to 1023. Default: no default
CLASSifier	Classifier to delete from this flow group. The classifier must belong to this flow group. Default: no default <i>classifier-list</i> Specific classifier that consists of: an integer from 1 to 9999 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges
ALL	Deletes all classifiers belonging to the flow group.

Examples To delete classifiers 2, 3, 4, 5 and 6 from flow group 42 use the command:

```
del qos fl=42 class=2-6
```

Related Commands

- [add qos flowgroup](#)
- [create classifier](#)
- [create qos flowgroup](#)
- [destroy qos flowgroup](#)
- [set qos flowgroup](#)
- [show qos flowgroup](#)

delete qos policy

Syntax `DELEte QOS POLIcy=id TRAfficclass={trafficclass-list|ALL}`

Description This command deletes all traffic classes from a QoS policy or specific ones.

Parameter	Description
POLIcy	Policy from which you want to delete a traffic class. The <i>id</i> can be an integer from 0 to 255. Default: no default
TRAfficclass	Traffic class to delete from this policy. The traffic class must belong to this policy. Default: no default <i>trafficclass-list</i> Specific traffic class that consists of: an integer from 0 to 1023 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges
ALL	Deletes all flow groups belonging to the traffic class.

Examples To delete the traffic classes 1, 2, 3, 4 and 8 from policy 8, use the command:

```
del qos poli=8 tr=1-4,8
```

Related Commands

- [add qos policy](#)
- [create qos policy](#)
- [destroy qos policy](#)
- [set qos policy](#)
- [set qos port](#)
- [show qos policy](#)

delete qos portgroup port

Syntax `DELEte QOS PORTGroup=group-id PORT={port-list|ALL}`

Description This command deletes specific ports from a port group, or all ports belonging to a port group.

Parameter	Description
PORTgroup	Port group from which you want to delete a port. The <i>group-id</i> can be an integer from 1 to 32. Default: no default
Port	Port to delete from this port group. Default: no default
<i>port-list</i>	Specific port that consists of: one or more ports a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges
ALL	All ports belonging to the port group are deleted.

Examples To delete all ports from the port group 1, use the command:

```
del qos portg=1 po=all
```

Related Commands

- [add qos portgroup port](#)
- [create qos portgroup](#)
- [destroy qos portgroup](#)
- [set qos portgroup](#)
- [show qos portgroup](#)

delete qos trafficclass

Syntax DELEte QOS TRAfficclass=*trafficclass-id*
FLOwgroup={*flowgroup-list* | ALL}

Description This command deletes specific flow groups from a traffic class or all flow groups belonging to a traffic class.

Parameter	Description
TRAfficclass	Traffic class from which you want to delete a flow group. The <i>trafficclass-id</i> consists of an integer from 0 to 1023. Default: no default
FLOwgroup	Flow group to delete from this traffic class. Default: no default <i>flowgroup-list</i> Specific flow group that consists of: an integer from 0 to 1023 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges
ALL	Deletes all flow groups belonging to the traffic class.

Examples To delete the flow groups 3, 4, 5, 6 and 9 from traffic class 42, use the command:

```
del qos tr=42 fl=3-6,9
```

To delete all flows from traffic class 42, use the command:

```
del qos tr=42 fl=all
```

Related Commands [add qos trafficclass](#)
[create qos trafficclass](#)
[destroy qos trafficclass](#)
[set qos trafficclass](#)
[show qos trafficclass](#)

destroy qos flowgroup

Syntax DESTroy QOS FLOWgroup={*flowgroup-list*|ALL}

Description This command destroys flow groups, which simply unlinks classifiers because QoS components are created as individual elements.

Parameter	Description
Flowgroup	Existing flow group that you want to destroy. Default: no default
<i>flowgroup-list</i>	Specific flow group that consists of: an integer from 0 to 1023 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges
ALL	Destroys all flow groups.

Examples To destroy Flow 42 use the command:

```
dest qos fl=42
```

To destroy the flow groups 2, 4, 7, 8, 9 and 10 use the command:

```
dest qos fl=2,4,7-10
```

To destroy all flow groups, use the command:

```
dest qos fl=all
```

Related Commands [add qos flowgroup](#)
[create qos flowgroup](#)
[set qos flowgroup](#)
[show qos flowgroup](#)

destroy qos policy

Syntax DESTroy QOS POLIcy={*policy-list*|ALL}

Description This command destroys all QoS policies or specific ones.

Parameter	Description
POLIcy	Policy you want to destroy. Default: no default
<i>policy-list</i>	Specific policy that consists of: an integer from 0 to 255 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges
ALL	All policies.

Examples To destroy QoS policy 42, use the command:

```
dest qos poli=42
```

```
dest qos poli=42
```

To destroy the QoS policies 1, 5, 6, 7, 8 and 42, use the command:

```
dest qos poli=1,5-8,42
```

To destroy all user-created QoS policies, use the command:

```
dest qos poli=all
```

Related Commands [add qos policy](#)
[create qos flowgroup](#)
[delete qos policy](#)
[set qos policy](#)
[set qos port](#)
[show qos policy](#)

destroy qos portgroup

Syntax DESTroy QOS PORTGroup=*group-list*

Description This command destroys port groups. No ports can belong to any you want to destroy. The *group-list* consists of:

- one or more port groups
- a range specified with a hyphen, such as 1-4
- a comma-separated list of numbers and/or ranges
- an integer from 1 to 32

Examples To destroy the port group 1, use the command:

```
dest qos portg=1
```

Related Commands [add qos portgroup port](#)
[create qos portgroup](#)
[delete qos portgroup port](#)
[set qos portgroup](#)
[show qos portgroup](#)

destroy qos red

Syntax DESTroy QOS RED={*red-list* | ALL}

Description This command destroys all RED curves or specific ones. See [“RED Curves” on page 27-19](#) for more information.

Parameter	Description
RED	RED curve set you want to destroy. It must not be in use by a port. Default: no default
<i>red-list</i>	Specific RED curve set that consists of: <ul style="list-style-type: none">an integer from 2 to 4a range specified with a hyphen, such as 2-4a comma-separated list of numbers and/or ranges
ALL	Destroys all RED curves except the default RED curve set.

Examples To destroy RED curve set number 4, use the command:

```
dest qos red=4
```

To destroy all RED curves except the default set, use the command:

```
dest qos red=all
```

Related Commands [create qos red](#)
[set qos red](#)
[show qos red](#)

destroy qos trafficclass

Syntax DESTroy QOS TRafficclass={ *trafficclass-list* | ALL }

Description This command destroys traffic classes, which simply unlinks flow groups because QoS components are created as individual elements.

Parameter	Description
TRafficclass	Existing traffic class that you want to destroy. Default: no default
<i>trafficclass-list</i>	Specific traffic class that consists of: an integer from 0 to 1023 a range specified with a hyphen, such as 2-4 a comma-separated list of numbers and/or ranges
ALL	Destroys all traffic classes.

Examples To destroy the traffic class 42 use the command:

```
dest qos tr=42
```

To destroy the traffic classes 2, 4, 7, 8, 9, and 10 use the command:

```
dest qos tr=2,4,7-10
```

To destroy all traffic classes, use the command:

```
dest qos tr=all
```

Related Commands

- [add qos trafficclass](#)
- [create qos trafficclass](#)
- [delete qos trafficclass](#)
- [set qos trafficclass](#)
- [show qos trafficclass](#)

disable qos debug

Syntax `DISable QOS DEBug={COMmand | DETail | TRAcE | ALL}`

Description This command disables output of QoS debug messages.

Parameter	Description
DEBug	Disables specific type of messages. Default: all
COMmand	Disables command handler trace debugging
DETail	Disables additional low level debugging
TRAcE	Disables all QoS trace debugging
ALL	Disables all debugging.

Examples To disable command debugging, use the command:

```
dis qos deb=command
```

Related Commands [enable qos debug](#)

enable qos debug

Syntax `ENABle QOS DEBug={COMmand | DETail | TRAcE | ALL}`

Description This command enables the output of QoS debug messages.

Parameter	Description
DEBug	Enables specific type of messages. Default: all
COMmand	Enables command handler trace debugging
DETail	Enables additional low level debugging
TRAcE	Enables all QoS trace debugging
ALL	Enables all debugging.

Examples If any QoS commands fail, enable trace debugging to trace the error by using the command:

```
ena qos deb=trace
```

Related Commands [disable qos debug](#)

purge qos

Syntax `PURge QoS`

Description This command purges the current QoS configuration.

Example To purge the current QoS configuration, use the command:

```
pur qos
```

reset qos accelerator counters

Syntax `RESET QOS ACCElerator COUnTERS`
`TRafficclass [= { trafficclass-list | DEFault | ALL }]`

Description This command applies to AT-8948 and AT-9924T/4SP switches and resets counters for traffic classes attached to an accelerator card.

Parameter	Description
TRafficclass	Traffic class for which you want to clear counters. Default: default
<i>trafficclass-list</i>	Specific traffic class that consists of: one or more traffic classes a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges an integer from 0 to 1023
DEFault	The default traffic class.
ALL	Resets counters for all traffic classes attached to the accelerator card. Also resets all of them if you enter no value.

Examples To clear counters for traffic classes 1 through 5 attached to port 4, use the command:

```
reset qos accel cou tr=1-5
```

Related Commands [show qos accelerator counters](#)

reset qos port counters

Syntax RESET QOS Port=*port-list* COunters
TRafficclass[={*trafficclass-list* | DEFault | ALL}]

Description This command resets counters for traffic classes attached a port. Use the **set switch enhancedmode** command in the *Switching* chapter to set counters.

Parameter	Description
PORT	Port for which you want to clear counters. The <i>port-list</i> consists of: <ul style="list-style-type: none">one or more portsa range specified with a hyphen, such as 1-4a comma-separated list of numbers and/or ranges Default: no default
TRafficclass	Traffic class counters to clear for this port. Default: default <i>trafficclass-list</i> Specific traffic class that consists of: <ul style="list-style-type: none">one or more traffic classesa range specified with a hyphen, such as 1-4a comma-separated list of numbers and/or rangesan integer from 0 to 1023
DEFault	The default traffic class.
ALL	Resets counters for all traffic classes attached to the port. Also resets all of them if you enter no value.

Examples To clear traffic class counters on traffic classes attached to port 4, use the command:

```
reset qos po=4 cou tr=all
```

Related Commands [set switch enhancedmode](#)
[show qos port counters](#)

reset qos portgroup counters

Syntax RESET QOS PORTGroup=*group-list* COUNters
TRAfficclass[={*trafficclass-list*|DEFAULT|ALL}]

Description This command resets traffic class counters for a port group. Use the **set switch enhancedmode** command in the *Switching* chapter to set counters.

Parameter	Description
PORTgroup	Port group for which you want to clear counters. The <i>group-list</i> consists of: <ul style="list-style-type: none">one or more port groupsa range specified with a hyphen, such as 1-4a comma-separated list of numbers and/or rangesan integer from 1 to 32 Default: no default
TRAfficclass	Traffic class counters to clear for this port group. Default: all <i>trafficclass-list</i> Specific traffic class that consists of: <ul style="list-style-type: none">one or more traffic classesa range specified with a hyphen, such as 1-4a comma-separated list of numbers and/or rangesan integer from 0 to 1023
DEFAULT	The default traffic class.
ALL	Resets counters for all traffic classes attached to the port group. Also resets all of them if you enter no value.

Examples To reset all traffic classes configured on port groups 1, 2, 3, 4, use the command:

```
reset qos portg=1-4 cou tr
```

Related Commands [set switch enhancedmode](#)
[show qos port counters](#)
[show qos portgroup](#)

set qos accelerator policy

Syntax SET QOS ACCElerator POLIcy={*id*|NONE}

Description This command applies to AT-8948 and AT-9924T/4SP switches and applies a QoS policy to packets egressing the IPv6 accelerator card.

Parameter	Description
POLIcy	Specific policy. Default: default
<i>id</i>	Integer from 0 to 255.
NONE	Any QoS policy that is currently applied to the IPv6 accelerator card is removed.

Examples To specify that QoS policy 2 applies to all packets egressing the IPv6 accelerator card, use the command:

```
set qos accel poli=2
```

Related Commands [create qos policy](#)
[set qos port](#)
[show qos policy](#)

set qos defaultpriority

Syntax SET QOS DEFAULtpriority=*q0,q1,q2,q3,q4,q5,q6,q7*

Description This command sets the VLAN Tag User Priority field for frames that were untagged at ingress; that is, frames that were assigned a egress queue according to the port default queue setting. Frames that do not have a User Priority value assigned by any other QoS mechanism (such as DSCPMAP or QUEUE2PRIOMAP) have a value assigned this way.

The **defaultpriority** parameter consists of:

- a comma-separated list of integers 0 to 7
- eight required values

The first value, *q0*, represents the VLAN Tag User Priority corresponding to an internal Class of Service queue of 0, and similarly values *q1* to *q7* represent the VLAN Tag User Priority corresponding to an internal Class of Service queue of 1 to 7.

The default set of values is 1, 2, 0, 3, 4, 5, 6, 7. This is the reverse of the default **prio2queuemap** setting.

Examples To map internal Class of Service queues 0-7 to VLAN Tag User Priority values 0, 0, 0, 3, 4, 5, 7 and 7 respectively, use the command:

```
set qos defau=0,0,0,3,4,5,7,7
```

Related Commands [set qos port](#)
[show qos defaultpriority](#)
[show qos port](#)

set qos dscpmap

Syntax SET QOS DSCPMap={PREmarking|REMarking}} DSCP=*dscp-list*
 [BWclass=*bwclass-list*] [NEWDscp=*dscp-value*]
 [NEWBwclass=*bandwidth-class*] [NEWQueue=*queuenumber*]
 [NEWPriority=*vlan-priority*]

where:

- *bwclass-list* is either an integer from 1 to 3; a range of integers (specified as 1-3), or a comma-separated list of integers and/or ranges, without spaces.
- *bandwidth-class* is an integer from 1 to 3.
- *dscp-list* is either an integer from 0 to 63; a range of integers (specified as 0-4), or a comma-separated list of integers and/or ranges (0,3,4-9,60-63).
- *dscp-value* is an integer from 0 to 63.
- *queuenumber* is an integer from 0 to 7.
- *vlan-priority* is an integer from 0 to 7.

Description This command sets the DSCP-based premarking or re-marking parameters. For each DSCP value, DSCPMap contains three sets of qos parameter values, one per bandwidth class. This lets you specify the per-hop marking and re-marking actions for each frame.

DSCP-based premarking is selected by setting the traffic class or flow group **premarking** parameter to **usedscp**. DSCP-based re-marking is selected by setting the traffic class **remarking** parameter to **usedscpmap**.

The **dscpmap** parameter specifies which of the two DSCP-based QoS marking tables to update. If **premarking** is specified, information related to the flow group and traffic class premarking table is updated. If **remarking** is specified, information for the post-metering re-marking tables is updated. If no value is specified, both tables are updated with the same settings.

The **dscp** parameter specifies the values of DSCP to update with the specified settings. A value must be supplied; there is no default.

The **bwclass** parameter specifies the values of the bandwidth class sub-index for which the specified settings should be updated. If this parameter is not specified, the settings apply for all bandwidth class sub-sets under the specified DSCP values. If the parameter is specified a value must be supplied; there is no default.

The **newdscp** parameter specifies the DSCP value to write into each frame selected by its previous DSCP and bandwidth class indexes. The initial value for **newdscp** is the same as the DSCPMap index value, i.e. entries relating to a DSCPMap index of 25 contain NEWDSCP of 25 at start-up. If **newdscp** is specified, a value must be supplied; there is no default.

The **newbwclass** parameter specifies the new bandwidth class to associate with each frame selected by its previous DSCP and bandwidth class indexes. The initial value for this parameter is the same as the **bwclass** index value, i.e. entries relating to a **bwclass** index of 1 contains NEWDSCP of 1 at startup. If **newbwclass** is specified, a value must be supplied; there is no default.

The **newqueue** parameter specifies the new internal queue to associate with each frame selected by its previous DSCP and bandwidth class indexes. The initial value for this parameter is 0. If specified, a value must be supplied; there is no default.

The **newpriority** parameter specifies the new VLAN Tag User Priority to use for each frame selected by its previous DSCP and bandwidth class indexes. The initial value for this parameter is 0. If specified, a value must be supplied; there is no default.

Examples To set the DSCPMAP so that incoming DSCP values between 32 and 48 that fall into bandwidth class 2 (over minimum reserve at metering stage), have their DSCP remarked to 49, new bandwidth class of 3 (high probability of dropping), a new internal queue of 0, and a new 802.1p priority of 1, use the command:

```
set qos dscpm=rem dscp=32-48 bwc=2 newd=49 newb=3 newq=0
newp=1
```

Related Commands

- [create qos flowgroup](#)
- [create qos trafficclass](#)
- [set qos flowgroup](#)
- [set qos trafficclass](#)
- [show qos dscpmap](#)

set qos fabric queue

Syntax SET QOS FABric QUEue={*queue-list*|all}
[SCHeduler={STrict|WRR}] [WRRweight=1..30]

Description This command specifies the scheduling method for one or more fabric queues on the x900-24X switch.

Parameter	Description
QUEue	Fabric queue to configure. Default: no default
<i>queue-list</i>	Specific fabric queue that consists of: one queue a range specified with a hyphen, such as 1-3 a comma-separated list of numbers and/or ranges
ALL	All fabric queues.
SCHeduler	The scheduling method by which frames on each fabric queue are allocated bandwidth for transmission onto the line. For details about scheduling methods, see “Scheduling Queues” on page 27-31 . Default: no default (but initial state is strict)
STrict	A strict priority algorithm so that fabric queues with higher numbers have priority over others. For example, when both fabric queues 3 and 1 are set to strict , fabric queue 3 has precedence over fabric queue 1. When fabric queue 3 is set to strict and fabric queue 1 is set to wrr , fabric queue 3 has priority.
WRR	A weighted round robin algorithm so that fabric queues take turns based on the value of wrrweight .
WRRweight	An integer from 1 to 30 that assigns a weight for each fabric queue to use in weighted round robin (WRR) scheduling. By setting this parameter, you set the scheduling method to WRR. Default: no default

Examples To schedule fabric queues 0 and 1 to be queued in equal turns (round robin), use the command:

```
set qos fab que=0,1 sch=wrr wrr=1
```

To assign a weight of 2 to fabric queue 2 when it is queued as weighted round robin, use the command:

```
set qos fab que=2 sch=wrr wrr=2
```

To schedule fabric queues from 1 to 3 to be processed in strict priority, use the command:

```
set qos fab que=1-3 sch=st
```

Related Commands [set qos fabric queuemap](#)
[set qos port egressqueue](#)
[show qos fabric](#)

set qos fabric queuemap

Syntax SET QOS FABric QUEUEMap=*q0,q1,q2,q3,q4,q5,q6,q7*

Description This command maps egress queues to fabric queues on the x900-24X switch. There are eight egress queues on each switch port but only four fabric queues.

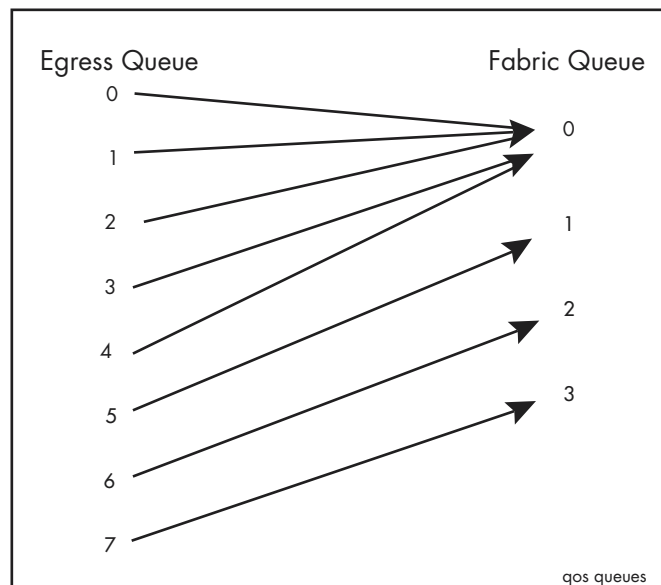
The **queuemap** parameter specifies a comma-separated list of eight values that identify fabric queues. Values must be integers from 0 to 3, and all eight are required. The *qn* value specifies which fabric queue you want to map to egress queue *n*, as shown in the following table.

The value for...	Maps that fabric queue to this egress queue...	Defaults are...
q0	0	0
q1	1	0
q2	2	1
q3	3	1
q4	4	2
q5	5	2
q6	6	3
q7	7	3

Examples To map egress queues 5 through 7 to fabric queues 1 through 3, and then map the remaining egress queues to fabric queue 0, use the command:

```
set qos fab queuem=0,0,0,0,0,1,2,3
```

The following figure shows these mappings:



Related Commands [set qos fabric queue](#)
[show qos fabric](#)

set qos flowgroup

Syntax SET QOS Flowgroup=*flowgroup-list* [Action={NONE|FORward|FORward,SENDMirror|DIScard|SENDMirror|SENDMirror,SENDVlanport|SENDVlanport}] [DESCription=*description*] [MArkvalue={*dscp-value*|NONE}] [PORT=*port*] [PREMarking={USEMarkvalue|USEDscp|NONE}] [VLAN=*vlan-id*]

Description This command modifies parameters on one or more existing flow groups.

Parameter	Description										
Flowgroup	Flow group you want to create. The <i>flowgroup-list</i> consists of: <ul style="list-style-type: none"> an integer from 0 to 1023 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges Default: no default										
Action	Action to be performed on traffic belonging to the flow group. Default: none <table border="1"> <tr> <td>NONE</td><td>The action is overridden with the setting of the flow group's traffic class.</td></tr> <tr> <td>FORward</td><td>Normally forwards traffic.</td></tr> <tr> <td>DIScard</td><td>Drops traffic.</td></tr> <tr> <td>SENDVlanport</td><td>Traffic goes to the VLAN specified by the vlan parameter and the port specified by the port parameter. Both vlan and port must also be specified. The VLAN must exist and the port must be a member of that VLAN. The switch determines whether the port is tagged or untagged for that VLAN and sends traffic accordingly.</td></tr> <tr> <td>SENDMirror</td><td>Traffic goes to the preconfigured mirror port. This option lets you mirror packets classified on any port. It is more flexible than standard mirroring, which only monitors traffic on a single port. You can also forward mirrored traffic normally, discard it, or send it to a particular port and VLAN.</td></tr> </table>	NONE	The action is overridden with the setting of the flow group's traffic class.	FORward	Normally forwards traffic.	DIScard	Drops traffic.	SENDVlanport	Traffic goes to the VLAN specified by the vlan parameter and the port specified by the port parameter. Both vlan and port must also be specified. The VLAN must exist and the port must be a member of that VLAN. The switch determines whether the port is tagged or untagged for that VLAN and sends traffic accordingly.	SENDMirror	Traffic goes to the preconfigured mirror port. This option lets you mirror packets classified on any port. It is more flexible than standard mirroring, which only monitors traffic on a single port. You can also forward mirrored traffic normally, discard it, or send it to a particular port and VLAN.
NONE	The action is overridden with the setting of the flow group's traffic class.										
FORward	Normally forwards traffic.										
DIScard	Drops traffic.										
SENDVlanport	Traffic goes to the VLAN specified by the vlan parameter and the port specified by the port parameter. Both vlan and port must also be specified. The VLAN must exist and the port must be a member of that VLAN. The switch determines whether the port is tagged or untagged for that VLAN and sends traffic accordingly.										
SENDMirror	Traffic goes to the preconfigured mirror port. This option lets you mirror packets classified on any port. It is more flexible than standard mirroring, which only monitors traffic on a single port. You can also forward mirrored traffic normally, discard it, or send it to a particular port and VLAN.										
DESCription	Description of the flow group to be created. The <i>description</i> consists of: <ul style="list-style-type: none"> a string 1 to 15 characters long any printable characters double quotes if it contains spaces Default: no default										
MArkvalue	Value to use as an index into the DSCP MAP table when the premarking parameter is set to usemarkvalue . Default: none <table border="1"> <tr> <td><i>dscp-value</i></td><td>Integer from 0 to 63 for a valid DSCP.</td></tr> <tr> <td>NONE</td><td>Premarking is not used by setting the markvalue parameter although it can still be set with premarking=usedscp.</td></tr> </table>	<i>dscp-value</i>	Integer from 0 to 63 for a valid DSCP.	NONE	Premarking is not used by setting the markvalue parameter although it can still be set with premarking=usedscp .						
<i>dscp-value</i>	Integer from 0 to 63 for a valid DSCP.										
NONE	Premarking is not used by setting the markvalue parameter although it can still be set with premarking=usedscp .										
PORT	Port where traffic is sent when action=sendvlanport . The port must belong to the VLAN specified by the vlan parameter										

Parameter (cont.)	Description (cont.)
PREMarking	Action to take on the flow group before traffic class bandwidth metering is applied. Values for premarking and markvalue in a flow group override the setting for the traffic class. Default: none
USEMarkvalue	Settings for the flow are selected from the DSCP MAP table using markvalue and a bandwidth class of 1
USEDscp	Settings for the flow are selected from the DSCP MAP table using the DSCP value in the matching data frames and a bandwidth class value of 1.
NONE	The flow is passed to the traffic class stage.
VLAN	Where traffic is sent when action=sendvlanport . Traffic is sent out the port specified by the port parameter, so the VLAN must contain this port. The <i>vlan-id</i> is an integer from 1 to 4094.

Examples To change QoS flow groups 5, and 10 through 15 inclusive, to use 50 as the index into the DSCP MAP table, and send this traffic to the mirror port, use the command:

```
set qos fl=5,10-15 ma=50 action-sendmirror
```

Related Commands

- [add qos flowgroup](#)
- [create qos flowgroup](#)
- [delete qos flowgroup](#)
- [destroy qos flowgroup](#)
- [show qos dscpmap](#)
- [show qos flowgroup](#)

set qos policy

Syntax SET QOS POLIcy=*id-list* [DESCRiption=*description*]
 [DTCAction={FORward|FORward,SEnDMirror|DIScard|SEnDMirror|SEnDMirror,SEnDVlanport|SEnDVlanport}]
 [DTCDRopbwclass3={OFF|NO|False|ON|YES|True}]
 [DTCIGnorebwclass={OFF|NO|False|ON|YES|True}]
 [DTCMAXBAndwidth={*bandwidth*|NONE}]
 [DTCMAXBUrstsiz=*burstsize*]
 [DTCMINBAndwidth={*bandwidth*|NONE}]
 [DTCMINBUrstsiz=*burstsize*]
 [DTCPRemarking={USEMarkvalue|USEDscp|NONE}]
 [DTCREmarking={USEDSCPMap|BWClass|NONE}]
 [DTCSTORMStatus={ENable|DISable}]
 [DTCSTORMWindow={*window size*|NONE}]
 [DTCSTORMRate={Rate|NONE}]
 [DTCSTORMAction={LINKDown|PORTdisable}]
 [DTCSTORMTimeout={*timeout length*|NONE}]
 [Markvalue={*dscp-value*|NONE}]
 [Port=*port*] [VLAN=*vlan-id*]

Description This command changes parameters about default traffic classes on one or more QoS policies. You can also change storm protection parameters with this command. For a description of bandwidth metering, see [“Bandwidth conformance classes” on page 27-25](#).

Parameter	Description
POLIcy	<p>The <i>id-list</i> is the policy you want to change, and consists of:</p> <ul style="list-style-type: none"> an integer from 0 to 255 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges <p>Default: no default</p>
DESCRiption	<p>Text that describes the policy being changed and consists of:</p> <ul style="list-style-type: none"> a string 1 to 15 characters long any printable character <p>If <i>description</i> contains spaces, it must be in double quotes.</p> <p>Default: no default</p>

Parameter (cont.)	Description (cont.)
DTCAction	<p>Action to be performed on traffic that is processed by the default traffic class.</p> <p>Default: forward</p>
FORward	Forwarded normally.
DIScard	Dropped.
SENDVlanport	<p>Sends traffic to the VLAN specified by the vlan parameter and the port specified by the port parameter. Both vlan and port must also be specified. The VLAN must exist and the specified port must be a member of that VLAN.</p> <p>The switch determines whether the port is tagged or untagged for that VLAN, and sends traffic with the correct tag if the port is tagged. If the port is untagged for the specified VLAN, the frame is sent untagged.</p>
SENDMirror	<p>Sends traffic to the preconfigured mirror port. This option lets you mirror packets classified on any port. It is more flexible than standard mirroring, which only monitors traffic on a single port. You can also forward mirrored traffic normally, discard it, or send it to a particular port and VLAN.</p>
DTCDropbwclass3	<p>Whether to drop frames exceeding the default traffic class dtcmaxbandwidth setting.</p> <p>Default: no</p>
YES	Data is dropped immediately if the rate is higher than the combined dtcmaxbandwidth and dtcmaxburstsize settings.
NO	Marks non-conforming traffic as bandwidth class 3 and allows this traffic to be selected for dropping by the RED curve settings, which have a more TCP-friendly algorithm.
DTCIgnorebwclass	<p>Whether the metering stage acknowledges any previous bandwidth class assigned to flows processed by the default traffic class.</p> <p>Default: no</p>
YES	<p>If bandwidth processing (dtcminbandwidth, dtcmaxbandwidth) is active on this traffic class, the metering function ignores any bandwidth class previously assigned to the flow in the premarking stage and sets the meter bandwidth class according to the meter conformance level of the flow.</p>
NO	<p>The meter bandwidth class is temporary unless the bwclass or usedscpmap option is entered for the dtcremarking parameter.</p>

Parameter (cont.)	Description (cont.)
DTCMAXBandwidth	<p>Maximum bandwidth available to the default traffic class. Maximum data rate for bandwidth class 2. If the traffic class is on a policy that is attached to a switch port, the resultant bandwidth must be valid for that port.</p> <p>Default: none</p> <hr/> <p><i>bandwidth</i> Value from 0 to 16 000 000 kbps. This value may be specified in kbps, Mbps or Gbps (in uppercase or lowercase). If no unit is specified, it is read as kbps. If Mbps or Gbps is specified, the value may contain a decimal fraction, for example, 1.25 Mbps.</p> <hr/> <p>NONE No maximum.</p>
DTCMAXBurstsize	<p>Specifies the burst tolerance for the dtcmaxbandwidth parameter. The dtcmaxburstsize parameter determines the maximum amount of data permitted above dtcmaxbandwidth for the traffic class before re-marking to bandwidth class 3 occurs, or frames are dropped depending on the setting of the dtcdropbwclass3 parameter.</p> <p><i>Burstsize</i> is a value from 0 to 16 777 216 bytes. This value may be specified in bytes, kbytes, or Mbytes (in uppercase or lowercase). If no unit is specified, it is read as bytes. If Mbytes is specified, the value may contain a decimal fraction, for example, 1.25 Mbytes. This parameter should always be as large as the largest size packet to be metered on the aggregate flow.</p> <p>Default: 0</p>
DTCMINBandwidth	<p>Specifies the minimum bandwidth reserved for the traffic class. This parameter determines the maximum rate of data in bandwidth class 1.</p> <p>Default: none</p> <hr/> <p><i>bandwidth</i> Value from 0 to 16 000 000 kbps. This value may be specified in kbps, Mbps or Gbps (in uppercase or lowercase). If no unit is specified, it is read as kbps. If Mbps or Gbps is specified, the value may contain a decimal fraction, for example, 1.25 Mbps.</p> <hr/> <p>NONE No minimum.</p>
DTCMINBurstsize	<p>Specifies the burst tolerance for dtcminbandwidth, or for dtcmaxbandwidth when dtcminbandwidth is none. This parameter determines the maximum amount of data permitted above dtcminbandwidth for the traffic class before re-marking to bandwidth class 2 occurs.</p> <p><i>Burstsize</i> is a value from 0 to 16 777 216 bytes. This value may be specified in bytes, kbytes, or Mbytes (in uppercase or lowercase). If no unit is specified, it is read as bytes. If Mbytes is specified, the value may contain a decimal fraction, for example, 1.25 Mbytes. If this parameter is not specified for class 2, its value must be less than the value of dtcmaxburstsize.</p> <p>Default: 0</p>

Parameter (cont.)	Description (cont.)
DTCPRemarking	Specifies the QoS action to take on the default traffic class before bandwidth metering is applied. Default: none
	USEMarkvalue Settings for the flow are selected from the DSCP MAP table using markvalue and a bandwidth class of 1.
	USEDscp Settings for the flow are selected from the DSCP MAP table using the DSCP value in the matching data frames and a bandwidth class value of 1.
	NONE The flow is passed to the metering stage.
DTCREmarking	Specifies the action to take after the metering stage. The metering stage assigns a temporary value of bandwidth class to the flow that is used to determine its per-hop behaviour. Default: none
	USEDSCPMap The temporary value is used (in conjunction with the DSCP of the frame) as an index into DSCP MAP, which then assigns the actual, new values for bandwidth class, DSCP, egress queue, and VLAN Tag User Priority.
	BWClass The temporary bandwidth class becomes the new bandwidth class for the flow.
	NONE No action.
DTCSTORMStatus	Whether storm protection is enabled for the default traffic class. Default: disabled
DTCSTORMWindow	Time between the polling of traffic class counters that checks whether storm protection should be activated. Required when storm protection is enabled. Default: none
	<i>windowsize</i> Number of milliseconds from 100 to 60 000.
	NONE Storm protection is inactive.
DTCSTORMRate	Storm protection is activated when this rate of traffic is exceeded. Required when storm protection is enabled. If the value of dtcstormwindow is less than one second, the rate is averaged over the last second. Default: none
	Rate Bits per second from 1Kbps to 10Gbps, specified in Kbps, Mbps or Gbps. If you do not specify a unit, it uses Kbps. If you specify Mbps or Gbps, the rate may contain a decimal fraction with up to 3 decimal places, for example, 1.25 Mbps.
	NONE Storm protection is inactive.
DTCSTORMAction	Action QoS takes when a storm is detected on a port. Default: portdisable
	LINKDown Operationally disables ports where a storm is detected.
	PORTdisable Administratively disables ports to which the policy is attached.

Parameter (cont.)	Description (cont.)
DTCSTORMTimeout	Length of time the port remains disabled after a storm is detected. Default: none
	<i>timeoutlength</i> Duration in seconds from 1 to 86 400.
	NONE The port remains disabled until you enable it again with the enable switch port command on page 7-94 of Chapter 7, Switching.
MArkvalue	Specifies an explicit value to use as an index into the DSCP MAP table when the dtcpremarking parameter is usemarkvalue . Default: none
	<i>dscp-value</i> An integer from 0 to 63.
	NONE No special index.
Port	Port where unclassified traffic is sent when dtcaction is sendvlanport . The port must belong to the VLAN specified by the vlan parameter.
VLAN	VLAN where unclassified traffic is sent when dtcaction is sendvlanport . Traffic is sent over the port specified by the port parameter so the VLAN must contain that port. <i>Vlan-id</i> is an integer from 1 to 4094.

Examples To set the description of policy 1 to *all ports*, use the command:

```
set qos poli=1 desc="all ports"
```

The following command enables storm protection for traffic processed by the default traffic class in the following manner:

- sets QoS Policy 1 with a description of *stormprotection*
- enables storm protection on the policy
- checks traffic every 200 milliseconds
- if the rate has exceeded 50kbps, activates storm protection
- when activated, storm protection operationally disables the port for 60 seconds

```
set qos poli=1 desc=stormprotection dtcstorms=ena
dtcstormw=200 dtcstormr=50kbps dtcstorma=linkd
dtcstormt=60
```

Related Commands

- [add qos policy](#)
- [create qos policy](#)
- [delete qos policy](#)
- [destroy qos policy](#)
- [set qos port](#)
- [show qos policy](#)

set qos port

Syntax SET QOS Port={*port-list*|ALL} [POLIcy={*id*|NONE}]
 [DEFAultqueue=*queue-number*] [FORCedefqueue={YES|NO}]
 [RED={*red-id*|NONE}]

Description This command configures a port so that it applies a QoS policy to all packets ingressing it.

For AT-9900 switches, you can attach a QoS policy to a port trunk group only when all members of the trunk belong to the same switch instance. A *switch instance* refers to a single switch chip. The switch contains two switch instances, which consist of ports 1-12 and ports 13-24.

For x900-24X switches, you can attach a QoS policy to a port trunk group only when all members of the trunk belong to the same switch instance. A *switch instance* refers to a single switch chip. The switch contains the following switch instances: ports 1-12, ports 13-24, and all ports that belong to a single expansion module.

Parameter	Description
Port	Port to configure. Default: no default
	<i>port-list</i> Specific port that consists of: one or more ports a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges
	ALL All ports.
POLIcy	QoS policy to assign to the port. Default: no default
	<i>id</i> An integer from 0 to 255 for a specific policy.
	NONE No policy is assigned.
DEFAultqueue	The <i>queue-number</i> is an integer from 0 to 7 that specifies the default queue to use for untagged frames that have no User Priority value. If the default queue is not reassigned by premarking and/or re-marking, this is the egress queue number. The initial queue values for tagged frames are assigned by the prio2queuemap settings. Default: 2
FORCedefqueue	Whether frames that the port receives are forced to the default queue. Default: no
	YES Frames go to the default queue regardless of whether they are tagged or untagged.
	NO Frames go to regular egress queues.

Parameter (cont.)	Description (cont.)
RED	Congestion avoidance algorithm to use for the switch port before frames are queued for egress.
<i>red-id</i>	An integer from 1 to 4 for a specific RED curve set.
NONE	The port uses a bandwidth class selective tail-drop mechanism according to the values of stop1 , stop2 and stop3 for each queue in the default RED curve set (RED=1). For the tail-drop mechanism, if a queue has a length greater than stop3 then no frames with bandwidth class 3 are added to the queue; they are dropped. If a valid RED curve set is selected, the port employs the 3-level RED drop-selection algorithm using the specified RED curve settings.

Examples To set switch port number 1 to use the QoS policy 1, use the command:

```
set qos port=1 poli=1
```

To set the default queue on switch port number 1 to queue 0 and force this value for all frames, use the command:

```
set qos port=1 defa=0 forc=yes
```

To set switch port number 1 to use RED curve set number 3, use the command:

```
set qos port=1 red=3
```

Related Commands

- [add qos policy](#)
- [set qos portgroup](#)
- [show qos policy](#)
- [show qos port](#)

set qos port egressqueue

Syntax SET QOS Port={*port-list*|ALL} EGressqueue[=*queue-list*]
 [Length=16..3648] [MAXbandwidth={0..16000000|NONE}]
 [SCHeduler={STRICT|WRR1|WRR2}] [WRRweight=6..255]

where:

- *port-list* is a single port or group of ports; a range of integers (specified as 0-4) or a comma-separated list of policy numbers and/or ranges (0, 3, 4-9).
- *queue-list* is either an integer from 0 to 7; a range of integers (specified as 0-3) or a comma-separated list of integers and/or ranges, without spaces.

Description This command sets egress queue parameters for one or more ports. The **port** parameter specifies one port, and **all** specifies all ports. The default is **all**.

The **egressqueue** parameter specifies which egress queues on the ports to change. If no value is specified, all queues on the specified ports are updated.

The **length** parameter specifies the length to set for the specified egress queue, measured in frames. Values are rounded up to the nearest 16 frames and limited to the maximum queue length for the port type (see table below).

The **maxbandwidth** parameter specifies the maximum bandwidth permitted. This value may be specified in kbps, Mbps, or Gbps (in uppercase or lowercase). If no unit is specified, the value is read as kbps. If Mbps or Gbps is specified, the value may contain a decimal fraction, for example, 1.25Mbps.

The **maxbandwidth** parameter determines the rate at which data leaves the internal queues in the switch to be transmitted onto the line. This rate is not equivalent to the transmission rate for data seen on the line. For example, 10Mbps of data leaving the internal queues is not equivalent to 10 Mbps of data transmitted on the line. This is because the actual transmission rate includes the transmission of bits for the inter-frame-gap and the preamble of the Ethernet packet. Bandwidth is allocated to queues in increments of approximately 650kbps and the value is rounded up.

When the **maxbandwidth** parameter is set to a value other than **none**, you must ensure the size of the queue length for all egress queues on that port is less than the maximum egress queue length. Failure to do so affects other queues because the egress port buffer fills with packets waiting to be requeued. The default maximum bandwidth is **none**. The following table shows the recommended values.

Port Type	Default Queue Length	Max Queue Length	And when Max Bandwidth is Specified
10/100Mbytes	128 frames	128 frames	16 frames
1 Gigabit	128 frames	896 frames	112 frames
10Gigabit	128 frames	3648 frames	256 frames

The **scheduler** parameter specifies the method by which frames on each egress queue is allocated bandwidth for transmission onto the line. For details about scheduling, see [“Scheduling Queues” on page 27-31](#). The following options are possible:

- **strict** to schedule based on queue number. Queues with higher numbers are served first—before lower numbered queues in the strict priority group and WRR, if there is a mix of the two types.

- **wrr1** to schedule weighted round robin. The queue shares bandwidth with other queues in the WRR1 group according to their relative values of **wwrweight**. The WRR1 group can transmit frames when the strict scheduling group is empty.
- **wrr2** to schedule weighted round robin. The queue shares bandwidth with other queues in the WRR2 group according to their relative values of **wwrweight**. The WRR2 group can transmit frames when both the strict and WRR1 scheduling groups are empty. The initial value is **strict**.

The **wwrweight** parameter specifies the weight to use for the queue when it is configured to use one of the WRR groups. The value of **wwrweight** specifies the number of bytes transmitted from a WRR queue in proportion to the values for other queues in the same WRR group (WRR1 or WRR2). For example, a queue with **wwrweight=24** would transmit four times as much traffic as a queue in the same group with **wwrweight=6**. The initial value is 6 for all queues.

Examples To configure all queues on port 1 with a maximum bandwidth of 1.25Mbps using equal-weighted scheduling on WRR group 1, use the command:

```
set qos port=1 egr max=1.25mb sch=wrr1 wrr=10
```

Related Commands [set qos fabric queue](#)
[show qos port](#)

set qos portgroup

Syntax SET QOS PORTGroup=*group-list* [POLIcy={*policy-list*|NONE}]
[DESCRiption=*description*]

Description This command attaches a policy to a port group, or removes the current policy.

Parameter	Description
PORTgroup	Port group affected. The <i>group-list</i> consists of: <ul style="list-style-type: none">one or more port groupsa range specified with a hyphen, such as 1-4a comma-separated list of numbers and/or rangesan integer from 1 to 32 Default: no default
POLIcy	Policy to attach or remove for this port group. Default: no default
	<i>policy-list</i> Integer from 0 to 255 for a specific policy.
	NONE Removes policy currently assigned to the port group.
DESCRiption	Description of the port group. Default: no default

Examples To assign policy 2 to port group 1, and name the port group “uplink”, use the command:

```
set qos portg=1 poli=2 desc=uplink
```

Related Commands

- [add qos portgroup port](#)
- [create qos portgroup](#)
- [delete qos portgroup port](#)
- [destroy qos portgroup](#)
- [show qos portgroup](#)

set qos prio2queuemap

Syntax SET QOS PRIO2queuemap=*p0,p1,p2,p3,p4,p5,p6,p7*

Description This command sets the mapping of incoming VLAN Tag User Priorities to the internal service queues for incoming packets that include a VLAN tag header.

The **prio2queuemap** parameter specifies a comma-separated list of eight values, all of which must be present. The first value, *p0*, represents the queue priority corresponding to an incoming VLAN tag User Priority of 0. Similarly, values *p1* to *p7* represent the queue priority corresponding to an incoming VLAN tag User Priority of 1 to 7. The defaults are 2, 0, 1, 3, 4, 5, 6, and 7 as recommended in IEEE Standard 802.1q (1998) section 8.7.3.

Examples To map incoming VLAN tag User Priorities 0 to 7 to queue priorities 0, 0, 3, 3, 4, 5, 6, and 7 respectively, use the command:

```
set qos prio2=0,0,3,3,4,5,6,7
```

Related Commands [show qos prio2queuemap](#)

set qos red

Syntax SET QOS RED=*red-id* [AVERaging=*averaging-factor*]
 [DESCription=*description*] [QUEue=*queue-list*]
 [START1=*start*] [STOP1=*stop*] [DROP1=*probability*]
 [START2=*start*] [STOP2=*stop*] [DROP2=*probability*]
 [START3=*start*] [STOP3=*stop*] [DROP3=*probability*]

where:

- *averaging-factor* is an integer from 0 to 15.
- *description* is a string 1 to 15 characters long. Valid characters are any printable characters. If the value contains spaces, it must be in double quotes.
- *red-id* is an integer from 1 to 4.
- *probability* is an integer from 0 to 15.
- *queue-list* is either an integer from 0 to 7; a range of integers (specified as 0-3), or a comma-separated list of integers and/or ranges without spaces.
- *start* is an integer from 0 to 16 000 000 followed by an optional unit of bytes, kbytes, Mbytes, or Gbytes (in uppercase or lowercase).
- *stop* is an integer from 0 to 16 000 000 followed by an optional unit of bytes, kbytes, Mbytes, or Gbytes (in uppercase or lowercase).

Description This command sets the properties of the specified set of RED curves for a single egress queue. There are eight RED curves in a set, one for each queue. Each RED curve has three thresholds, one for each bandwidth class.

The **red** parameter specifies which RED curve set has its settings updated by the specified values. Values for **stop1**, **stop2**, and **stop3** for all egress queues on RED curve set 1 (the default set) also apply to the Tail-Drop congestion avoidance mechanism employed when **red** is set to **none** for a port.

The **averaging** parameter specifies the weight to use in the time-based averaging calculation of queue length for the RED curve algorithm. If 0 is specified, the average queue length follows the actual queue length exactly. A larger **averaging** value applies a longer time constant to the calculation, improving the performance of TCP sessions around the **stop** values by helping to avoid synchronous dropping of frames from all sessions on the queue. The default is 9.

The **description** parameter is a text label for the RED curve of up to 15 characters long. The specified label is applied to the entire set of RED curves, regardless of the value of the **queue** parameter

The **queue** parameter specifies which egress queues in the set have their settings updated by the specified values. If this parameter is not specified, all queues in the set are updated. There is no default.

The **start1** parameter specifies, for frames associated with bandwidth class 1, the queue length in bytes at which the RED probability leaves the baseline. As the queue length increases above the start level for bandwidth class 1, the random probability that a frame in that class will be dropped increases linearly until the queue length reaches the **stop1** value, at which point the drop-probability is equal to that specified by **drop1**. The default is 25 kilobytes.

The **stop1** parameter specifies, for frames associated with bandwidth class 1, the queue length in bytes at which the RED probability reaches the top of the linear portion of the curve. When the queue length is at the **stop1** value, the drop-probability for frames marked with that class is determined by the value of **drop1**. For a queue length exceeding the **stop1** value, the drop-probability is 100%. In the default RED curve set, the **stop1** parameter also determines the queue length at which Tail-Drop blocking occurs for frames associated with bandwidth class 1 when no RED curve is selected for a port. In Tail-Drop mode, no queue length averaging is performed. The default is 30 kilobytes.

The **drop1** parameter specifies the maximum drop-probability for frames associated with bandwidth class1 on a RED curve controlled queue at the length specified by **stop1**. The drop-probability is 100% for a **drop1** value of 0, and halves with each increment. For example, a **drop1** value of 4 gives a drop-probability of 1/16, or 6.25%. The default is 1.

The **start2** parameter specifies, for frames associated with bandwidth class 2, the queue length in bytes at which the RED probability leaves the baseline. As the queue length increases above the start level for bandwidth class 2, the random probability that a frame in that class will be dropped increases linearly until the queue length reaches the **stop2** value, at which point the drop-probability is equal to that specified by **drop2**. The default is 15 kilobytes.

The **stop2** parameter specifies, for frames associated with bandwidth class 2, the queue length in bytes, at which the RED probability reaches the top of the linear portion of the curve. When the queue length is at the **stop2** value, the drop-probability for frames marked with that class is determined by the value of **drop2**. For a queue length exceeding the **stop2** value, the drop-probability is 100%. In the default RED curve set, this parameter also determines the queue length at which Tail-Drop blocking occurs for frames associated with bandwidth class 2 when no RED curve is selected for a port. In Tail-Drop mode, no queue length averaging is performed. The default is 25 kilobytes.

The **drop2** parameter is used to specify the maximum drop-probability for frames associated with bandwidth class2 on a RED curve controlled queue at the length specified by **stop2**. The drop-probability is 100% for a **drop2** value of 0, and halves with each increment. For example, a **drop2** value of 4 gives a drop-probability of 1/16, or 6.25%. The default is 1.

The **start3** parameter specifies, for frames associated with bandwidth class 3, the queue length in bytes at which the RED probability leaves the baseline. As the queue length increases above the start level for bandwidth class 3, the random probability that a frame in that class will be dropped increases linearly until the queue length reaches the **stop3** value, at which point the drop-probability is equal to that specified by **drop3**. The default is 5 kilobytes.

The **stop3** parameter specifies, for frames associated with bandwidth class 3, the queue length in bytes at which the RED probability reaches the top of the linear portion of the curve. When the queue length is at the **stop3** value, the drop-probability for frames marked with that class is determined by the value of **drop3**. For a queue length exceeding the **stop3** value, the drop-probability is 100%. In the default RED curve set, this parameter also determines the queue length at which Tail-Drop blocking occurs for frames associated with bandwidth class 3, when no RED curve is selected for a port. In Tail-Drop mode, no queue length averaging is performed. The default is 15 kilobytes.

The **drop3** parameter is used to specify the maximum drop-probability for frames associated with bandwidth class3 on a RED curve controlled queue at the length specified by **stop3**. The drop-probability is 100% for a **drop3** value of 0, and halves with each increment. For example, a **drop3** value of 4 gives a drop-probability of 1/16, or 6.25%. The default is 1.

Examples To specify that RED curve set 2 uses the default settings, use the command:

```
set qos red aver=9 start1=25 stop1=30 drop1=1
start2=15 stop2=25 drop2=1 start3=5 stop3=15 drop3=0
```

Related Commands [create qos red](#)
[destroy qos red](#)
[show qos red](#)

set qos trafficclass

Syntax SET QOS TRAfficclass=*trafficclass-list*
 [DESCRiption=*description*]
 [ACTion={FORward|FORward,SEnDMirror|DIScard|SEnDMirror|SEnDMirror,SEnDVlanport|SEnDVlanport}]
 [DROPBwclass3={OFF|NO|False|ON|YES|True}]
 [IGNorebwclass3={OFF|NO|False|ON|YES|True}]
 [MARKvalue={*dscp-value*|NONE}]
 [MAXbandwidth={*bandwidth*|NONE}]
 [MAXBUrstsize=*burstsize*]
 [MINbandwidth={*bandwidth*|NONE}]
 [MINBUrstsize=*burstsize*] [PORT=*port*]
 [PREMarking={USEMarkvalue|USEDscp|NONE}]
 [REMarking={USEDSCPMap|BWClass|NONE}]
 [STORMStatus={ENable|DISable}]
 [STORMWindow={*windowsize*|NONE}]
 [STORMRate={Rate|NONE}]
 [STORMAction={LINKDown|Portdisable|VLANDisable}]
 [STORMTimeout={*timeoutlength*|NONE}]
 [VLAN=*vlan-id*]

Description This command changes parameters on one or more QoS traffic classes. You can also change storm protection parameters with this command. For more information about bandwidth metering, see [“Bandwidth conformance classes” on page 27-25](#).

Parameter	Description
TRAfficclass	<p>The <i>trafficclass-list</i> is the traffic class you want to change that consists of:</p> <ul style="list-style-type: none"> an integer from 0 to 1023 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges <p>Default: no default</p>
DESCRiption	<p>Text that describes the traffic class being changed and consists of:</p> <ul style="list-style-type: none"> a string 1 to 15 characters long any printable character <p>If <i>description</i> contains spaces, it must be in double quotes.</p> <p>Default: no default</p>

Parameter (cont.)	Description (cont.)
ACtion	Action to be performed on traffic belonging to this traffic class. Default: forward
	FORward Forwarded normally.
	DIScard Dropped.
	SENDVlanport Sends traffic to the VLAN specified by the vlan parameter and the port specified by the port parameter. Both vlan and port must also be specified. The VLAN must exist and the specified port must be a member of that VLAN. The switch determines whether the port is tagged or untagged for that VLAN, and sends traffic with the correct tag if the port is tagged. If the port is untagged for the specified VLAN, the frame is sent untagged.
	SENDMirror Sends traffic to the preconfigured mirror port. This option lets you mirror packets classified on any port. It is more flexible than standard mirroring, which only monitors traffic on a single port. You can also forward mirrored traffic normally, discard it, or send it to a particular port and VLAN.
DROPBwclass3	Whether to drop frames exceeding the traffic class maxbandwidth setting. Default: no
	YES Data is dropped immediately if the rate is higher than the combined maxbandwidth and maxburstsize settings.
	NO Marks non-conforming traffic as bandwidth class 3 and allows this traffic to be selected for dropping by the RED curve settings, which have a more TCP-friendly algorithm.
IGNorebwclass	Whether the metering stage acknowledges any previous bandwidth class assigned to flows processed by the default traffic class. Default: no
	YES If bandwidth processing (minbandwidth , maxbandwidth) is active on this traffic class, the metering function ignores any bandwidth class previously assigned to the flow in the premarking stage and sets the meter bandwidth class according to the meter conformance level of the flow.
	NO The meter bandwidth class is temporary unless the bwclass or usedscpmap option is entered for the remarking parameter.
MArkvalue	Specifies an explicit value to use as an index into the DSCP MAP table when the premarking parameter is usemarkvalue . Default: none
	<i>dscp-value</i> An integer from 0 to 63.
	NONE No special index.

Parameter (cont.)	Description (cont.)
MAXBAndwidth	<p>Maximum bandwidth available to the traffic class. Maximum data rate for bandwidth class 2. If the traffic class is on a policy that is attached to a switch port, the resultant bandwidth must be valid for that port.</p> <p>Default: none</p> <hr/> <p><i>bandwidth</i> Value from 0 to 16 000 000 kbps. This value may be specified in kbps, Mbps or Gbps (in uppercase or lowercase). If no unit is specified, it is read as kbps. If Mbps or Gbps is specified, the value may contain a decimal fraction, for example, 1.25Mbps.</p> <hr/> <p>NONE No maximum.</p>
MAXBUrsize	<p>Specifies the burst tolerance for the maxbandwidth parameter. The maxburstsize parameter determines the maximum amount of data permitted above maxbandwidth for the traffic class before re-marking to bandwidth class 3 occurs, or frames are dropped depending on the setting of the dropbwclass3 parameter.</p> <p><i>Burstsize</i> is a value from 0 to 16 777 216 bytes. This value may be specified in bytes, kbytes, or Mbytes (in uppercase or lowercase). If no unit is specified, it is read as bytes. If Mbytes is specified, the value may contain a decimal fraction, for example, 1.25 Mbytes. This parameter should always be as large as the largest size packet to be metered on the aggregate flow.</p> <p>Default: 0</p>
MINBAndwidth	<p>Specifies the minimum bandwidth reserved for the traffic class. This parameter determines the maximum rate of data in bandwidth class 1.</p> <p>Default: none</p> <hr/> <p><i>bandwidth</i> Value from 0 to 16 000 000 kbps. This value may be specified in kbps, Mbps or Gbps (in uppercase or lowercase). If no unit is specified, it is read as kbps. If Mbps or Gbps is specified, the value may contain a decimal fraction, for example, 1.25Mbps.</p> <hr/> <p>NONE No minimum.</p>
MINBUrsize	<p>Specifies the burst tolerance for minbandwidth, or for maxbandwidth when minbandwidth is none. This parameter determines the maximum amount of data permitted above minbandwidth for the traffic class before re-marking to bandwidth class 2 occurs.</p> <p><i>Burstsize</i> is a value from 0 to 16 777 216 bytes. This value may be specified in bytes, kbytes, or Mbytes (in uppercase or lowercase). If no unit is specified, it is read as bytes. If Mbytes is specified, the value may contain a decimal fraction, for example, 1.25 Mbytes. If this parameter is not specified for class 2, its value must be less than the value of maxburstsize.</p> <p>Default: 0</p>
Port	<p>Port where unclassified traffic is sent when action is sendvlanport. The port must belong to the VLAN specified by the vlan parameter.</p>

Parameter (cont.)	Description (cont.)
PRemarking	Specifies the QoS action to take on the traffic class before bandwidth metering is applied. Default: none
	USEMarkvalue Settings for the flow are selected from the DSCP MAP table using markvalue and a bandwidth class of 1.
	USEDscp Settings for the flow are selected from the DSCP MAP table using the DSCP value in the matching data frames and a bandwidth class value of 1.
	NONE The flow is passed to the metering stage.
REmarking	Specifies the action to take after the metering stage. The metering stage assigns a temporary value of bandwidth class to the flow that is used to determine its per-hop behaviour. Default: none
	USEDSCPMap The temporary value is used (in conjunction with the DSCP of the frame) as an index into DSCP MAP, which then assigns the actual, new values for bandwidth class, DSCP, egress queue, and VLAN Tag User Priority.
	BWClass The temporary bandwidth class becomes the new bandwidth class for the flow.
	NONE No action.
STORMStatus	Whether storm protection is enabled for the default traffic class. Default: disabled
STORMWindow	Time between the polling of traffic class counters that checks whether storm protection should be activated. Required when storm protection is enabled. Default: none
	<i>windowsize</i> Number of milliseconds from 100 to 60 000.
	NONE Storm protection is inactive.
STORMRate	Storm protection is activated when this rate of traffic is exceeded. Required when storm protection is enabled. If the value of stormwindow is less than one second, the rate is averaged over the last second. Default: none
	Rate Bits per second from 1Kbps to 10Gbps, specified in Kbps, Mbps or Gbps. If you do not specify a unit, it uses Kbps. If you specify Mbps or Gbps, the rate may contain a decimal fraction with up to 3 decimal places, for example, 1.25 Mbps.
	NONE Storm protection is inactive.

Parameter (cont.)	Description (cont.)
STORMAction	Action QoS takes when a storm is detected on a port. Default: portdisable
	LINKDown Operationally disables ports with storms to which the traffic class is attached.
	PORTdisable Administratively disables ports with storms to which the traffic class is attached.
	VLANdisable Administratively disables ports with storms to which the traffic class is attached for the VLAN on which the classifier is matching.
STORMTimeout	Length of time the port remains disabled after a storm is detected. Default: none
	<i>timeoutlength</i> Duration in seconds from 1 to 86400.
	NONE The port remains disabled until you enable it again with the enable switch port command on page 7-94 or the enable switch port vlan command on page 7-95 of Chapter 7, Switching.
VLAN	VLAN where unclassified traffic is sent when action is sendvlanport . Traffic is sent over the port specified by the port parameter so the VLAN must contain that port. <i>Vlan-id</i> is an integer from 1 to 4094.

Examples The following command sets QoS traffic class 10 to:

- premark all member flows not previously marked by their flow group according to the DSCPMAP values indicated by the DSCP value of the incoming frames
- a bandwidth class 1 bandwidth reserve of 1Mbps with 64kbytes burst tolerance
- a maximum bandwidth class 2 limit of 2Mbps with 64kbyte burst tolerance
- drop frames in bandwidth class 3
- preserve premetering bandwidth class allocation, and a meter-based re-marking based on DSCPMAP settings
- send this traffic to the mirror port

```
set qos tr=10 prem=used min=1mb minbu=64kb max=2mb maxbu=64kb
dropb=yes ign=no rem=usedscpm action=sendmirror
```

The following command enables storm protection as follows:

- sets QoS traffic class 1 with a description of *stormprotection*
- enables storm protection on the traffic class
- checks traffic every 200 milliseconds
- if the rate has exceeded 50kbps, activates storm protection
- when activated, storm protection operationally disables the port for 60 seconds

```
cre qos tr=1 desc=stormprotection storms=ena stormw=200
stormr=50kbps storma=linkd stormt=60
```

Related Commands

- [add qos trafficclass](#)
- [create qos trafficclass](#)
- [destroy qos trafficclass](#)
- [show qos trafficclass](#)

show qos accelerator counters

Syntax SHOW QOS ACCElerator COUNTERs
 TRafficclass[={*trafficclass-list*|DEFAULT|ALL}]

SHOW QOS ACCElerator COUNTERs EGressqueue[=*queue-list*]

where:

- *queue-list* is either an integer from 0 to 7; a range of integers (specified as 0-3) or a comma-separated list of integers and/or ranges, without spaces
- *trafficclass-id* is an integer from 0 to 1023; a range of integers (specified as 0-3) or a comma-separated list of integers and/or ranges without spaces

Description This command applies to AT-8948 and AT-9924T/4SP switches and displays QoS configuration information for accelerator card counters.

If **trafficclass** is specified, counters for the traffic classes belonging to the policy attached to the accelerator card are displayed. If no value or **all** is specified, then information about all traffic classes is displayed. If **default** is specified, then only information about the default traffic class is displayed. If a list of traffic classes is specified, then information about those classes is displayed.

If **egressqueue** is specified, counters for the specified queues are displayed. If no value is specified, then information about all egress queues is displayed. If a list of queues are specified, then only information about those queues is displayed.

Figure 27-8: Example output from the **show qos accelerator counters egressqueue** command

```

Accel Card Egress Queue Counters:
Total queue length ..... 0 (maximum 896)
Egress queue length:
Queue 0 ..... 0 (maximum 896)
Queue 1 ..... 0 (maximum 896)
Queue 2 ..... 0 (maximum 896)
Queue 3 ..... 0 (maximum 896)
Queue 4 ..... 0 (maximum 896)
Queue 5 ..... 0 (maximum 896)
Queue 6 ..... 0 (maximum 896)
Queue 7 ..... 0 (maximum 896)
  
```

Table 27-3: Parameters in output of the **show qos accelerator counters egressqueue** command

Parameter	Meaning
Total queue length	Total number of packets queue for transmission on the accelerator card.
Queue n	Number of packets currently queued for transmission in the given queue.

Figure 27-9: Example output from the **show qos accelerator counters trafficclass** command

```
QOS Counter Information
Accelerator Interface:
  Policy: 1
  There are no traffic classes to display.
Default Traffic Class:
  Aggregate Bytes ..... 0
  BwConformanceClass1 bytes .... 0
  BwConformanceClass2 bytes .... 0
  BwConformanceClass3 bytes .... 0
  Dropped bytes ..... 0
```

Table 27-4: Parameters in output of the **show qos accelerator counters trafficclass** command

Parameter	Meaning
Policy	Number of the policy attached to the port.
Traffic class	Number of the traffic class belonging to the policy.
Aggregate Bytes	Number of bytes classified by this traffic class.
BwConformanceClass1 bytes	Number of bytes conforming to bandwidth class 1.
BwConformanceClass2 bytes	Number of bytes conforming to bandwidth class 2.
BwConformanceClass3 bytes	Number of bytes conforming to bandwidth class 3.
Dropped bytes	Number of bytes dropped by this traffic class.

Related Commands [reset qos accelerator counters](#)

show qos defaultpriority

Syntax SHow QOS DEFAUltpriority

Description This command displays the default queue to VLAN tag User Priority mapping scheme ([Figure 27-10](#), [Table 27-5](#)).

Figure 27-10: Example output from the **show qos defaultpriority** command

```
QoS Queue to Vlan Tag User Priority Mapping
-----
Queue UserPriority
-----
0 1
1 2
2 0
3 3
4 4
5 5
6 6
7 7
```

Table 27-5: Parameters in output of the **show qos defaultpriority** command

Parameter	Meaning
Queue	Number of the egress queue.
User Priority	User Priority field in the tagged frame transmitted on the egress port.

Examples To displays the default queue to VLAN tag User Priority mapping scheme, use the command:

```
sh qos defau
```

Related Commands [set qos defaultpriority](#)

show qos dscpmap

Syntax SHow QOS [DSCPMap={PREmarking|REMarking}] [DSCP=*dscp-list*]

Description This command displays the DSCP-based re-marking parameters (Figure 27-11, Table 27-6 on page 27-102).

Parameter	Description
DSCPMap	The DSCP-based marking table to display. Default: information from both tables
PREmarking	Displays information related to the flow group and traffic class premarking table.
REMarking	Displays information for the post-metering re-marking tables.
DSCP	List of DSCP values for which information should be displayed. The <i>dscp-list</i> consists of: an integer from 0 to 63 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges If a list of DSCP values is specified with the dscpmap parameter, the marking table entries that match the given values are displayed. If the dscp parameter is not present, the entire DSCP-based marking table is displayed for all values of DSCP. Default: no default

Figure 27-11: Example output from the **show qos dscpmap** command

DSCP-based QOS Marking Parameters

DSCP/Markvalue 0:

BandwidthClass	1	2	3
NewDSCP	0	0	0
NewBandwidthClass	1	2	3
NewQueue	0	0	0
NewPriority	0	0	0

DSCP/Markvalue 1:

BandwidthClass	1	2	3
NewDSCP	1	1	1
NewBandwidthClass	1	2	3
NewQueue	0	0	0
NewPriority	0	0	0

•
•
•

DSCP/Markvalue 63:

BandwidthClass	1	2	3
NewDSCP	63	63	63
NewBandwidthClass	1	2	3
NewQueue	0	0	0
NewPriority	0	0	0

Table 27-6: Parameters in output of the **show qos dscpmap** command

Parameter	Meaning
NewDSCP	DSCP value to write into each frame selected by its previous DSCP and bandwidth class indexes.
NewBandwidthClass	New bandwidth class to associate with each frame selected by its previous DSCP and bandwidth class indexes.
NewQueue	New internal queue to associate with each frame selected by its previous DSCP and bandwidth class indexes.
NewPriority	New VLAN Tag User Priority to use for each frame selected by its previous DSCP and bandwidth class indexes.

Examples To displays the DSCP-based QoS re-marking parameters, use the command:

```
sh qos dscpm=rem
```

Related Commands [set qos dscpmap](#)

show qos fabric

Syntax SHow QOS FABric

Description This command displays information about the switch fabric on the x900-24X switch ([Figure 27-12](#), [Table 27-7](#)).

Figure 27-12: Example output from the **show qos fabric** command

```

QOS settings on the Fabric
=====

Egress Queue to Fabric Queue mapping
-----

      Egress Queue      Fabric Queue
      -----
      0                  0
      1                  0
      2                  1
      3                  1
      4                  2
      5                  2
      6                  3
      7                  3

Individual Fabric Queue Settings
-----

Fabric Queue 0:
  Scheduler ..... Weighted Round Robin
  WRR Weight ..... 1
  Egress Queue ..... 0,1

Fabric Queue 1:
  Scheduler ..... Weighted Round Robin
  WRR Weight ..... 3
  Egress Queue ..... 2,3

Fabric Queue 2:
  Scheduler ..... Strict Priority
  WRR Weight ..... N/A
  Egress Queue ..... 4,5

Fabric Queue 3:
  Scheduler ..... Strict Priority
  WRR Weight ..... N/A
  Egress Queue ..... 6,7

```

Table 27-7: Parameters in output of the **show qos fabric** command

Parameter	Meaning
Egress Queue	The eight egress queues on each switch port.
Fabric Queue	The four queues on the switching fabric that links all switch ports. QoS is applied on the fabric.
Scheduler	Which scheduling method the fabric queue uses.
WRR Weight	Weight the fabric queue uses with the weighted round robin scheduling method.

Examples To display information about the current QoS settings for the switch fabric, use the command:

```
sh qos fab
```

Related Commands [set qos fabric queue](#)
[set qos fabric queuemap](#)

show qos flowgroup

Syntax SHow QOS FLOWgroup [= { *id* | ALL }]

Description This command displays configuration information for one or more QoS flow groups (Table 27-8).

If no value is specified for the **flowgroup** parameter, summary information about all flow groups is displayed (Figure 27-13).

If a value is specified, details about either the specific flow group or all flow groups is displayed (Figure 27-14). The *id* can be an integer from 0 to 1023.

Figure 27-13: Example output from the **show qos flowgroup** command

Flow Group Information			
Id	Description	Assigned TC	Classifiers
1	Bobs Video	2	1
2	all FTP	None	3, 6-9
9	Janes Video	5	8

Figure 27-14: Example output from the **show qos flowgroup=9** command

Identifier	9
Description	Janes Video
TC Assigned to	5
Classifiers	8
Premarking	USEMARKVALUE
Mark Value	0
Action	SENDVLANPORT
VLAN	2
Port	4

Table 27-8: Parameters in output of the **show qos flowgroup** command

Parameter	Meaning
Identifier	Numerical identifier of the flow group.
Description	Description of the traffic group.
TC Assigned to	Numerical identifiers of the traffic class to which the flow group is assigned.
Classifiers	Numerical identifiers of the Classifiers assigned to this flow group.
Premarking	Specifies the QoS action to take on the flow group.

Table 27-8: Parameters in output of the **show qos flowgroup** command (cont.)

Parameter	Meaning
Mark Value	Specifies a replacement value to write into the Differentiated Services value for all packets.
Action	Action taken on traffic belonging to the flow group; either none (the traffic class settings are used instead), forward (traffic is forwarded normally), discard (traffic is dropped), sendvlanport (traffic is sent to a port in a VLAN) or sendmirror (traffic is sent to the mirror port).
VLAN	VLAN where traffic is sent when action is sendvlanport .
Port	Port where traffic is sent when action is sendvlanport .

Examples To display summary information for all flow groups, use the command:

```
sh qos flowgroup
```

To display detailed configuration information for flow group 12, use the command:

```
sh qos fl=12
```

Related Commands

- [add qos flowgroup](#)
- [create qos flowgroup](#)
- [delete qos flowgroup](#)
- [destroy qos flowgroup](#)
- [set qos flowgroup](#)

show qos policy

Syntax `SHoW QoS POLIcY [= {id|ALL}]`

Description This command displays configuration information for one or more QoS policies.

If no value is given for the **policy** parameter, summary information about all policies is displayed (Figure 27-15, Table 27-9).

If a value is given, details about either the specific policy or all policies are displayed (Figure 27-16 on page 27-107, Table 27-10 on page 27-107). The *id* can be an integer from 0 to 255.

Figure 27-15: Example output from the **show qos policy** command

QoS Policy Information			
Id	Description	Trafficclasses	Ports Assigned to
1	all ports	3,5-7	port: 1-24
12	special	1,4	NONE
15	IPv6	8	Accelerator

Table 27-9: Parameters in output of the **show qos policy** command

Parameter	Meaning
Id	Numerical identifier of the policy.
Description	Description of the policy.
Trafficclasses	Numerical identifiers of the traffic classes assigned to this policy.
Ports Assigned to	Ports to which the policy is assigned, or none. "Accelerator" indicates that the policy is assigned to the IPv6 accelerator card for AT-8948 switches.

Figure 27-16: Example output from the **show qos policy=1** command

```

Identifier ..... 1
Description ..... all ports
TCs Assigned ..... 5,7,22,31-33
Port(s) Assigned to ..... 1-24
Port Group(s) Assigned to ... 1(1-12)
                             2(13-24)
Trunk(s) Assigned to ..... None
Default Traffic Class:
  Minimum Bandwidth ..... None
  Minimum Burst Size ..... 0 B
  Maximum Bandwidth ..... 10 Mbps
  Maximum Burst Size ..... 64 kbyte
  Drop BandwidthClass3 ..... YES
  Ignore BandwidthClass ..... YES
  Premarking ..... USEMARKVALUE
  Remarking ..... UESDSCPMAP
  Mark value ..... 0
  Action ..... SENDVLANPORT
    VLAN ..... 2
    PORT ..... 4
Storm Protection:
  Status ..... ENABLED
  Action ..... PORTDISABLE
  Rate ..... 1kbps
  Window ..... 100ms
  Timeout ..... None

```

Table 27-10: Parameters in output of the **show qos policy** command

Parameter	Meaning
Identifier	Numerical identifier of the policy.
Description	Description of the policy.
TCs Assigned	Numerical identifiers of the traffic classes assigned to this policy.
Port(s) Assigned to	Ports to which this policy is assigned, if any. "Accelerator" indicates that the policy is assigned to the IPv6 accelerator card for AT-8948 switches.
Port Group(s) Assigned to	ID of the port group that is assigned to the policy.
Trunk(s) Assigned to	Trunks to which the policy has been assigned.
Default Traffic Class: Settings that process unclassified traffic on the policy's port	
Minimum Bandwidth	Minimum bandwidth reserved for the traffic class.
Minimum Burst Size	The burst tolerance for minimum bandwidth.
Maximum Bandwidth	Maximum bandwidth available to the traffic class.
Maximum Burst Size	The burst tolerance for maximum bandwidth.
Drop BandwidthClass3	Whether frames exceeding the traffic class maximum bandwidth setting should be dropped.
Ignore BandwidthClass	Whether the metering stage acknowledges any previous bandwidth class assigned to flows processed by this traffic class.
Premarking	Action to take on the traffic class before any bandwidth metering is applied.
Remarking	Action to take after the metering stage.
Mark Value	The explicit value to use as an index into the DSCPMAP table.

Table 27-10: Parameters in output of the **show qos policy** command (cont.)

Parameter	Meaning
Action	Action taken on traffic processed by the DTC. For more information, see “Configuration Examples” on page 27-40.
VLAN	VLAN where unclassified traffic is sent when action is sendvlanport .
Port	Port where unclassified traffic is sent when action is sendvlanport .
Storm Protection settings	
Status	Whether storm protection is enabled for the default traffic class.
Action	Whether the port is administratively or operationally disabled when the volume of traffic exceeds the rate .
Rate	Allowable traffic volume before action is executed.
Window	Interval in milliseconds between checking the traffic class for storms.
Timeout	Length of time in seconds that the port remains disabled after having been disabled by storm protection.

Examples To display summary information about all QoS policies, use the command:

```
show qos poli
```

To display detailed information about QoS policy 112, use the command:

```
show qos poli=112
```

Related Commands

- [add qos policy](#)
- [create qos policy](#)
- [delete qos policy](#)
- [destroy qos policy](#)
- [set qos policy](#)
- [set qos port](#)

show qos port

Syntax `SHoW QoS PORT [= {port-list | ALL}] [EGResSqueue=queue-list]`

Description This command displays QoS configuration information for one or more ports, including information about egress queues ([Figure 27-17 on page 27-110](#), [Figure 27-18 on page 27-111](#), [Table 27-11 on page 27-111](#)).

Parameter	Meaning
PORT	Port for which to display information. Default: all
<i>port-list</i>	A specific port that consists of: <ul style="list-style-type: none">one or more portsa range specified with a hyphen, such as 1-4a comma-separated list of numbers and/or ranges
ALL	Displays information about all ports.
EGResSqueue	Number of the egress queue. The <i>queue-list</i> consists of: <ul style="list-style-type: none">an integer from 0 to 7a range specified with a hyphen, such as 1-4a comma-separated list of numbers and/or ranges Default: no default

Figure 27-17: Example output from the **show qos port=1** command

```
QOS Port Configuration

Port ..... 1
Port Group ..... 1
Trunk Group ..... None
Policy Assigned ..... 1(all ports)
Default Queue ..... 2
Force Default Queue ..... No
Red Curve ..... 2

Egress Queue Configuration:

Egress Queue 0:
  Queue Length ..... 128
  Maximum Bandwidth ..... None
  Scheduler ..... Strict
  WRR Weight ..... 6

Egress Queue 1:
  Queue Length ..... 128
  Maximum Bandwidth ..... None
  Scheduler ..... Strict
  WRR Weight ..... 6

Egress Queue 2:
  Queue Length ..... 128
  Maximum Bandwidth ..... None
  Scheduler ..... Strict
  WRR Weight ..... 6
.
.
.
Egress Queue 7:
  Queue Length ..... 128
  Maximum Bandwidth ..... None
  Scheduler ..... Strict
  WRR Weight ..... 6
```

Figure 27-18: Example output from the **show qos port=1 egressqueue=0,1** command

```

QOS Port Configuration

Port ..... 1
Policy Assigned ..... 1(all ports)
Default Queue ..... 2
Force Default Queue ..... No
Red Curve ..... 2

Egress Queue Configuration:

Egress Queue 0:
  Queue Length ..... 128
  Maximum Bandwidth ..... None
  Scheduler ..... Strict
  WRR Weight ..... 6

Egress Queue 1:
  Queue Length ..... 128
  Maximum Bandwidth ..... None
  Scheduler ..... Strict
  WRR Weight ..... 6

```

Table 27-11: Parameters in output of the **show qos port=1** command

Parameter	Meaning
Port	Number of the port.
Port Group	ID of the port group to which the port belongs.
Trunk Group	ID of the trunk group to which the port belongs.
Policy Assigned	Numerical identifier of the policies assigned to this port.
Default Queue	The default queue to use for untagged frames.
Force Default Queue	Whether to force all frames that the port receives to use the default queue.
Red Curve	The congestion avoidance algorithm to use before frames are queued for egress.
Egress Queue	The egress queue number on the nominated port.
Queue Length	The length set for the queue.
Maximum Bandwidth	Maximum bandwidth available to the traffic class.
Scheduler	Scheduler group for the queue.
WRR Weight	Weight to use for the queue.

Examples To display QoS information about all ports, use the command:

```
sh qos po
```

To display detailed information about QoS port 2, use the command:

```
sh qos po=2
```

Related Commands [set qos port](#)
[set qos port egressqueue](#)

show qos port counters

Syntax `SHoW QoS Port[={port-list|ALL}] COUnters`
 `EGressqueue[=queue-list]`

`SHoW QoS Port[={port-list|ALL}] COUnters`
 `TRafficclass[={trafficclass-id|DEFAult|ALL}]`

Description This command displays QoS configuration information for one or more ports.

Parameter	Meaning
Port	Specifies a port. Default: all
<i>port-list</i>	A specific port that consists of: one or more ports a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges
ALL	Displays information about all ports.
EGressqueue	Number of the egress queue (Figure 27-19 , Table 27-12 on page 27-113). The <i>queue-list</i> consists of: an integer from 0 to 7 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges Default: all
TRafficclass	Specifies traffic classes attached to the port (Figure 27-20 on page 27-113 , Table 27-13 on page 27-113). For this parameter to work, you must have already enabled QoS counters with the set switch enhancedmode command on page 7-103 of Chapter 7, Switching . Default: all
<i>trafficclass-id</i>	Displays details about a specific traffic class. The variable consists of: an integer from 0 to 1023 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges
DEFAult	Displays information about the default traffic class.
ALL	Displays information about all traffic classes.

Figure 27-19: Example output from the **show qos port counters egressqueue** command

```

Port 1 Egress Queue Counters:
Port queue length ..... 48 (maximum 128)
Egress queue length:
Queue 0 ..... 0 (maximum 16)
Queue 1 ..... 16 (maximum 16)
Queue 2 ..... 16 (maximum 16)
Queue 3 ..... 16 (maximum 16)
Queue 4 ..... 0 (maximum 16)
Queue 5 ..... 0 (maximum 16)
Queue 6 ..... 0 (maximum 16)
Queue 7 ..... 0 (maximum 16)

```


Table 27-12: Parameters in output of the **show qos port counters egressqueue** command

Parameter	Meaning
Port queue length	Total number of packets queue for transmission on port.
Queue n	Number of packets currently queued for transmission in the given queue.

Figure 27-20: Example output from the **show qos port counters trafficclass** command

```

QOS Counter Information
Port 1:
  Policy: 0
  Traffic Class 0:
    Aggregate Bytes .....
    BwConformanceClass1 bytes .... 15220
    BwConformanceClass2 bytes .... 0
    BwConformanceClass3 bytes .... 0
    Dropped bytes ..... 15220
  Default Traffic Class:
    Aggregate Bytes ..... 680
    BwConformanceClass1 bytes .... 680
    BwConformanceClass2 bytes .... 0
    BwConformanceClass3 bytes .... 0
    Dropped bytes ..... 0

```

Table 27-13: Parameters in output of the **show qos port counters trafficclass** command

Parameter	Meaning
Port	Number of the port.
Policy	Number of the policy attached to the port.
Traffic Class	Number of the traffic class belonging to the policy.
Aggregate Bytes	Number of bytes classified by this traffic class.
BwConformanceClass1 bytes	Number of bytes conforming to bandwidth class 1.
BwConformanceClass2 bytes	Number of bytes conforming to bandwidth class 1.
BwConformanceClass3 bytes	Number of bytes conforming to bandwidth class 1.
Dropped Bytes	Number of bytes dropped by this traffic class.

show qos portgroup

Syntax SHow QOS PORTGroup [= {*group-list* | ALL}]

Description This command displays information about port groups.

Parameter	Meaning
PORTgroup	Specifies a port group for which to display information. Default: all
<i>group-list</i>	Integer from 1 to 32 (Figure 27-22, Table 27-14).
ALL	All port groups.
no value	Displays summary information about all port groups (Figure 27-21, Table 27-14).

Figure 27-21: Example output from the **show qos portgroup** command

QOS Port Group Information			
ID	Description	Policy Assigned	Ports
1	Uplink	None	1-2,5
2		1	10-20

Figure 27-22: Example output from the **show qos portgroup=1** command

Identifier	1
Description	Uplink
Policy Assigned to	None
Ports	1-2,5

Table 27-14: Parameters in output of the **show qos portgroup** command

Parameter	Meaning
ID/Identifier	Port group ID.
Description	Description of the port group.
Policy Assigned/ Policy Assigned to	Policy attached to the port group.
Ports	Ports that belong to the port group.

Examples To display all configured port groups, use the command:

```
sh qos portg=all
```

Related Commands

- [add qos portgroup port](#)
- [set qos portgroup](#)
- [delete qos portgroup port](#)
- [show qos portgroup counters](#)

show qos portgroup counters

Syntax `SHoW QoS PORTGroup[={group-list|ALL}] COUnTers
TRaFFicclass[={trafficclass-list|DEFAult|ALL}]`

Description This command displays information about traffic class counters for port groups.

Parameter	Meaning
PORTgroup	Specifies a port group for which to display information. Default: all
	<i>group-list</i> Integer from 1 to 32.
	ALL All port groups.
	no value Displays summary information about all port groups.
TRaFFicclass	Traffic class attached to the port group (Figure 27-26 on page 27-119 , Table 27-17 on page 27-118). Default: all
	<i>trafficclass-list</i> A specific traffic class that consists of: one or more traffic classes a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges an integer from 0 to 1023
	DEFAult The default traffic class.
	ALL Displays counters for all traffic classes.

Figure 27-23: Example output from the **show qos portgroup counters trafficclass** command

```

QOS Counter Information
Port Group 1:
  Policy: 1

  Traffic Class 1:
    Aggregate Bytes ..... 2176
    BwConformanceClass1 bytes .... 2176
    BwConformanceClass2 bytes .... 0
    BwConformanceClass3 bytes .... 0
    Dropped bytes ..... 0
  Default Traffic Class:
    Aggregate Bytes ..... 0
    BwConformanceClass1 bytes .... 0
    BwConformanceClass2 bytes .... 0
    BwConformanceClass3 bytes .... 0
    Dropped bytes ..... 0

Port Group 2:
  Policy: 2

  Traffic Class 2:
    Aggregate Bytes ..... 0
    BwConformanceClass1 bytes .... 0
    BwConformanceClass2 bytes .... 0
    BwConformanceClass3 bytes .... 0
    Dropped bytes ..... 0
  Default Traffic Class:
    Aggregate Bytes ..... 0
    BwConformanceClass1 bytes .... 0
    BwConformanceClass2 bytes .... 0
    BwConformanceClass3 bytes .... 0
    Dropped bytes ..... 0

```

Table 27-15: Parameters in output of the **show qos portgroup counters trafficclass** command

Parameter	Meaning
Port Group	Port group ID.
Policy	Policy attached to the port group.
Traffic Class	Counters for this traffic class.
Aggregate Bytes	Total number of bytes this traffic class counted.
BwConformanceClass1 bytes	Number of bytes that conforms with band with class 1.
BwConformanceClass2 bytes	Number of bytes that conforms with band with class 2.
BwConformanceClass3 bytes	Number of bytes that conforms with band with class 3.
Dropped bytes	Number of bytes this traffic class discarded.

Examples To display all configured port groups, use the command:

```
sh qos portg=all
```

Related Commands

- [add qos portgroup port](#)
- [set qos portgroup](#)
- [delete qos portgroup port](#)
- [reset qos portgroup counters](#)
- [show qos portgroup](#)

show qos prio2queuemap

Syntax SHow QOS PRIO2queuemap

Description This command displays the default VLAN tag User Priority to queue to mapping scheme ([Figure 27-24](#), [Table 27-16](#)).

Figure 27-24: Example output from the **show qos prio2queuemap** command

Vlan Tag	User Priority	Queue
0		2
1		0
2		1
3		3
4		4
5		5
6		6
7		7

Table 27-16: Parameters in output of the **show qos prio2queuemap** command

Parameter	Meaning
User Priority	User Priority field in the untagged frame transmitted on the egress port.
Queue	Number of the egress queue.

Examples To displays the default VLAN tag User Priority to queue mapping scheme, use the command:

```
sh qos prio2
```

Related Commands [set qos prio2queuemap](#)

show qos red

Syntax `SHoW QoS RED[={red-id|ALL}] [QUEue=queue-list]`

Description This command displays configuration information about one RED curve set or all RED curves.

Parameter	Description
RED	RED curve set for which to display information. Default: all
<i>red-id</i>	Integer from 1 to 4 for a specific RED curve set (Figure 27-26 on page 27-119, Table 27-18 on page 27-119).
ALL	Displays all RED curve sets (Figure 27-25, Table 27-17).
QUEue	Egress queue that belongs to the port (Figure 27-27 on page 27-120, Table 27-19 on page 27-120). The <i>queue-list</i> consists of: an integer from 0 to 7 a range specified with a hyphen, such as 1-4 a comma-separated list of numbers and/or ranges Default: no default

Figure 27-25: Example output from the **show qos red** command

Random Early Detection Information			
Id	Description	Assigned Ports	Ports using Tail Drop
1	Red1	4, 5	1, 10-52
2	Red2	3, 9	
3	Red3	None	
4	Red4	2, 6-8	

Table 27-17: Parameters in output of the **show qos red** command

Parameter	Meaning
Identifier	Numerical identifier of the RED curve set.
Description	Description of the RED curve set.
Assigned Ports	Number of the ports to which the RED curve is assigned.
Ports using Tail Drop	Number of the port using the default RED curve set in Tail Drop mode. Displayed for RED=1 only.

Figure 27-26: Example output from the **show qos red=1** command

```

QOS RED Curve Information

Identifier ..... 1(default)
Description ..... redOne
Assigned Ports ..... 4,5
Ports using Tail-Drop ..... 1,10-52

Queue 0:
  Queue length averaging factor ... 9
  BandwidthClass   Start           Stop           Drop Probability Factor
  -----
  1                 25kbytes       30Kbytes       1 (50%)
  2                 20kbytes       25Kbytes       1 (50%)
  3                 10kbytes       15Kbytes       0 (50%)
  -----

Queue 1:
  Queue length averaging factor ... 9
  BandwidthClass   Start           Stop           Drop Probability Factor
  -----
  1                 25kbytes       30Kbytes       1 (50%)
  2                 20kbytes       25Kbytes       1 (50%)
  3                 10kbytes       15Kbytes       1 (50%)
  -----

Queue 2:
  Queue length averaging factor ... 9
  BandwidthClass   Start           Stop           Drop Probability Factor
  -----
  1                 25kbytes       30Kbytes       1 (50%)
  2                 20kbytes       25Kbytes       1 (50%)
  3                 10kbytes       15Kbytes       1 (50%)
  -----

.
.
.
Queue 7:
  Queue length averaging factor ... 9
  BandwidthClass   Start           Stop           Drop Probability Factor
  -----
  1                 25kbytes       30Kbytes       1 (50%)
  2                 20kbytes       25Kbytes       1 (50%)
  3                 10kbytes       15Kbytes       1 (50%)
  -----

```

Table 27-18: Parameters in output of the **show qos red=1** command

Parameter	Meaning
Identifier	Numerical identifier of the RED curve.
Description	Description of the RED curve.
Assigned Ports	Number of the ports to which the RED curve is assigned.
Ports using Tail Drop	Number of the ports using the default RED curve set in Tail Drop mode. Only displayed for RED=1.
Queue	Number of egress queue.
Queue length averaging factor	Weight to use in the time-based averaging calculation of queue length for the RED curve algorithm.

Table 27-18: Parameters in output of the **show qos red=1** command (cont.)

Parameter	Meaning
BandwidthClass	Bandwidth class for which each set of start , stop , and drop settings applies on the specified queue.
Start	Queue length in bytes at which the RED probability leaves the baseline for frames associated with each bandwidth class.
Stop	Queue length in bytes at which the RED probability reaches the top of the linear portion of the curve for frames associated with each bandwidth class.
Drop Probability Factor	Maximum drop probability for frames associated with each bandwidth class on a RED curve controlled queue at the length specified by stop .

Figure 27-27: Example output from the **show qos red=2 queue=1** command

```

QOS RED Curve Information
-----
Identifier ..... 19
Description ..... fRed
Ports Assigned to ..... 3,9

Queue 1:
  Queue length averaging factor ... 9
  BandwidthClass   Start       Stop           Drop Probability Factor
  -----
  1                25kbytes   30Kbytes       1 (50%)
  2                20kbytes   25Kbytes       1 (50%)
  3                10kbytes   15Kbytes       1 (50%)
  -----

```

Table 27-19: Parameters in output of the **show qos red=2 queue=1** command

Parameter	Meaning
Identifier	Numerical identifier of the RED curve.
Description	Description of the RED curve.
Assigned Ports	Number of the ports to which the RED curve is assigned.
Queue	Number of egress queue.
Queue length averaging factor	Weight to use in the time-based averaging calculation of queue length for the RED curve algorithm.
BandwidthClass	Bandwidth class for which each set of start , stop , and drop settings applies on the specified queue.
Start	Queue length in bytes, at which the RED probability leaves the baseline for frames associated with each bandwidth class.
Stop	Queue length in bytes at which the RED probability reaches the top of the linear portion of the curve for frames associated with each bandwidth class.
Drop Probability Factor	Maximum drop probability for frames associated with each bandwidth class on a RED curve controlled queue at the length specified by stop .

Examples To display configuration information for all RED curves, use one of the following commands:

```
sh qos red=all
```

```
sh qos red
```

Related Commands [create qos red](#)
[destroy qos red](#)
[set qos red](#)

show qos trafficclass

Syntax `SHoW QoS TRAfficclass[={id|ALL}]`

Description This command displays configuration information about one or more QoS traffic classes.

If no value is given on the **trafficclass** parameter, summary information about all traffic classes is displayed ([Figure 27-28](#), [Table 27-20](#)).

If a traffic class is specified, details about it are displayed ([Figure 27-29 on page 27-123](#), [Table 27-21 on page 27-123](#)). The *id* can be an integer from 0 to 1023.

If **all** is specified, all traffic classes are displayed.

Figure 27-28: Example output from the **show qos trafficclass** command

QoS Traffic Class Information			
Id	Description	Policy	FlowGroups
1	FTP Traffic	3	1-3,16
13	Telnet Traffic	None	None
18	Interactive Voi	1	8-11
23	TCP/IP Traffic	6	12,14,17-18

Table 27-20: Parameters in output of the **show qos trafficclass** command

Parameter	Meaning
Id	Numerical identifier for the traffic class.
Description	Description for the traffic class.
Policy Assigned to	Numerical identifiers of the policy to which the traffic class is assigned.
FlowGroups	Numerical identifiers of the flow groups assigned to this traffic class.

Figure 27-29: Example output from the **show qos trafficclass=18** command

```

Identifier ..... 18
Description ..... Interactive Voice
Policy Assigned to ..... 1
Flow Groups ..... 8-11
Drop BandwidthClass3 ..... YES
Ignore BandwidthClass ..... YES
Maximum Bandwidth ..... 10Mbps
Maximum Burst Size ..... 64kbyte
Minimum Bandwidth ..... None
Minimum Burst Size ..... None
Premarking ..... USEMARKVALUE
Remarking ..... USEDSCPMAP
Mark Value ..... 0
Action ..... SENDVLANPORT
    VLAN ..... 2
    Port ..... 4
Storm Protection:
    Status ..... ENABLED
    Action ..... PORTDISABLE
    Rate ..... 1kbps
    Window ..... 100ms
    Timeout ..... None

```

Table 27-21: Parameters in output of the **show qos trafficclass=18** command

Parameter	Meaning
Identifier	Numerical identifier of the traffic class.
Description	Description for the traffic class.
Policy Assigned to	Numerical identifiers of the Policy to which the traffic class is assigned.
Flow Groups	Numerical identifiers of the Flow Groups assigned to this traffic class.
Drop BandwidthClass3	Specifies whether frames exceeding the traffic class maximum bandwidth setting should be dropped.
Ignore BandwidthClass	Specifies whether the metering stage acknowledges any previous bandwidth class assigned to flows processed by this traffic class.
Maximum Bandwidth	Specifies the maximum bandwidth in Kbps, Mbps, or Gbps available to the traffic class.
Maximum Burst Size	Specifies the burst tolerance for maximum bandwidth.
Minimum Bandwidth	Minimum bandwidth in Kbps, Mbps, or Gbps guaranteed to the traffic class.
Minimum Burst Size	Specifies the burst tolerance for minimum bandwidth.
Premarking	Specifies the QoS action to take on the traffic class before any bandwidth metering is applied.
Remarking	Specifies the action to take after the metering stage.
Mark Value	Specifies an explicit value to use as an index into the DSCPMAP table.
Action	Action taken on traffic belonging to the traffic class. For more information, see “Configuration Examples” on page 27-40.
Port	Port where traffic is sent when action is sendvlanport .
VLAN	VLAN where traffic is sent when action is sendvlanport .

Table 27-21: Parameters in output of the **show qos trafficclass=18** command

Parameter	Meaning
Storm Protection settings	
Status	Whether storm protection is enabled for the default traffic class.
Action	Whether the port is administratively or operationally disabled when the volume of traffic exceeds the rate .
Rate	Allowable traffic volume before action is executed.
Window	Interval in milliseconds between checking the traffic class for storms.
Timeout	Length of time in seconds that the port remains disabled when it is disabled by storm protection.

Examples To display summary information for all traffic classes, use the command:

```
sh qos tr
```

To display detailed configuration information for traffic class 12, use the command:

```
sh qos tr=12
```

Related Commands

- [add qos trafficclass](#)
- [create qos trafficclass](#)
- [delete qos trafficclass](#)
- [destroy qos trafficclass](#)
- [set qos trafficclass](#)