5 The QoS Manager

QoS Overview

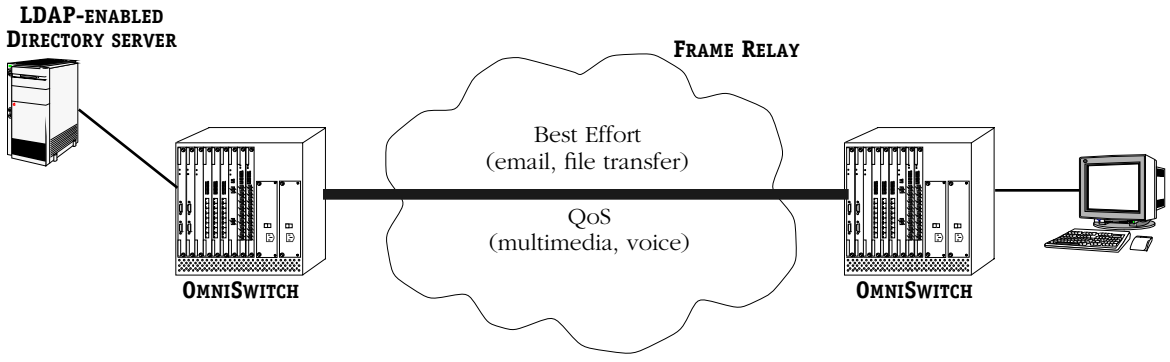
Quality of Service (QoS) refers to transmission quality and available service that is measured and sometimes guaranteed in advance for a particular type of traffic in a network. QoS lends itself to circuit-switched networks like ATM, which bundle traffic into cells of the same length and transmit the traffic over predefined virtual paths. In contrast, Frame Relay, IP, and other packet-switched networks operate on the concept of shared resources and "best effort" routing, using bandwidth as needed and reassembling packets at their destinations. Applying QoS to these networks requires some different mechanisms.

This chapter describes the QoS Manager, which is one building block used in the switch to apply QoS to packet-switched flows. See the "Managing Cell Switching Modules" chapter of your switch user manual for information about QoS parameters for ATM networks.

QoS is often defined as a way to manage bandwidth. Another way to handle different types of flows and increasing bandwidth requirements is to add more bandwidth. But bandwidth is expensive, particularly at the WAN connection. And if LAN links that connect to the WAN are not given more bandwidth, bottlenecks can still occur. Also, adding enough bandwidth to compensate for peak load periods will mean that at times some bandwidth will be unused. In addition, adding bandwidth does not guarantee any kind of control over network resources.

Using QoS, a network administrator can gain more control over networks where different types of traffic (or *flows*) are in use or where network congestion is high (such as on a WAN link like Frame Relay). Individual flows can receive preferential treatment as needed. Voice over IP (VoIP) traffic or mission-critical data can be marked as priority traffic and/or given more bandwidth on the link. QoS can also prevent large flows (like a video stream) from consuming all the link's bandwidth. Using QoS, a network administrator can decide which traffic needs preferential treatment, and which traffic can be adequately served with best effort.

QoS can also be negotiated by the flow itself through signaling via the Resource ReSerVation Protocol (RSVP). At each hop, the flow's requirements are checked and enforced if the switch allows the requested service. See Chapter 7, "The Resource Reservation Protocol," for more information about RSVP.



QoS Application

QoS and WAN Switching Modules (WSMs)

The Omni Switch/Router currently supports QoS over WAN Switching Modules (OSWSM, WSM3, or WSX) running Frame Relay. For more details about WSMs and Frame Relay, see the "Managing WAN Switching Modules (WSMs)" and "Managing Frame Relay" chapters of your switch manual.

Each WSM can support up to 32 queues per virtual port, 128 queues per WSM slot.

QoS Manager Overview

The switch has two software components it uses to make decisions about applying QoS to flows: the QoS Manager and the Policy Manager. This chapter describes the functions of the QoS Manager and how they relate to the Policy Manager. For more information, see Chapter 6, "The Policy Manager."

A submodule of the QoS Manager, the Classifier, has two functions. First, it classifies the first frame of a QoS flow and sends this classification to the Policy Manager to determine the type of QoS that should be applied (this is called *policy decision*). Second, it classifies subsequent frames in the flow to make sure they are mapped to the appropriate queue (this is called *policy enforcement*).

QoS Policy Decision

The policy decision is made one time for the flow, based on the first frame of the flow. The QoS Manager classifies the first frame of an incoming flow as either layer 2 (identified by MAC address) or layer 3 traffic (identified by source or destination IP address). The flow is then matched to a policy.

♦ Important Note ♦

Layer 2 information is identified for traffic that is switched. Layer 3 information is identified for traffic that is routed when an HRE-X is installed on the switch.

For the policy decision, the QoS Manager and Policy Manager interact differently depending on whether the flow is layer 2 or layer 3.

Policy Decision for Layer 2 Flows

If the QoS Manager identifies the first frame of a flow as layer 2 traffic, it checks for any policies created through the QoS Manager UI that match the flow. If no policies for the layer 2 flow are found in the QoS Manager, the QoS Manager polls the Policy Manager for a matching policy. The Policy Manager then polls an attached LDAP-enabled server for policies. (Policies on the LDAP-enabled server are created through the PolicyView application. See Chapter 5 for more details.) Any matching policies are downloaded to the switch. If no policies are found, a default policy for the traffic is used. (Default policies are set up through the Policy Manager.)

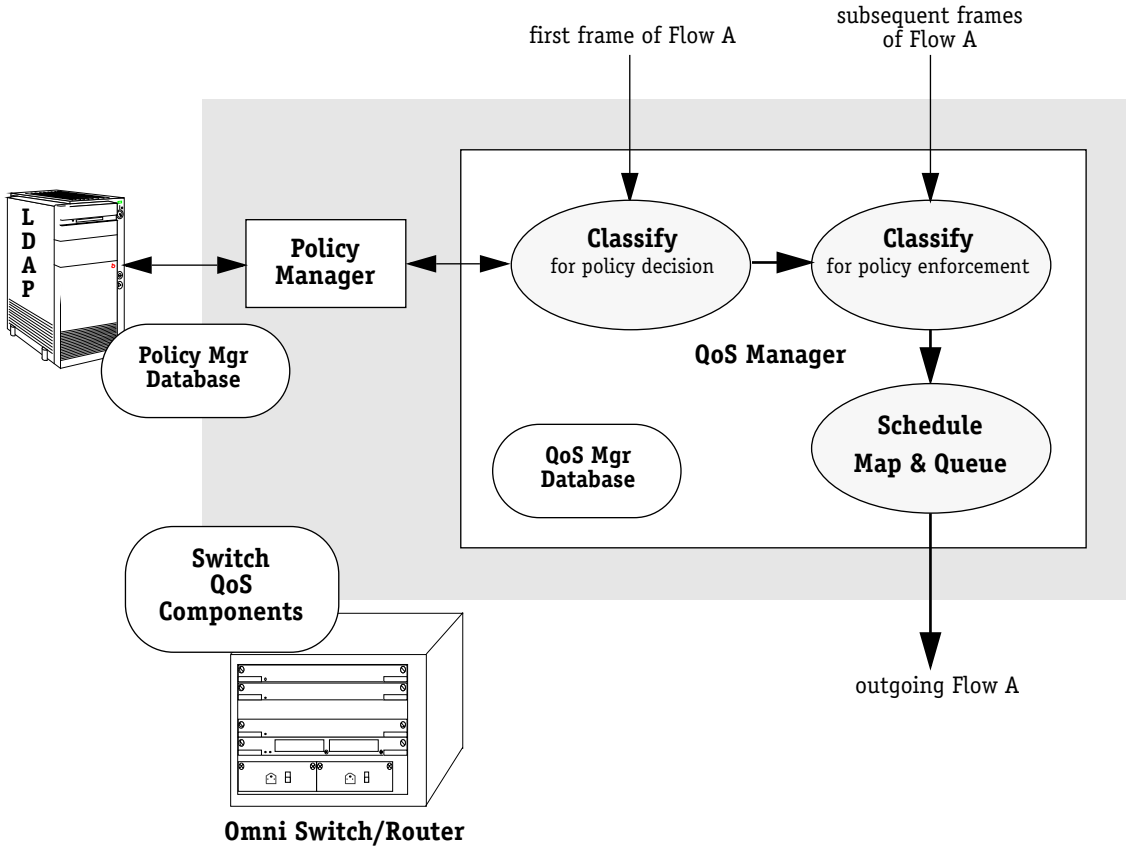
Policy Decision for Layer 3 Flows

At switch startup, the Policy Manager polls the attached LDAP-enabled server for all Layer 3 policies. The Layer 3 policies are downloaded to the switch and merged with Layer 3 policies created through the QoS Manager UI. When the first frame of a Layer 3 flow arrives on the switch, the QoS Manager checks for matching policies on the switch. If no policies are found, the flow is treated as best effort.

For all subsequent frames in the flow, the QoS Manager identifies the frame and associates it with the relevant policy. It then schedules the flow on the output port and maps the flow to a queue.

Based on the action and condition specified by the policy, the QoS Manager classifies the flow, schedules the flow on the output port, and maps the flow to a queue.

These functions are illustrated here and described in the following sections of this chapter.



How QoS Is Applied

Provisioned and RSVP Traffic

QoS flows coming into the switch may be either *provisioned* or *RSVP* traffic. Any flow that does not fall into either of these categories, or for which there is no QoS policy, is treated by the switch as best-effort traffic.

- Provisioned flows may be layer 2 or layer 3 traffic that the switch identifies from information in the header of the first arrived packet. All policies configured through the QoS Manager UI are considered "provisioned."
- RSVP flows are layer 3 traffic that uses the Resource ReSerVation Protocol to request bandwidth. RSVP allows an end station to send a reservation request for bandwidth prior to actually sending the data stream that requires it. The switch identifies the flow as RSVP and determines whether to accept or deny the request. If the request is denied, the flow is treated as best effort. If the request is allowed, the flow must adhere to the signaled rate.

♦ Note ♦

RSVP policies may only be configured through the PolicyView application. RSVP is described in Chapter 7, "Resource Reservation Protocol."

Traffic Parameters for Provisioned Flows

An overview of traffic parameters that may be configured in policies for provisioned traffic are listed here. (Traffic parameters in policies for RSVP flows may only be configured through the PolicyView application.) For additional information about policies, see Chapter 6, "The Policy Manager." Information about policies is also included in the help text for the PolicyView application.

In the current release of QoS software, bandwidth and queue parameters are the only configurable traffic parameters. They are described here:

Minimum and Maximum Bandwidth—The minimum and maximum bandwidth may be configured for the provisioned flow. The maximum bandwidth value depends on the data rate of the physical port. For WSMs, the maximum bandwidth may be up to 2,048 kbps, depending on the type of module. See the "Managing WAN Switching Modules" chapter of your switch user manual.

Queue Parameters—The queue parameters include priority level, queue depth, and the maximum number of buffers allowed for the queue. The priority level indicates which queue the flow should be scheduled on. There are four priority levels, from 0 (highest priority) to 3 (lowest priority). The queue depth indicates the number of total bytes that may be buffered in a queue before the switch starts dropping packets.

QoS Policy Enforcement

Once the flow is classified for a policy decision, and a policy is assigned to the flow by the Policy Manager, the QoS Manager enforces the policy by mapping each packet of the flow to the appropriate queue and scheduling it on the output port.

Mapping and Queuing Flows

The QoS Manager uses the QoS policy to map queues onto virtual ports (VPNs) of network interfaces. The QoS Manager stores an identification policy tag for the flow so that additional frames coming in from this flow can be classified for policy enforcement and placed into the correct queue. For layer 2 flows, the QoS Manager maps the flow to a QoS queue on the relevant interface. For layer 3 flows, the QoS Manager configures the HRE-X so that all frames matching the identification policy tag will be queued on the interface.

Queues are mapped by the switch according to the priority configured in the policy for the arriving flow. The action in the flow's policy specifies the priority. The number of flows per queue is determined by the number of conditions configured for the action and the number of flows with those conditions that arrive on the switch. If multiple flows (multiple conditions) have the same action, more than one flow will be scheduled on the same queue.

If the policy for an incoming flow specifies a destination address, the queue is mapped on the VPN for that address. If a policy for an incoming flow specifies only a source address, queues may be mapped on more than one VPN to handle the flow.

Queues that are set up on the same VPN are considered a QoS group. In the current release of QoS software, the switch automatically places all queues into QoS group 1 for the VPN. (Note that QoS groups are different from VLAN groups on the switch.) In future releases, additional QoS groups may be user-configured on a single VPN.

Up to 128 queues may be set up on a WSM, with 32 queues per VPN.

Shaping Flows

By nature, packet-switched flows are bursty. Shaping ensures that flows are sent out at the bandwidth rate specified in the flow's policy. The scheduling algorithm in the switch will shape the incoming flow to level the burstiness of the flow through the output port.

The scheduler determines how many frames from each queue to send at one time. The scheduling algorithm is similar to a well-known scheduling algorithm called weighted fair queuing. Frames are forwarded from each non-empty queue in order of priority. A frame in one queue will not have to wait until another queue is entirely empty before it is sent through the output port.

Hardware/Software Requirements

The QoS Manager supports layer 2 QoS on all WSXs on the Omni Switch/Router (OmniS/R), later generation WSMs on the OmniSwitch, and all OSWSMs on the 2xxx, 3xxx, and 5xxx models of OmniStack.

The QoS Manager supports layer 3 QoS on all OmniS/Rs. For the QoS Manager to classify layer 3 traffic, routing must be enabled, and an HRE-X must be installed on the switch. (In future releases, layer 3 QoS will also be supported on OmniSwitches with later-generation WSMs and an HRE-VX.)

Installing the QoS Manager

To run the QoS Manager, the **qos.img** file must be loaded on the switch. To upload the file, use standard FTP or ZMODEM procedures. Refer to your switch user manual for information about uploading the software.

Configuring QoS

Most QoS configuration consists of creating QoS policies through the PolicyView application, configuring the Policy Manager through the switch UI, and enabling the QoS Manager. Some provisioned policies may also be configured through the QoS Manager UI.

This section describes the basic steps required to configure the QoS Manager as well as other QoS components on the switch. QoS Manager configuration is described in this chapter. Policy Manager and RSVP configuration are described in other chapters as indicated.

Step 1. Configure the Policy Manager Components

- The Policy Manager image file (**policy.img**) must be installed on the switch. See Chapter 6, "The Policy Manager," for details about installation and for more information about configuring the Policy Manager and the external components described here.
- If you are using an LDAP-enabled directory server for managing policies, the following external components are required:
  - An external LDAP-enabled directory server must be connected to the switch. Primary and secondary servers are recommended for redundancy. See Chapter 8, "IP Control," for more information about LDAP-enabled servers. The server must configured with the necessary schema extensions. Java Runtime Environment 1.1 must be installed on the workstation running PolicyView.
  - The PolicyView NMS management application must be installed on an external workstation that is attached to the directory server. Solaris (UNIX) and Windows NT are supported. A web browser must also be installed on the workstation.
  - The Policy Manager must be configured to recognize LDAP-enabled servers.

Step 2. Configure Policies

- Configure policies on the policy server using the PolicyView application. See Chapter 5, "The Policy Manager," for more information about policies and PolicyView.
- Set up default policies for provisional flows using the Policy Manager UI commands. Typically, when a flow comes into the switch and no policy exists for the flow in the Policy Manager database or the QoS Manager database, the flow is treated as best-effort traffic. However, default policies may be set up using the **pqosdef** command so that particular flows have priority. See Chapter 5, "The Policy Manager," for more information about this command.
- By default, when there are no policies for an RSVP flow, the flow is accepted on the switch and treated as best effort. Use the **qparams** command if you want the switch to deny any RSVP flow for which there are no policies. See *Modifying QoS Manager Parameters* on page 5-10.
- *Optional.* Create policies through the QoS Manager by adding actions and conditions through the **qosaa** and **qosac** commands. Actions are used to apply queue parameters to particular flows. Conditions are used to associate particular flows with QoS actions. Adding actions/conditions through the QoS Manager is not necessary if you have configured policies through the PolicyView application.

Step 3. Enable the QoS Manager

- By default, the QoS Manager is disabled on the switch. Enable the QoS Manager using the **qparams** command. See *Modifying QoS Manager Parameters* on page 5-10.
- Statistics are available for tracking the number of layer 2 and layer 3 events on the switch. Information may also be displayed for all QoS actions and conditions that have been configured on or downloaded to the switch. Commands for these statistics are listed in the QoS submenu. See *QoS Manager UI Commands* on page 5-9.
- Use the **mapper** submenu to display statistics about physical/virtual ports and queues. See *Mapper Submenu* on page 5-21.

QoS Configuration Example

This is a basic example of how QoS policies influence the creation of queues on the switch. For the purposes of this chapter, it assumes you are using the QoS Manager to create the policies; however, the policies described would typically be created with Alcatel's PolicyView application.

Policies consist of an action and a condition. Use the PolicyView application or the QoS Manager UI described in this chapter to create policies. For example:

Action ID	Min Band	Max Band	Priority	Shared Queue
1	128k	—	1	No
2	512k	—	0	No
3	0	256k	2	Yes

Create conditions associated with the actions. For example:

Condition	Action ID	Min Band	Max Band	Priority	Shared Queue
Source addr=173.22.4.1 Source mask=255.255.0.0	1	128k	—	1	No
Source address=173.25.5.8 Source mask=255.255.0.0	1	128k	—	1	No
Source address=173.28.10.2 Source mask=255.255.0.0	1	128k	—	1	No
Source address=10.4.3.2	2	512k	—	0	No
Dest. port=21 (FTP)	3	0	256k	2	Yes
Dest. port=23 (Telnet)	3	0	256k	2	Yes

If there are flows coming into the switch that match all of the above conditions, the switch will create 5 queues on the WSM VPN(s).

- Three queues would be created to handle the three flows coming in from subnets. These flow conditions are associated with Action ID 1. Three separate queues are created because the policy specifies that the flows will not share queues.
- One queue is created for the highest priority flow, which is traffic from a particular source address. The policy specifies that the queue cannot be shared.
- One queue is created for the FTP and Telnet traffic. The policies for these flows specify that the queue may be shared, so the switch maps these flows to the same queue.

QoS Manager UI Commands

When the QoS Manager is loaded into the switch, it adds a submenu to the Networking menu of the User Interface (UI).

Commands in the UI are executed by typing the command and pressing **<Enter>**. On configuration screens, parameters may be changed by entering the number next to the relevant parameter, an equal sign, and the desired value at the prompt. After changes are made, press **<Enter>** to redraw the screen and see the changed value(s) or press **q** to quit the screen.

♦ Note ♦

For general information about the UI, see your switch user manual.

To display the QoS Manager submenu, enter **qos** at the system prompt.

If the UI is configured for terse mode, enter a **?** to display the submenu. In verbose mode, the UI automatically displays the submenu.

```
Command          QoS Menu
---------------- ------------------------------------------------------------
qparams          Display and modify manager parameters
qostats          Display QoS Manager statistics
qossa            Show classification actions
qosaa            Add a classification action
qosda            Delete a classification action
qosma            Modify a classification action
qossc            Show classification conditions
qosac            Add a classification condition
qosdc            Delete a classification condition
qosmc            Modify a classification condition
mapper           Enter the QoS/Mapper menu

    Main      File      Summary  VLAN      Networking
    Interface Security  System   Services  Help
```

You can get help for parameters listed on these screens by entering the number corresponding to the parameter, an equal sign, and **help** or **h**.

For example:

```
1=help
```

You can also get the syntax for configuring a parameter by entering the number corresponding to the parameter, an equal sign, and a question mark.

For example:

```
1=?
```

Modifying QoS Manager Parameters

Use the QoS Manager Configuration screen to enable or disable the QoS Manager, enable or disable RSVP on the switch, or set the debug level. To display the QoS Manager screen, enter the following command:

```
qparams
```

The screen displays similar to the following:

```
                QoS Manager Configuration

1) QoS Manager Enabled    : No
2) RSVP Enabled           : No
4) Debug Level            : 0

Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw):
```

Fields are defined as follows:

QoS Manager Enabled

Enables (**yes**) or disables (**no**) the QoS Manager. The QoS Manager is disabled by default. When disabled, the QoS Manager will continue to examine incoming packets and classify flows. It will also consult the Policy Manager for appropriate policies, but it will not enforce the policies when it is disabled.

RSVP Enabled

Enables (**yes**) or disables (**no**) RSVP on the switch. The switch must be rebooted before a change to this parameter will take effect.

Debug Level

Changes the level of detail given in diagnostic messages.

To modify parameters on the QoS Manager Configuration screen:

1. At the prompt, enter the desired parameter number, an equal sign, and the desired value. For example, to enable the QoS Manager, enter the following:

   ```
   1=y
   ```

2. Enter any other changes in the same way.

3. Enter **s** to save the changes, then **q** to quit the screen. If you changed the RSVP Enabled parameter, the switch must be rebooted.

Viewing QoS Manager Statistics

You can view information about layer 2 and layer 3 provisioned flows as well as RSVP flows on the switch. To view these statistics, enter the following command:

qostats

The screen displays similar to the following:

```
QoS Statistics
L2 Events:          1
L3 Events:          0
RSVPEvents:         0
RSVPAccept:         0
RSVPFailed:         0
Num Conditions:     0
Num Actions:        0
Num Queues:         0
Num Groups:         0
```

Fields are defined as follows:

L2 Events. The number of provisioned flows received on the switch and classified by MAC address (layer 2).

L3 Events. The number of provisioned flows received on the switch and classified by IP address (layer 3).

RSVPEvents. The total number of RSVP reservation requests received on the switch.

RSVPAccepts. The number of RSVP reservation requests accepted on the switch.

RSVPFailed. The number of RSVP reservation requests denied on the switch because of lack of resources to support the flow.

Num Conditions. The number of conditions configured through the QoS Manager.

Num Actions. The number of actions configured through the QoS Manager.

Num Queues. The number of queues configured on the switch.

Num Groups. The number of QoS resource groups configured on the switch. Resource groups are configured by associating multiple QoS conditions with a QoS action. QoS groups are *not* the same as VLAN groups on the switch.

Configuring QoS Actions

A QoS action is a particular set of bandwidth and queue parameters that may be applied to multiple QoS conditions. An action defines the characteristics of a QoS group (resource group).

♦ Note ♦

QoS groups are not the same as VLAN groups on the switch. VLAN groups may be associated with QoS conditions through the PolicyView application.

QoS classification actions may be added, modified, or deleted. At least one QoS action must be configured on the switch (through the PolicyView application or through the QoS Manager UI) in order for QoS to be active. Actions are configured using the Add QoS action screen. To display the Add QoS action screen, enter the following command:

```
qosaa
```

The screen displays similar to the following:

```
                    Add QoS action

1) QOS Action id:                0
2) Bandwidth                     :
   21) Min bandwidth (bits/sec):       0
   22) Max bandwidth (bits/sec):       0
3) Queue                         :
   31) Shared                    :   No
   32) Depth (bytes)             :   0
   33) Buffers                   :   0
   34) Priority                  :   0
   35) *802.1p bits              :   0
   36) *Latency (usec)           :   0
   37) *Jitter                   :   0
   38) *TOS                      :   0

Command {Item=Value/?/Help/Quit/Save/Redraw} (Redraw):
```

♦ Note ♦

Asterisks indicate that the parameter is not yet supported for QoS classification on the switch.

The parameters are defined as follows:

QOS Action id

A number that identifies the QoS action, in the range 1 to 65535.

Min bandwidth (bits/sec)

The minimum bandwidth for the QoS action, in bits per second. The maximum bandwidth that is dependent on the type of module you are using. For WSMs, the maximum bandwidth may be up to 2,048 kbps. Check your switch user manual for information about your module's bandwidth. If you configure this value to be the maximum bandwidth, the Max bandwidth parameter does not have to be set.

Max bandwidth (bits/sec)

The maximum bandwidth for the QoS action, in bits per second. The maximum bandwidth that is dependent on the type of module you are using. For WSMs, the maximum bandwidth may be up to 2,048 kbps. Check your switch user manual for information about your module's bandwidth.

Shared

Specifies whether the queue may be shared by flows of different priorities (either **Yes** or **No**). Typically a queue buffers traffic for one priority level. Sharing queues enables effective use of overall buffer resources because there is a statistical chance that traffic of one priority will need additional buffers while traffic of another priority will have unused buffers. If this parameter is set to **Yes**, buffers still may be reclaimed by higher priority flows.

Depth (bytes)

The maximum queue depth assigned to this action, in bytes. The queue depth determines the amount of buffer allocated to each queue. When the queue depth is reached, the switch will start dropping packets.

Buffers

The maximum number of buffers that may be assigned to this action. The maximum number of buffers on a WSM that may be used for queues is 128.

Priority

The priority given to scheduling and queuing the flow on the output port, from 0 (highest priority) to 3 (lowest). The lowest priority is best effort, which is allocated only bandwidth that is not allocated to any higher priority queue(s).

802.1p bits

For ports that are configured for 802.1Q, which is a layer 2 VLAN tagging mechanism, this value defines the priority to be set on outgoing layer 2 frames. When a frame is queued, it is assigned the priority of the queue and mapped to the outgoing 802.1p priority. The priority is combined with the VLAN group ID to create the 802.1p/Q header for transmission. The range of values is 0 (highest priority) to 7 (lowest priority). See "Managing 802.1Q Groups" in your switch user manual for more information about 802.1Q.

Latency (usec)

The maximum amount of delay, in microseconds, that is allowed for packets in the flow. Delay may occur when packets wait in a buffer or when packets wait for other traffic to be transmitted.

Jitter

The variance in delay, in milliseconds.

TOS

A three-bit Type of Service (ToS) value that indicates priority for outgoing layer 3 frames. The range of values is 0 (highest priority) to 255 (lowest priority). This bit is set when the frame is transmitted on the output port.

Adding a New Action

To *add* a new action:

1. At the prompt for the Add QoS action screen, enter the relevant action ID. For example:

   1=1

2. Enter the minimum bandwidth (in bits per second) that the action will support. For example:

   2=1000

3. Enter the maximum bandwidth (in bits per second) that the action will support. For example:

   3=5000

4. Enter any other desired parameters in the same way.

5. Enter **s** for save, then **q** to quit the screen.

Modifying an Action

Only actions configured with the **qosaa** command may be modified using the **qosmc** command. To *modify* an existing QoS action, enter the **qoscm** command with the relevant action ID. For example:

qosmc 1

The screen displays information for the specified QoS action. Modify any desired parameters as described for adding a new action in *Adding a New Action* on page 5-14. Enter **s** to save your changes.

Deleting an Action

Only actions configured with the **qosaa** command may be deleted through the **qosdc** command. To *delete* an existing QoS action, enter the **qosdc** command with the relevant action ID. For example:

qosdc 2

The indicated action is deleted from the configuration.

Displaying QoS Actions

To display the current QoS actions, enter the following command:

```
qossa
```

The screen displays similar to the following:

```
Action  Bandwidth (bps)  Depth/Buf  Pri  Lat   Jit  TOS  DS Group  NumC/NumQ
1u      10 -  0          0/ 0       0    0     0    0    0  1      0/    0
2        0 -  0          0/ 0       0    0     0    0    0  2      0/    0
```

These parameters are configured when you add an action using the **qosaa** command.

Action. The action ID number and an indication of how the action was received on the switch.

- **u** — configured through the QoS Manager UI
- **l** — pushed down from an LDAP-enabled directory server through Policy Manager
- **p** — received by a layer 2 policy request
- **r** — signaled via RSVP
- ***** — indicates that the action contains traffic parameters not supported on the switch

Bandwidth (bps). The range of bandwidth (minimum and maximum) configured for the action, in bits per second.

Depth/Bufs. The queue depth and the number of buffers associated with the queue.

Priority. The priority associated with the QoS action, in the range from 0 to 7.

Latency. The latency associated with the QoS action.

Jit. The jitter associated with the QoS action.

802.1p. The 802.1p bit associated with the QoS action. (Not supported in the current release.)

DS. The Differentiated Service value. (Not supported in the current release.)

Group. The QoS resource group. Resource groups are configured by associating multiple QoS conditions with a QoS action.

NumC/NumQ. The number of conditions associated with this action and the number of queues created for this action. Conditions are described in *Configuring QoS Conditions* on page 5-16.

Configuring QoS Conditions

QoS classification conditions are used to associate layer 2 or layer 3 traffic with a particular QoS action. For layer 3 traffic, a particular QoS action may be associated with traffic flowing from a particular IP source and destination, a source and destination TCP/UDP number, or a protocol. For layer 2 traffic, a QoS action may be associated with traffic flowing from a specific source MAC address and a specific destination MAC address, traffic flowing from a specific source VLAN to a specific destination VLAN, traffic flowing from a specific slot/port to a specific destination slot/port, or traffic flowing from a particular source interface to a particular destination interface. Parameters may be used in combination to specify the flow.

♦ Note ♦

Conditions and actions for RSVP traffic must be configured through the PolicyView application. For more information about PolicyView, see Chapter 6, "The Policy Manager."

Conditions are configured using the Add QoS condition screen. To display the Add QoS condition screen, enter the following command:

```
qosac
```

The screen displays similar to the following:

```
                    Add QoS condition

1) QoS Action Id              : 0
2) Precedence                 : 0
3) Layer 3                    :
    30) Source IP                 : Any
    31) Source Mask               : Any
    32) Dest IP                   : Any
    33) Dest Mask                 : Any
    34) Source TCP/UDP Port       : Any
    35) Dest TCP/UDP Port         : Any
    36)* Protocol                 : Any
    37) *TOS                      : Any
4) Layer 2                    :
    40) *Source MAC               : Any
    41) Dest MAC                  : Any
    42) *Source VLAN              : Any
    43) Dest VLAN                 : Any
    44) *Source VPN               : Any
    45) Dest VPN                  : Any
    46) *Source slot/port         : Any
    47) Dest slot/port            : Any
    48) *Source IFtype            : Any
    49) *DestIFtype               : Any

Command {Item=Value/?/Help/Quit/Save/Redraw} (Redraw):
```

♦ Note ♦

Asterisks indicate that the parameter is not yet supported for QoS classification on the switch.

The parameters are defined as follows:

QoS Action Id

The QoS action associated with the condition. QoS actions are defined using the **qosaa** command. An action must already be configured through the **qosaa** command to be associated with a condition on this screen.

Precedence

The precedence that this rule takes over any other condition for the same flow. This value must be a number in the range 1 to 65535. A higher number indicates a higher precedence. If a flow matches multiple conditions, it is queued according to the condition with the highest precedence.

Source IP

The source IP address of the layer 3 flow.

Source Mask

The source IP address mask of the layer 3 flow.

Dest IP

The destination IP address of the layer 3 flow.

Dest Mask

The destination IP address mask of the layer 3 flow.

Source VPN

The source virtual port number of the layer 3 flow.

Dest VPN

The destination virtual port number of the layer 3 flow.

Source TCP/UDP Port

The TCP or UDP port number of the source address of the layer 3 flow.

Dest TCP/UDP Port

The TCP or UDP port number of the destination address of the layer 3 flow.

Protocol

The protocol associated with the layer 3 flow.

Source MAC

The source MAC address of the layer 2 flow.

Dest MAC

The destination MAC address of the layer 2 flow.

Source VLAN

The source VLAN of the layer 2 flow.

Dest VLAN

The destination VLAN of the RSVP flow for this condition.

Source slot/port

The slot/port number of the source address of the RSVP flow for this QoS condition.

Dest slot/port

The slot/port number of the destination address of the RSVP flow for this QoS condition.

Source IFtype

The interface on which the RSVP flow arrives for this QoS condition.

DestIFtype

The interface on which the RSVP flow is transmitted for this QoS condition.

Adding a Condition

To *add* a QoS condition:

1. Make sure that at least one action is configured on the switch through the **qosaa** command. To display currently configured actions, use the **qossa** command.
2. At the prompt for the Add QoS rule screen, enter the layer 3 or layer 2 parameters relevant to the rule. Enter the number next to the parameter, an equal sign, and the desired value.
3. Enter the desired precedence for the condition. For example:

   3=1

4. Enter the QoS class to be associated with the condition. For example:

   4=2

5. Enter **s** to save the changes, then **q** to quit the screen.

Modifying a Condition

Only QoS conditions that were configured through the **qosac** command may be modified with the **qosmc** command.

To *modify* a QoS condition, enter the **qosmc** command with the desired QoS condition number. For example:

```
qosmr 1
```

The screen displays the parameters for the condition. Make changes to any of the parameters as described in *Adding a Condition* on page 5-18. Enter **s** to save your changes.

Deleting a Condition

Only QoS conditions that were configured through the **qosaa** command may be deleted with the **qosdc** command.

To *delete* a QoS condition, enter the **qosdc** command with the number of the condition that you want to delete. For example:

```
qosdc 1
```

The condition is deleted from the configuration.

Displaying QoS Conditions

A list may be displayed of all QoS conditions available on the switch. To display QoS conditions, enter the following command:

```
qossc
```

The screen displays similar to the following:

```
Cond      Actn     Prec     M     NumQ        Traffic Specifiers
 1 u       5 u       5      2        0
 L3:      198.206.184.0 (0xffffff00) ->          10.0.5.1 (0xffffffff)

 2 u       1 u       5      2        1
 L3       198.206.184.0 (0xffffff00) ->          10.0.3.1 (0xffffffff)
```

The fields are defined as follows:

Cond. The ID number of the condition and an indication of how the condition was received on the switch.

- **u** — configured through the QoS Manager UI
- **l** — pushed down from an LDAP-enabled directory server through Policy Manager
- **p** — received by a layer 2 policy request
- **r** — signaled via RSVP
- ***** — indicates that the condition contains traffic parameters not supported on the switch

Actn. The action ID associated with the condition.

Prec. The precedence level associated with the condition.

M. The level of precision stored in the HRE-X for the policy (destination address, destination and source address, source address only, etc).

NumQ. The number of active queues associated with this condition.

Traffic Specifiers. Indicates what kind of traffic the condition is configured for. **L3** indicates layer 3; **L2** indicates layer 2. For layer 3, the source and destination IP address, port, and net mask are also given. For layer 2, the source and destination MAC address, virtual port number, VLAN, and interface type are displayed.

Mapper Submenu

Statistics are available for viewing how the QoS Manager maps queues to physical and virtual ports. The QoS Mapper submenu is available from the QoS Manager menu. To display the submenu, enter the following command:

mapper

If the UI is configured for terse mode, enter a **?** to display the submenu. In verbose mode the submenu automatically displays.

```
Command          Mapper Menu
---------------  ---------------------------------------------
mapports         Display Mapper Ports
mapvports        Display Mapper Virtual Ports
mapactports      Display Only Active Mapper Ports
mapqueues        Display Mapper Queues
mapgroups        Display active mapper groups

    Main       File       Summary  VLAN       Networking
    Interface  Security   System   Services   Help
```

These commands are described in the following sections of this chapter.

Viewing Mapper Ports

To view all mapper ports, enter the following command:

mapports

All ports on which queues are set up (not just QoS ports) are displayed. The screen displays similar to the following:

```
Slot/                                                                    Queues
Port  VPN  QOS  MaxBW   AlcBW   CurBW  NumG  NumQ  NumVP  MTU   Req/Fail/Err
 1/1                0       0      0             0      3
      251           0       0      0     0       0         1500   0/  0/  0
      252           0       0      0     0       0         1500   0/  0/  0
      253           0       0      0     0       0         1500   0/  0/  0
 3/1               10.0M    0      0             0      1
        1          10.0M    0      0     0       0         1500   0/  0/  0
 3/2               10.0M    0      0             0      1
        2          10.0M    0      0     0       0         1500   0/  0/  0
 3/3               10.0M    0      0             0
        3     Y    2.05M   128K    0     0       0         1500   0/  0/  0
        4     Y    2.05M    0      0     0       0         1500   0/  0/  0
        5     Y    2.05M   128K    0     1       2         1500   6/  0   0
More? [<SP>, <CR>,/,F,N,Q,?]
```

Fields are defined as follows:

Slot/Port. The slot and physical port number associated with the virtual port.

VPN. The virtual port number.

QOS. Displays **Y** if QoS is available on the port (WAN ports only).

AlcBW. The amount of bandwidth allocated to the associated queue.

CurBW. The amount of bandwidth the flow is currently using.

NumG. The QoS group number (valid values are 0 or 1 for this release.)

NumQ. The queue ID.

NumVP. The virtual port number.

MTU. The Maximum Transmission Unit associated with the port.

Req Req/Fail/Err. Statistics for requested queues. **Req** is the number of queues requested. **Fail** is the number of queues that failed to be created due to insufficient resources, and **Err** is the number of those that failed due to some other unexpected error.

Viewing Mapper Virtual Ports

To view mapper virtual ports, enter the following command:

```
mapvports
```

The screen displays similar to the following:

```
VPN   Slot/Port     PhysBW      AlcBW
  1       3:1       10.0M          0
  2       3:2       10.0M          0
  3       3:3        2.05M      128K
  4       3:3        2.05M          0
  5       3:3        2.05M      128K

More? [<SP>, <CR>,/,F,N,Q,?]
```

Fields are defined as follows:

VPN. The virtual port number.

Slot/Port. The slot/port number associated with the VPN.

PhysBW. The amount of available bandwidth on the physical interface associated with the VPN.

AlcBW. The amount of bandwidth allocated to the virtual port.

Viewing Active Mapper Ports

To view only active mapper ports, enter the following command:

```
mapactports
```

The screen displays similar to the following:

```
Slot/                                          NumQ/                  Req
Port  VPN    PhysBW     AlcBW    CurBW    NumVP   MTU      Req/Fail/Err
5: 6         10.0M          0        0     0/ 1
        22                  0        0     0/ 1  1500     0/    0/    0
        27                  0        0     0/ 1  1500     0/    0/    0
```

Fields are defined as follows:

Slot/Port. The slot and physical port number associated with the virtual port.

VPN. The virtual port number.

PhysBW. The physical bandwidth available for the port based on the type of interface.

AlcBW. The amount of bandwidth allocated to the associated queue.

CurBW. The amount of bandwidth the flow is currently using.

NumQ/NumVP. The queue ID and the virtual port number.

MTU. The Maximum Transmission Unit associated with the port.

Req Req/Fail/Err. Statistics for requested queues. **Req** is the number of queues requested. **Fail** is the number of queues that failed to be created due to insufficient resources, and **Err** is the number of those that failed due to some other unexpected error.

Viewing Mapper Queues

To view mapper queues, enter the following command:

```
mapqueues
```

The screen displays similar to the following:

QID	S/P	VPN	Grp	Actn	NmC	NmM	P	MinBw	MaxBW	CurBW	Ave/Max	Depth
0x032303	4/ 2	35	1	1	1	1	0-	512K	768K	0	0/ 1	80000
0x032300	4/ 2	35	1	5	1	1	1-	512K	2.05M	0	0/1	65535
0x032302	4/ 2	35	1	5	1	1	1-	512K	2.05M	0	0/ 0	65535
0x032301	4/ 2	35	1	-	0	0	3b	0	2.05M	216	0/ 1	0

The fields are defined as follows:

QID. The queue ID.

S/P. The slot and physical port associated with the queue.

VPN. The virtual port number associated with the queue.

Grp. The QoS group number.

Actn. The ID of the action associated with the queue.

NmC. The number of conditions associated with the queue. Multiple conditions may be associated with the queue if the conditions have actions that are configured for sharing queues.

NmM. The number of MAC addresses associated with the queue.

P. The priority associated with the queue, ranging from 0 (highest priority) to 3 (lowest priority). This field also indicates the type of priority queue as follows: **f** for flood queue, **d** for default queue, and **b** for best effort queue. These queues are displayed for comparison with QoS queues. Flood queues service broadcast traffic; default queues are used for undirected frames (frames for which a destination address is not known). Best effort queues are associated with flows that are not QoS flows, that is, flows for which there is no associated policy to be applied.

MinBw. The minimum bandwidth requirement for this queue (the bandwidth allowed by the lowest minimum configured for all actions associated with the queue).

MaxBw. The maximum bandwidth allowed for the queue (the bandwidth allowed by the maximum configured for all actions associated with this queue).

CurBW. The current bandwidth used by the queue.

Ave/Max. The average number of buffers used by the queue, divided by the maximum buffers used for the queue.

Depth. The maximum queue depth allowed by all actions configured for this queue.

Viewing Mapper Groups

To display a list of all QoS groups and queue information for those groups, enter the following command:

mapgroups

The screen display is similar to the following:

Id	VPN	MinBW	MaxBw	AlcBW	CurBW	NumQ/MaxQ	Buf/MBuf
1	35	0	1.54M	128K	0	2/ 0	0/128

The fields are defined as follows:

Id. The number assigned by the switch to the QoS resource group. A resource group is a group of different flows (with different conditions) assigned to the same action.

VPN. The virtual port number.

MinBW. The minimum bandwidth configured for the group. Minimum bandwidth is configured in the action of the policy through the **qosaa** command or through the PolicyView application.

MaxBW. The maximum bandwidth configured for the group. Maximum bandwidth is configured in the action of the policy through the **qosaa** command or through the PolicyView application.

AlcBW. The bandwidth that has been allocated for the QoS group.

CurBW. The bandwidth that is currently being used by the QoS group.

NumQ/MaxQ. The number of queues currently set up for the QoS group, and the maximum number of queues the physical port supports. For example, WSM ports support a maximum of 128 queues.

Buf/MBuf. The number of buffers currently used by the QoS group, and the maximum number of buffers available on the port. For example, WSM ports support a maximum of 128 buffers.