6 Policy Manager

Introduction

This chapter describes the quality of service (QoS) functions of the Policy Manager, a software module that brings policy-based traffic control features to the OmniSwitch, OmniS/R and the Omnistack. The Policy Manager, which works in conjunction with Alcatel's QoS Manager, permits maximum use of available network resources via QoS bandwidth management, and can be used in lieu of increasing capacity to improve network performance. Specifically, the Policy Manager informs the QoS Manager how to treat flows of traffic, based on predetermined flow requirements set through policies, so that quality of service is not compromised or degraded in the switch.

Setup and configuration instructions for implementing the Policy Manager are provided in this chapter, followed by the required User Interface (UI) settings for the switch. See *User Interface (UI) Commands* on page 6-18.

Policy Manager General Description

The Policy Manager dynamically assigns static network policies to flows of traffic in the switch, manages the relationships between the policies, and maintains policy flow states. Information contained in the policies define the traffic flow parameters for various classes of users and applications, enabling the Policy Manager to decide which "traffic rules" to apply.

The Policy Manager utilizes the Java-based X-WebVision application called PolicyView to provide control over QoS policies from a workstation in the network. PolicyView configures policies, prioritizes traffic, and defines RSVP and traffic profiles for the network. See *PolicyView* on page 6-16 for more information about PolicyView.

Specific traffic flows that can be assigned policies by the Policy Manager include Provisioned and RSVP (Resource Reservation Protocol). Provisioned QoS Policies define priority and bandwidth for traffic, while RSVP policies set limits on the amount of bandwidth that can be reserved for traffic. RSVP is sometimes referred to as a native QoS signaling protocol and policy transaction protocol.

Currently available interfaces used by the Policy Manager to handle traffic flow transmissions include Frame Relay and PPP (Point to Point protocol), which function specifically on Alcatel switches containing either OSWSM, WSM3 or WSX modules.

Policies are stored on directory servers and accessed by the Policy Manager using Version 3 of the repository access protocol, LDAP (Lightweight Directory Access Protocol), which uses TCP/IP as its transport protocol. The rules used by the Policy Manager to provide QoS for traffic flows are stored on an LDAP-enabled directory server and read in when the switch is initialized. As a prerequisite to this chapter, especially for details on directory servers and LDAP, see Chapter 8, "IP Control."

Relationship between the QoS Manager and the Policy Manager

QoS through the switch can be improved with bandwidth transmission management by designating how network traffic can flow most efficiently with current network resources. Usually, when all available bandwidth is used QoS is reduced, yet proper manipulation of traffic flows using the Policy Manager can further sustain QoS.

Policy-based management is necessary to efficiently configure, control and monitor the thousands of traffic flows occurring regularly in a network. The Policy Manager is particularly suited to this function due to its ability to handle assorted traffic using policies, and is

extremely useful in converged networks which must simultaneously accommodate data, voice and multimedia traffic.

Furthermore, use of the LDAP client in the switch allows switching and traffic information for quality of service as a whole to be integrated into unified directories of user information stored on one or more directory servers.

The QoS Manager, which consists mostly of software modules, uses policies to activate, administer, deliver, monitor and control the quality of service for enterprise network traffic. It maps and queues flows in addition to enforcing policies for the Policy Manager.

Policies and QoS

Policies are rules that modify how traffic flows through the switch. The intended action of the traffic most often determines what QoS is assigned by a policy.

Policy rules are represented in the form of if <condition> then <action>, meaning when the condition is satisfied, the action is implemented.

Since policies reflect business decisions and define how resources are to be allocated to satisfy the decisions, they necessarily involve considerable forethought before being implemented to enhance network services; however, network capacity planning and provisioning are beyond the scope of this chapter.

Policy Manager Operations

The Policy Manager interprets policies assigned to a switch and decides which policies should be implemented to 1) guarantee switch traffic passing through the QoS Manager is mapped and continuously adheres to traffic flow requirements, and 2) the traffic is classified, queued, and scheduled by the QoS Manager for delivery to its destination according to its predetermined traffic needs and assigned policy.

The Policy Manager software module is central to all QoS operations in the switch. Other software modules contained within the QoS Manager work in conjunction with the Policy Manager to provide QoS through the switch. These include the Mapper and the Classifier, both of which are subordinate to the Quality of Service Manager and the Policy Manager.

The Classifier is responsible for analyzing incoming traffic flows by comparing them to policy rules set through the Policy Manager to identify the flows for the QoS Manager. The Mapper manages QoS requests from networked hosts and the hardware required to implement the requests. Aspects of these other modules are discussed in this chapter, but only as they directly relate to the Policy Manager. For more information on the other modules, see Chapter 5, "QoS Manager."

Another name for the Policy Manager is Policy Decision Point (PDP) as it is the point where QoS policy decisions concerning network traffic flowing through the switch are made.

How the Policy Manager Works with the QoS Manager

When the switch is initialized the Policy Manager executes on the **policy.img** file, at which time it receives its configuration data stored on the switch. The Policy Manager then reads in the policy rules set through PolicyView.

Applicable Layer 3 rules are pushed to the QoS Manager when the Policy Manager is initialized, although only one rule is applied to a traffic flow at any given time. Currently, acceptable Layer 3 rules use header information such as IP address and port; Layer 2 rules use MAC addresses.

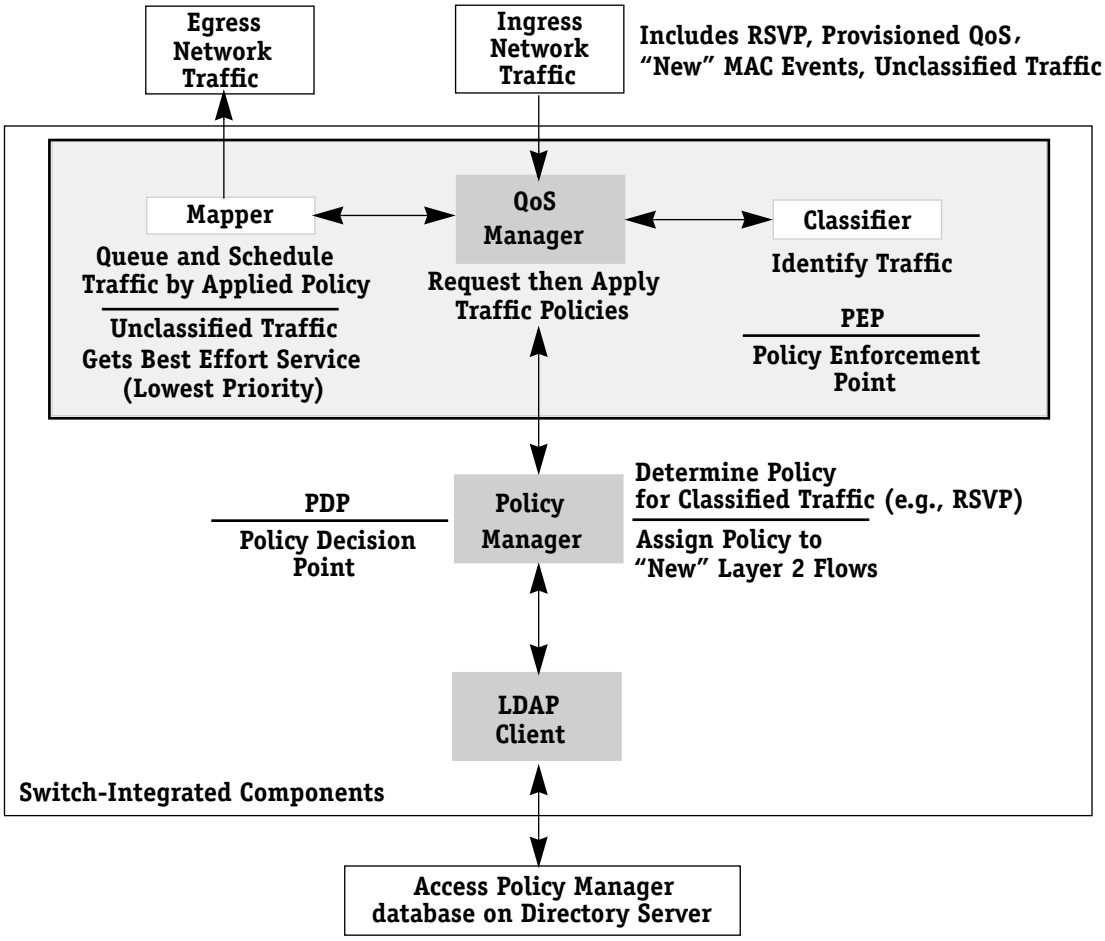
Note

For the QoS Manager to classify Layer 3 traffic, routing must be enabled, and an HRE-X must be installed on the switch. See Chapter 5, "QoS Manager" for details.

In addition, whenever the QoS Manager receives notification of "*new*" MAC events in reference to new or unknown hosts and protocols, the information is forwarded to the Policy Manager to determine which traffic rules apply. The Policy Manager, in turn, looks through its configured policies for a matching rule, then sends an answer back to the QoS Manager stipulating how the traffic should be handled.

If there is no policy rule on the WAN interface to assign QoS to the traffic, then the traffic is implicitly treated as best effort traffic. Policy-defined QoS is applied to the traffic on egress from the switch on WAN interface modules.

Unsolicited policy responses are asynchronously issued by the Policy Manager to the QoS Manager when policy state information changes. When an RSVP flow is terminated, the QoS Manager informs the Policy Manager. The Policy Manager applies policy information via requests from the QoS Manager as shown in this flow diagram.



Traffic Flow Diagram for QoS using Policies

Policy Manager Decisions

Policy decisions made by the Policy Manager in Alcatel switches can be based on one or more of the following traffic conditions:

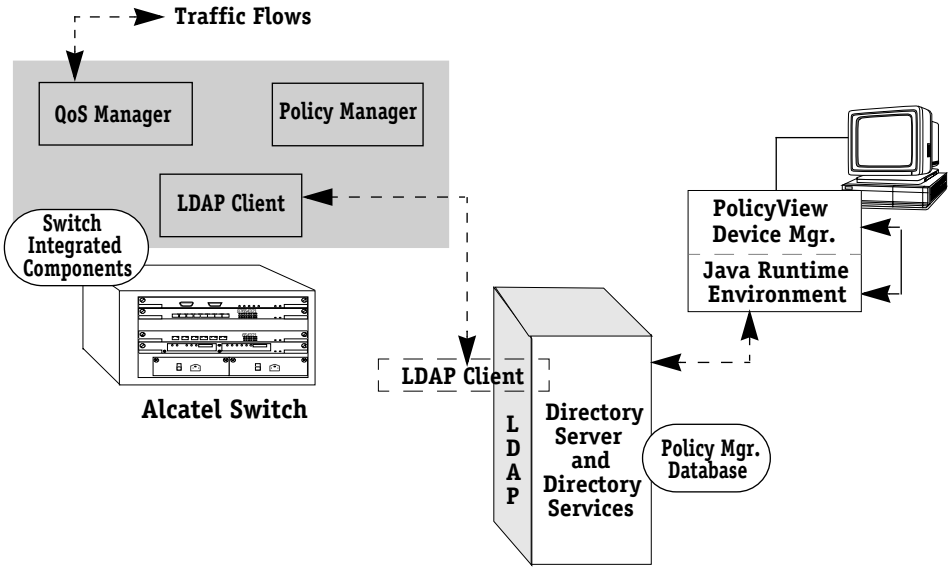
- Media Access Control (MAC) addresses
- Internet Protocol (IP) addresses
- TCP port
- Virtual LAN (VLAN) group membership
- Time of day, week, and month

Switch traffic requesting or being assigned QoS is directed through the network based on rules set in the Policy Manager using PolicyView. The conditions specified in the traffic patterns must be satisfied in order for the policies to be valid. Updates to the rules are implemented through PolicyView. See *PolicyView* on page 6-16 for more information about PolicyView.

In summary, the Policy Manager derives its policy decisions from policy rules set through PolicyView, static policy data stored in directory servers, and extrinsic data gathered from traffic flows.

Note

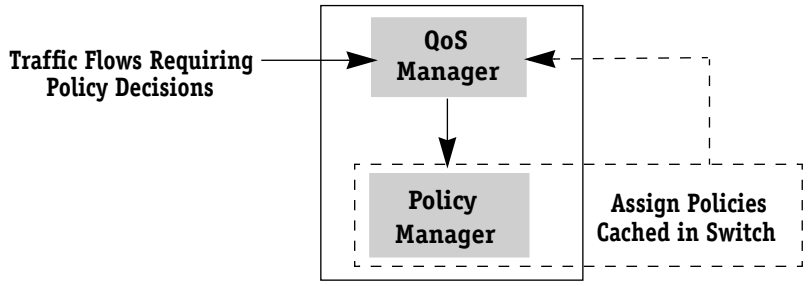
Descriptions of Alcatel's Policy Manager were derived in accordance with IETF draft, Terminology for Describing Network Policy and Services, dated Feb. 26, 1999.



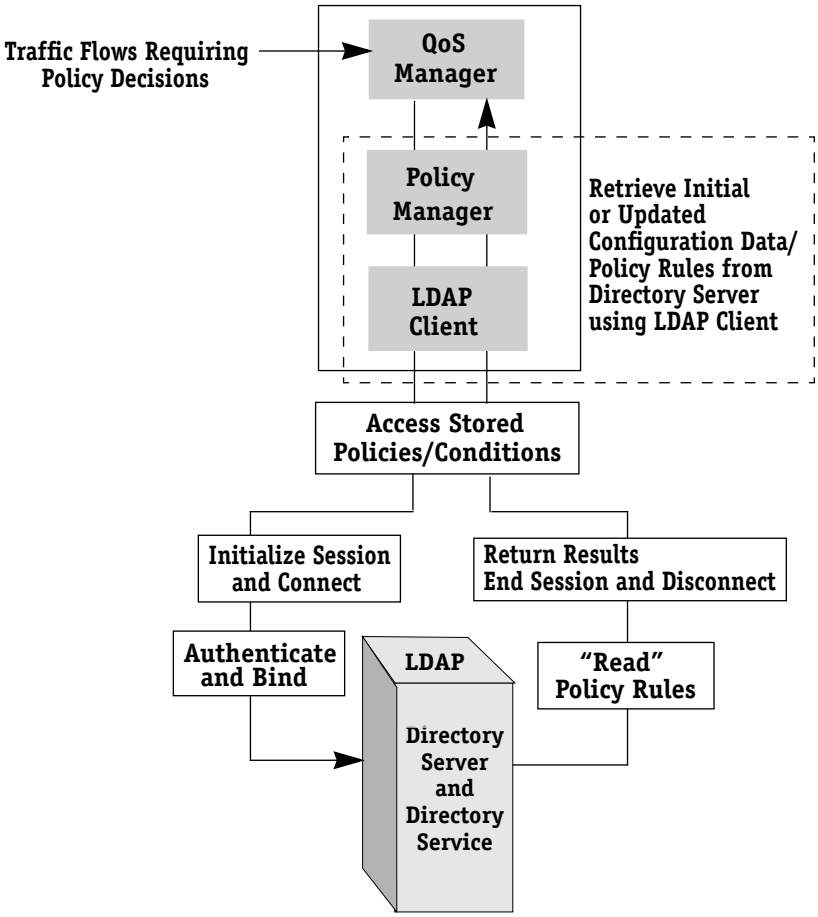
How PolicyView Works with the Policy Manager

Policy Manager QoS Operations with LDAP

The Policy Manager and the QoS Manager in the switch provide the policy decision and enforcement functions of the PDP/PEP for all traffic classified to receive QoS treatment based on policy. The QoS Manager uses policy information from the Policy Manager to assign proper priority and bandwidth allocations to the traffic. When policies are updated using PolicyView, or the switch is rebooted, the Policy Manager retrieves policy data anew from the directory server, flushes the existing cache, and updates the QoS Manager as needed.



Policy Manager QoS Operations using Cached Policies



Policy Manager QoS Operations after Startup or Database Update

Traffic Flows and Policy Messages

Traffic is classified for QoS treatment using one of the following: RSVP, provisioned assignments using Layer 2, or provisioned assignments using Layer 3. QoS traffic flows with policy messages supported by the Policy Manager include RSVP (Resource Reservation Protocol) and Provisioned QoS.

When the QoS Manager receives bandwidth requests via RSVP signaling, it forwards the requests to the Policy Manager which determines if the reservation should be accepted based on policy defined limits.

The transfer of information and manipulation of QoS using policy control parameters by the Policy Manager is normally transparent to users. For example, error messages would only be issued to devices requesting RSVP when policy approval was not obtained, in which case no resources could be reserved. A brief description of how the Policy Manager deals with RSVP messages is provided below. See Chapter 7, "RSVP" for an in-depth discussion.

RSVP Policy Messages for QoS Bandwidth Reservations

RSVP policy messages refer to the flow of information between the QoS Manager and the Policy Manager to support RSVP, including the contents defined in the RSVP message. RSVP reservations are one way requests issued in advance from authorized hosts to receive a particular QoS bandwidth for real-time traffic streams from audio or video applications. RSVP actions normally define limits on the amount of bandwidth that can be reserved. These limits (in kilobits per second or percentage of link) are ultimately communicated to the switch-enabled Policy Manager and enforced by the QoS Manager. RSVP allows applications to reserve bandwidth where most network congestion occurs — across WANs.

RSVP Components

The basic components of RSVP are traffic senders and receivers, e.g., end station hosts with the Policy Manager and the switch in-between. Senders inform receivers when they have data to send and the QoS needed via "*path messages*". Receivers are responsible for making the reservations via RESV messages to obtain the QoS, and for maintaining the resource reservations used for the flows.

RSVP traffic flows, or "*flowspecs*", travel from a "*sender*" to one or more "*receivers*". Prior to sending flows, senders transmit "*path messages*" to receivers. The RSVP messages contain source and destination IP addresses, including the flowspec consisting of numerical rate and delay bounds, and the quality of service required by the flow. These path messages are routed to receivers by hosts and routers along the flow paths (administratively significant sets of flows that traverse path segments).

RSVP and the Policy Manager

When the QoS Manager receives RSVP reservation messages, the QoS Manager sends a policy request message to the Policy Manager. The Policy Manager returns an *"accept"* or *"deny"* decision. The Policy Manager uses information held in the directory server to check maximum limits on reservations, and in deciding whether or not to deny or accept them. Parameters for reservations are set using PolicyView. The QoS Manager terminates signaled RSVP requests that are rejected by the Policy Manager.

RSVP reservation messages are used by the Policy Manager to allow, deny or assign priority based on one or more of the following:

- group membership by IP address
- ingress and egress subnet or switch interface
- time of day and week
- requested vs. set bandwidth limits
- type of RSVP service such as controlled load and guaranteed

RSVP Policy Controls

Limitations can be set for RSVP QoS policies (using PolicyView) to determine whether or not a reservation should be accepted as follows:

- type of RSVP service such as RSVP controlled load
- allow or deny all reservations from a particular address or subnet
- maximum token rate per flow
- maximum token bucket size per flow
- minimum delay per flow
- maximum flow duration
- user authentication policy such as simple or kerberos

Provisioned Notifications

Provisioned policy notifications refer to traffic flows between the QoS Manager and the Policy Manager to support Provisioned QoS. The Policy Manager assigns Provisioned QoS to traffic based on policy rules that define actions to be taken on traffic meeting the conditions of the rules.

Provisioned QoS differs from RSVP QoS in that no explicit client-driven "*reservations*" are used. Provisioned QoS assigns priority and bandwidth to particular types of traffic. For more information on available queuing methods used to provide quality of service, refer to Chapter 5, "QoS Manager."

Provisioned QoS assigns priority and bandwidth (traffic shaping) to provisioned traffic flows.

The Policy Manager uses one or more of the following parameters to classify traffic for QoS support:

- Group ID (as provided by source learning)
- Time of day, week, and month
- Interface type on which frame was received
- MAC address
- IP address
- TCP port

Provisioned Policy Controls

Limitations can be set for Provisioned QoS policies (using PolicyView) to assign traffic priority and guarantees as follows:

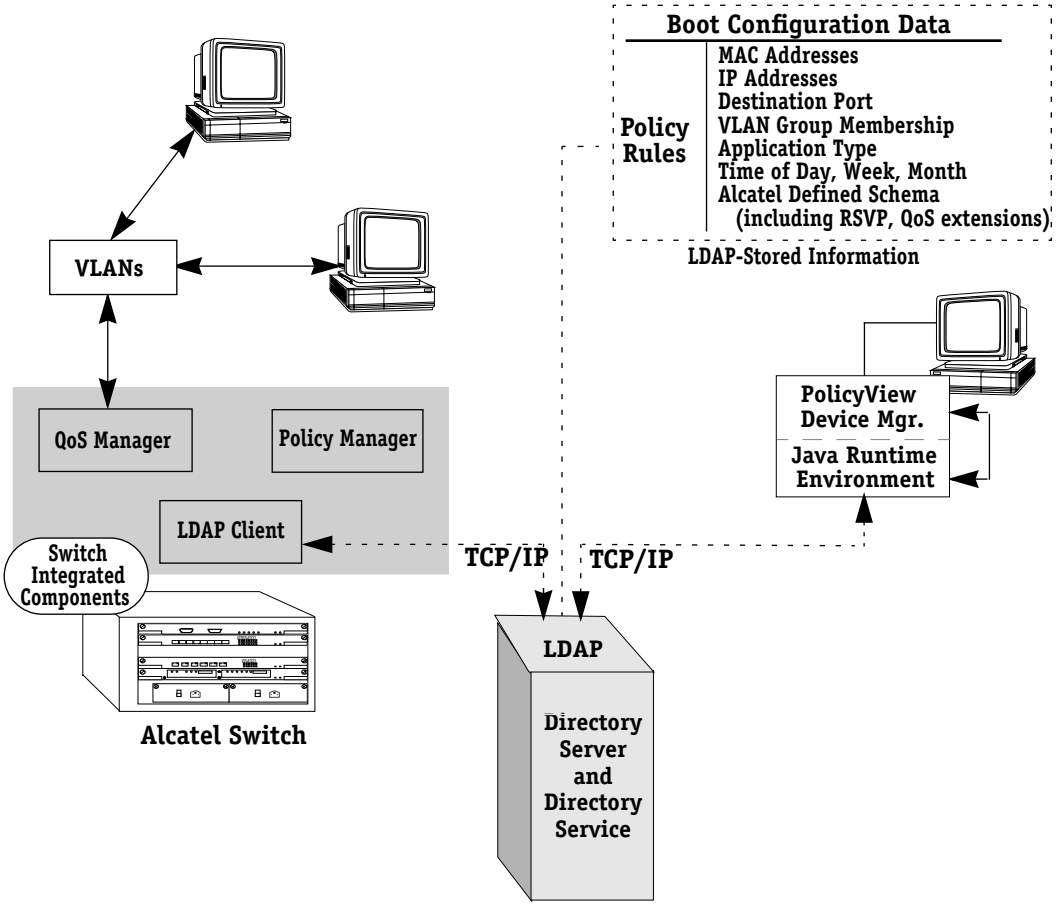
- priority level
- minimum output rate
- peak output rate
- 802.1p priority level (available in a future release)
- queue depth
- maximum latency

Components of the QoS Policy Manager

The QoS Policy Manager requires the following Alcatel and third–party components. Operations between the components are depicted on the next page.

Policy Manager Components

Components	Description
QoS Policy Manager Components	**•QoS Policy Manager** The Policy Manager is part of the dynamically loadable Policy Manager software module (policy.img). The Policy Manager is a module that must be used with Alcatel's QoS Manager. As a result, QoS operations of the Policy Manager are contingent upon the hardware requirements of the QoS Manager (for details see Chapter 5, "QoS Manager." **• PolicyView NMS Management Application/Java Runtime Environment (JRE)** This program is supported on Solaris (UNIX) and Windows NT 4.0. Java is an object-oriented programming language developed by Sun Microsystems, that is typically used to create Java applications which are executable from within a web browser. Java Runtime Environment 1.1 must also be installed on the workstation in order to deploy PolicyView.
Third–party Components	**•LDAP–enabled Directory Server** *(primary and secondary servers recommended)* Servers must be networked, fully operational, and have necessary schema extensions installed before using the Policy Manager. Note: The Policy Manager must be able to contact LDAP-enabled directory servers using Alcatel's LDAP client, or it will not operate.



How Policy Manager Components Work Together

Policy Manager Component Setup

Components required to implement the Policy Manager as described above, must be set up and configured in addition to setting the UI commands for the Policy Manager, the QoS Manager, to enable LDAP operations through the switch (see *User Interface (UI) Commands* on page 6-18 for more information).

The Policy Manager image file (**policy.img**) is included on the CD that contains the base switch software in the directory xxx-Policy Management (xxx=OSTK, MPM or MPX . . . depending on the switch in use, e.g., Omnistack=OSTK).

Policy Manager Installation

The following instructions address the minimum installation requirements to render the Policy Manager operational in most configurations, **and are geared toward setting up the switch to use PolicyView on an NT 4.0 workstation using Netscape directory server 4.0 or an NT 4.0 server, as an example**. Please note that this does not imply in any way an endorsement of Netscape's directory server, or Windows NT.

These instructions should be modified accordingly to match the server operating system and directory server being used to support the Policy Manager and PolicyView, and should be performed in the order presented.

- Configure the switch for the Policy Manager, LDAP operations, and set the switch time.
- Install the directory server on the PC running NT 4.0 server.
- Install the Java Runtime Engine (1.1) and PolicyView on the machine running NT 4.0
- Copy the contents of Alcatel's schema extension (.conf) files to the directory server (may be on the CD or possibly downloadable from Alcatel.
- Copy the Policy Manager database file (.ldif) to the directory server, then modify and import the file to the directory server. (may be on the CD or possibly downloadable from Alcatel.)
- Configure the Policy Manager using PolicyView.
- Confirm that the **qos.img** file for the QoS Manager is installed on the switch, and that the Qos Manager is properly configured (see Chapter 5, "QoS Manager," for details).

Configure the Switch for the Policy Manager, LDAP Operations, and Set the Switch Time

1. Confirm the **policy.img** file for the Policy Manager is on the switch. If not, copy the file from the switch software CD to the switch.
2. Set the *User Interface (UI) Commands* on page 6-18 (as described) to 1) enable the Policy Manager and LDAP operations through the switch, 2) configure the Policy Manager switch operations, and 3) set the time in the switch to coincide with the Policy Manager/Policy-View.

   Switch settings must be entered in addition to enabling LDAP operations for the Policy Manager in PolicyView as described in the proceeding instructions.

Note

Some settings between the switch, the directory server, and PolicyView must match in order for the Policy Manager to work. Keep the settings readily available for reference purposes as each component of the Policy Manager is installed.

Install the Directory Server

1. Set up an NT 4.0 server (NTFS partition) with at least Service Pack 3 using the vendor-supplied instructions.

2. Load the Netcape Directory server 4.0 software (for LDAP operations) onto the NT server, and then create the directory server using the vendor-supplied instructions (version 4.0 recommended). During the installation, take special consideration of the following:

   - The same port number, e.g., **389** (the default for TCP/IP LDAP), must be used in the switch UI (item 4 in the **ldapcfg** menu) and for the directory server.
   - The same password (recommended), e.g., secret 88, should be used in the switch UI (item 5 in the **ldapcfg** menu), for the directory server, IP Control web management application, and the associated **ldapcfg** file in use.
   - The same bind name, e.g., **cn=manager**, must be used in the switch UI (item 6 in the **ldapcfg** menu) and for the directory server.
   - The same base suffix, .e.g, **o=Alcatel**, must be used in the switch UI (item 8 in the **ldapcfg** menu) and for the directory server.

Note

Important! Do not use the default setting "enabled" for Schema Checking when installing the directory server. The Schema Checking setting must be changed to "disabled."

Install the Java Runtime Environment (JRE 1.1) and PolicyView

1. Set up a machine with NT 4.0 and at least Service Pack 3 (general guidelines above).

2. Download and install the JRE from Sun Microsystems at http://www.javasoft.com/products/jdk/1.1/jre/index.html.

3. Load Alcatel's PolicyView onto the NT 4.0 machine. Before installing it, review the Install notes supplied with PolicyView.

4. To start PolicyView, click Start/Programs/Alcatel PolicyView. The PolicyView application will load and prompt for a user ID and password. The default user ID is *"admin"* and the default password is *"switch"*. It is recommended that this default password be changed.

Copy Alcatel's Schema Extension (.conf) Files to the Directory Server

Extend the directory server schema on the directory server as follows:

Copy the contents of Alcatel's object class and attribute schema extension configuration (**.conf**) files to the directory server directory (or folder) ***netscape/server4/slapd-server (name identifier)/config*** to replace the same files installed by the directory server:

Object class configuration file: **slapd_user_oc.conf**

Attribute configuration file: **slapd_user_at.conf**

Note

Do not replace the LDAP configuration files currently residing on the directory server if the files have been modified and need to be retained in that form. Instead, using a text editor, cut and paste Alcatel's **.conf** files and add them into the existing files.

Alcatel's object class and attribute configuration files are crucial to the operation of the Policy Manager, and are used either to replace or modify the existing configuration files on the directory server.

Copy and Modify IP Control Database File (Xylan.ldif) to the Directory Server

Copy and then modify the **Xylan.ldif** database file containing the Policy Manager database information to the directory server as follows:

1. Copy the **Xylan.ldif** file to the directory server directory (or folder) ***netscape/server4/slapd-server (name identifier)/ldif*** to replace the same files installed by the directory server, and then modify the file on the server as follows:
   - Using a text editor, modify the **xylan.ldif** file to meet your business needs, making certain that information such as the search base is changed from **o=Alcatel, c=US,** to something that applies to your organization. (These values must be changed to the values entered for the base suffix when the directory server was created.)
   - Save the modified file on the directory server using the same name.
2. Start or restart the directory server.

Configure Policies with PolicyView

The Policy Manager and the polices or rules controlled by the Policy Manager must be set up and configured using PolicyView. This should be done once the following tasks have been completed:

- The QoS Manager **(qos.img)** on the switch is enabled.
- The directory server is installed on either an NT 4.0 (with at least service pack 3) or other machine. All the necessary schema files contain the correct information and are on the directory server.
- The JRE 1.1 and PolicyView are installed on another machine and communicating with the directory server.
- The switch time is configured.
- The UI commands are set for the Policy Manager and LDAP operations.

The Policy Manager setup procedures are performed through the menus in PolicyView. For a general guideline as to the use and contents of these options, especially for setup purposes, see the PolicyView description on Page 6-15.

1. Start PolicyView by clicking Alcatel PolicyView under Start/Programs.
2. Click the Wizard button for instructions on setting up the Policy Manager policies using PolicyView, or scroll through the online help file to locate the setup instructions.
   - As a minimum for operating the Policy Manager, this will require defining at least one policy in PolicyView as described in the online instructions.
   - Begin by selecting Applications from the main menu, and then selecting PolicyView and QoS Policies. Refer to the content-specific online help for valid policy settings.

Note

Be sure to select the service and then select Update and Apply Policies from the main menu after all of the required settings for PolicyView have been entered, and every time thereafter when *any* changes to the service or policies are made for the changes to take effect.

PolicyView

PolicyView is a Java-based application used to configure certain components of the Policy Manager for QoS, to set up policies, and to monitor operations of the Policy Manager. PolicyView is part of Alcatel's integrated network management suite that allows organizations to easily manage their entire campus, enterprise or local area switched networks.

From a single management console, X-WebVision allows administrators to implement network-wide policies to minimize overall network administration. On the same console, administrators can easily track network usage, performance, and manage all available interface types for the Policy Manager (currently only Frame Relay is available). PolicyView provides a graphical user interface to Alcatel's Policy Manager functions.

Policies are defined using PolicyView and are enforced by the switch in the order specified during switch assignment. One of the most notable time-saving features of PolicyView is its ability to add policies to multiple switches at one time.

The screens provide a logical view of policy profiles and make them easier to manage. Two basic steps are involved in the creation of one or more QoS service classes and the creation of one or more profile classes. The Profile class defines the traffic (by VLAN ID, IP address, port numbers, resource group, MAC address, and Policy Validation Period), and the QoS service that should be applied to the traffic. The QoS service classes and the profile classes are stored in the directory server.

PolicyView is used to discover QoS-capable switches on the network, to assign policies to the switch, to enable QoS services, and to assign LDAP-enabled directory servers to hold policies for the switch. It is also used along with the UI commands (described on page 19) to define LDAP-enabled directory servers.

PolicyView Menus

The following information is a general guideline concerning the use and contents of the options contained in PolicyView to peruse before actual use of the application. It it *not* intended to replace the online help included with PolicyView which provides detailed operational parameters and instructions.

The PolicyView menu options are mainly used to identify, define, and view operational parameters for the policies, and to enable operations with LDAP-enabled directory servers. *Please note that currently there is no Undo command.*

Using PolicyView to Create and Assign Policies

Network/Switches — Use this option to add or auto-discover the QoS-capable switches that will be included in PolicyView. A list of available switches is provided to show assigned policies.

Network/Switches/IP Address of Switch — Use this option to view policies assigned to the switch along with the list of assigned primary/secondary LDAP servers. Four LDAP servers can connect to one QoS switch.

Network/Switches/IP Address — Use this option to determine the order of policy precedence set for a list of policies in a selected switch. The switch processes policies rules in the order defined in this list; once it finds a matching rule, it takes the action defined in that rule and does not process any other rules for that match.

Switches/LDAP Servers — Use this option to assign the LDAP-enabled directory servers assigned to a selected switch, and to select the primary directory server.

Network/LDAP Servers — Use this option to define LDAP-enabled directory servers.

QoS Services/Policies — Use this option to create or view a policy. This screen allows network managers to define a QoS policy based on a selected condition and desired action. A policy consists of a condition and an action. If the condition is satisfied, then the policy manager in the switch takes the specified action. The condition defines the traffic profile and policy validity period for applying the action. The type of action being applied defines the policy type. The Policy Manager currently supports RSVP and Provisioned QoS actions.

The Policy Table contains policies associated with the switch and contains the following:

- Policy Names
- Policy Type (PROV QoS or RSVP QoS).
- Policy Action Status
- Condition name associated with each policy.
- Action name associated with each policy.

QoS Services/Policy subfolders (Conditions, Actions, Policy Validity Periods, Resource Groups, Groups) — Use these options to view or modify policies assigned to the switch.

/Policies/Condition — Use this option to define the traffic profile (e.g., MAC address and/or IP address), interface type, group (VLAN), and policy validity periods that must be satisfied by the traffic before the associated action defined by the policy rule is taken.

If a condition consists of multiple attributes, the traffic pattern must match all of the attributes in order for the condition to be true. A list of associated policies is also displayed. The list of groups/VLANs that have been defined in the network is provided by the X-WebVision framework. Makes a new instance of a condition.

/Policies/Action — Use this option to create a Provisioned QoS action to be taken on traffic that meets the condition of the rule. The priority level, min. output rate, peak output rate, 802.1.p bits, queue depth, and maximum latency are attributes used to effectively manage bandwidth. This option is also used for RSVP QoS to define the action to be taken on RSVP reservation requests (e.g., set limits on the size, number and total bandwidth that can be allocated to network applications using RSVP.)

/Policies/Policy Validity Periods — Use this option to set times when policies are valid. All policy validity periods are enforced using the time configured on the switch.

/Policies/Resource Groups — Use this option to create a resource group used in the QoS Policy Condition screen. The Resource Group screen provides additional aggregate limits on RSVP reservations.

/Policies/Groups — Use this option to create or view a switch VLAN obtained from a list of groups defined in a network. This information is obtained from within the X-WebVision framework, or the ID of the VLAN group can be entered directly.

User Interface (UI) Commands

The following UI commands must be set through the switch to enable Policy Manager QoS operations:

- LDAP Configuration (for SNS LDAP-enabled server that stores policies)
- Policy Configuration (for Administering SNS Policies)
- Switch Time Configuration (for synchronizing switch time with Policy Manager/PolicyView). Please refer to the chapter "Configuring Switch-Wide Parameters" in the switch manual for information on time configuration using the **System** menu, including commands and valid parameters for the time zone, offset, and DST.

In addition to the UI commands, other components of the Policy Manager must also be set up and configured. *Components of the QoS Policy Manager* on page 6-10.

LDAP Configuration

The switch UI interface for LDAP is used to load and flush cached policies as needed, view LDAP policy statistics, and to specify and configure primary and secondary directory servers. A single, primary LDAP-enabled directory server can be assigned to each QoS-capable switch. Multiple secondary directory servers can be assigned for backup purposes.

User Interface commands for configuring LDAP to work with the Policy Manager are located in the Networking/LDAP and Networking/Policy configuration submenus.

LDAP Submenu

The LDAP submenu can be accessed by typing **ldap** in the command line. Available **ldap** submenu commands are shown here and defined below.

Command	LDAP Sub-Menu
ldapshow	Show LDAP server definitions
ldapcfg	Add/Modify an LDAP server definition
ldapdel	Delete an LDAP server definition
ldapflush	Flush all cached LDAP data from switch
ldapload	Reload all cached LDAP data from server
ldapcache	Show LDAP policy cache on switch
ldapstats	Show LDAP policy statistics

Displaying a List of Defined LDAP-enabled Servers

To display a list of defined LDAP-enabled servers, enter the following command:

```
ldapshow
```

A screen displays similar to the following.

```
ldapshow command

ServerIP Addr    port    enabled oper    pref    last change       auth type
================================ ====  ====  ======================
1222.22.22.2     389     Yes     Up      150     99/06/10 13:21:07N QoS
2172.33.33.3     399     Yes     Up      151     99/06/11 03:01:287N QoS
```

Each row of entries applies to one server. Servers are defined using the **ldapcfg** command below.

With an Authentication entry of **Yes**, the following kind of UI output should display:

```
ServerIP Addr    port     enabled oper   pref     last change       auth type
============================== ====  ====   ======================
1172.19.33.4     399      Yes     Up     150      00/02/15 09:38:31Y QoS
 authentication: Password, authDN = 'cn=directory manager'
2172.19.33.10    330      Yes     Up     0        00/02/11 14:15:117Y QoS
 authentication: Password, authDN = 'cn=directory manager'
```

The following describes the fields/messages in more detail:

Server
Number one position indicates first LDAP-enabled server in the list. Up to four servers can be used.

IP Addr
Indicates the IP address for LDAP-enabled server.

port
Indicates TCP/IP port number used for communications with LDAP-enabled server; **389** is the default port number, but other numbers can be used.

enabled
Yes indicates server is enabled; **No** indicates server is disabled.

oper
Up indicates server is functioning; **Down** indicates server is not functioning.

preference
Number indicates which directory server is to be accessed first (**0**=low; **255**=high. Numbers can be assigned arbitrarily.

last change
Indicates date and time server was last updated.

auth type
Indicates authentication required, e.g., **No QoS** means authentication for QoS not required.

Displaying and Modifying a List of Parameters for LDAP-enabled Servers

To display and modify a list of parameters for LDAP-enabled servers used with the Policy Manager, enter the following command:

ldapcfg

A server configuration screen for LDAP displays. Items 1 through 8 must match configuration information entered for LDAP and Policy Manager through PolicyView.

Enter the number in the command line and the appropriate values to add or modify LDAP server definitions, e.g., **1=yes, 2=222.22.22.2,** etc. Values such as the following are output from the switch:

LDAP Server Configuration

1. **LDAP Server enabled:Yes**
2. **LDAP Server IP Address:222.22.22.2**
3. **LDAP Server IP Port:389**
4. **Server Preference:0**
5. **Authentication:Simple Password**
6. **User ID:cn=Directory Manager**
7. **Password:secret88**
8. **Searchbase:ou=QOS, o=Alcatel, c=US**

Note

At initial configuration of these UI commands, item 1 will be set to **No**; items 2 through 8 will be set to **Unset**.

The **ldapcfg** command may be entered so that it specifies a directory server number to replicate settings between the servers (e.g, **ldapcfg 1**, or **ldapcfg 2**, etc.) Only settings which must differ between the servers, such as the IP address, will then need to be changed. If no server configuration exists for the server number specified, default settings will display.

The following information is available in more detail from the switch help commands for the **ldapcfg** menu:

LDAP Server enabled

Enables LDAP server. The default is **No**. When LDAP Server is set to **No**, the Policy Manager will not use LDAP server selection processing.

LDAP Server IP address

IP Address of primary LDAP-enabled directory server.

LDAP Server IP Port

TCP/IP Port number used by Policy Manager to connect to the Primary LDAP-enabled server. Default port number is **389**, but server may use other port as defined when directory server was created. (The default SSL port number is **636**, although this is not yet supported by Alcatel's LDAP client).

Server Preference

Enables directory server by arbitrary, but user-defined preference number. Valid preference number range: **0**-**255** (**0**=low, **255**=high).

Authentication

When the Authentication field is set to **none**, the User ID and Password are not used; LDAP queries are performed using the anonymous query method. The default is **none**.

User ID

Username used for accessing the Policy Manager database entries on the directory server. This name must be preceded by **cn=**. The Username is the directory manager name defined when the directory server is created.

When the Authentication field is set to **none**, the User ID and Password are not used; LDAP queries are performed using the anonymous query method. The default is **none**.

Password

Password for the Username used to access the directory server. It is used when the Policy Manager binds to the directory server via the LDAP client. The Password is defined when the directory server is created.

When the Authentication field is set to **none**, the User ID and Password are not used; LDAP queries are performed using the anonymous query method. The default is **none**.

Searchbase

Domain Name of the Policy Manager entries on the directory server established during its configuration to indicate where policy data is stored, where **o=organization** and **c=country**. In most directory servers, **o= is required**, and **c= is optional**. The searchbase is defined in the **.ldif** file used to populate the directory server.

Removing LDAP-enabled Server from Server List

To remove an LDAP-enabled server from server list, enter the following command:

ldapdel

If no server index number is specified, the UI prompts the user for an entry.

Note

Important! There is no verification prompt for removal of servers from the list when asked which entry to delete. When a server is deleted, established policies will remain in the Policy Manager cache unless the switch is rebooted.

Flushing Cached LDAP Data from the Switch

To flush all cached LDAP data (policies) from the switch, enter the following command:

ldapflush

Manually Loading Policy Rules Set through PolicyView

To manually load policy rules set through PolicyView, enter the following command:

ldapload

Note

If more than one server is in use it is assumed that the servers are replicated, in which case there is no need to specify a server when using this command.

If intending to load policies when the directory servers are not replicated, policies will be loaded from the directory server with the highest preference setting; this server must also be enabled and operational (able to bind). Use the **ldapcfg** command to enable the server and change the server preference number, if necessary. Another option is to disable the other servers before loading the policies.

A message similar to the following displays.

```
/Networking/LDAP %
/Networking/LDAP % ldapload

15 Policies already loaded from 222.22.22.2, port 389
Backing up existing policies before performing load

15 policy rules loaded from 222.22.22.2, port 389
Backup policy rules flushed.
```

Displaying Cached Policies

To display selected portions of all policies loaded on the switch, enter the following command.

```
ldapcache
```

The display provides general guidance as to what policy definitions are loaded. Although PolicyView is used to define policies for QoS, the policies can be viewed in the LDAP cache as shown in this shortened example:

```
/Networking/LDAP %
/Networking/LDAP % ldapcache
Policy data loaded from 222.22.22.2/389 at 99/06/10 13:21:07
POLICY: MAC1    priority: 7         scope: Provisioned
          Traffic Profile Condition: MACSLCTP1
          Single-Value Action:     SLCAlcatelPqos1
POLICY: MAC2    priority: 6         scope: Provisioned
          Traffic Profile Condition: MACSLCTP2
          Single-Value PVP(*):     AllTheTime
          Single-Value Action:     SLCAlcatelPqos2
POLICY: MAC3    priority: 5         scope: Provisioned
          Traffic Profile Condition: MACSLCTP9
          Single-Value PVP(*):     AllTheTime
          Single-Value Action:     SLCAlcatelPqos3
POLICY: Entry1  priority: 0         scope: RSVP
          Traffic Profile Condition: Profile3
          RSVP action: RSVPGold

    (*)PVP=Policy Validation Period)
```

For an in-depth discussion of the parameters shown here, please refer to PolicyView online help descriptions.

Monitoring General Performance

To monitor general performance of LDAP-enabled directory servers defined on the switch, enter the following command:

```
ldapstats
```

A screen similar to the following displays to indicate the number of times the switch successfully queried different LDAP-enabled directory servers.

```
ServerIP Addr     port     queries  server access          successful not found
============================== ============                 ================
1172.19.33.4      399      0        14              14          0
2172.19.33.10     330      0        84              84          0
```

Policy Manager Configuration

User Interface commands for configuring the Policy Manager are located in the Networking/ Policy submenu.

Policy Submenu

The Policy submenu can be accessed by typing **policy** in the command line. Available **policy** submenu commands are as follows.

Command	Policy Manager Sub-Menu
flowshow	Show policy-based flows
defrsvp	Define the RSVP default policy
pqosshow	Show the Provisioned QoS default policies
pqosdef	Define a Provisioned QoS default policy
pqosdel	Delete a Provisioned QoS default policy
polevents	Show policy events

The menu items are defined below.

Displaying a List of Policy-Based Flows

To display a list of policy-based flows known by the Policy Manager, enter the following command:

```
flowshow
```

A screen displays similar to the following.

```
 flowshow command

Flow IDTypeIP address          Max BW      Policy rule
==================================       =========
1Provisioned   172.12.12.12    56          MAC1
2Provisioned   172.22.22.11    826         MAC3
```

This screen example lists policy-based flows known by the Policy Manager along with some identifying information about the flow. When the Policy Manager cannot match a policy rule to a new flow, or the cached rule definitions are flushed, the Policy Manager sets the rule field to **no policy applied**.

Defining RSVP Default Policy

To define the RSVP default policy, enter the following command:

```
defrsvp
```

When there are no LDAP-enabled directory servers available, the default policy applied to RSVP control messages is **accept**. Depending on the current setting, one of the following messages will display.

```
Change to deny?

Change to accept?
```

To change the current setting, enter **y**.

To keep the current setting, press **Enter** without making an entry.

The QoS Manager also has an RSVP enable/disable command which may impact the **defrsvp** setting for the Policy Manager. See Chapter 5, “QoS Manager” for more information.

Displaying a list of Provisioned QoS Default Policies

To display a list of provisioned QoS default policies, enter the following command:

```
pqosshow
```

A screen similar to the following displays.

```
 pqosshow command

Group IDProvisioned QoS priority
================================
9                       6
8                       6
7                       2
5                       6
1                       6
```

When no LDAP servers are available, the default policy applied to a group is based on priority.

Assigning a Provisioned QoS Default Policy a Group ID

To display a list of provisioned QoS default policies, enter the following command:

```
pqosdef
```

Enter the Group ID number to assign to a policy.

```
 LDAP server unavailable configuration

1) Group ID: 1
2) Provisioned QoS Priority         : 0

Command (Item=Value/?/Help/Quit/Redraw/Save) (Redraw) : 1=1, 6, 8-10
Command (Item=Value/?/Help/Quit/Redraw/Save) (Redraw) : 2=6


LDAP server unavailable configuration


1) Group ID: 1, 6, 8-10
2) Provisioned QoS Priority         : 6


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

When no LDAP servers are available, the default policy applied to a group is based on priority [the higher the number the lower the priority]. Current QoS priorities per group:

```
Group IDProvisioned QoS priority
================================
9                       6
8                       6
7                       2
5                       6
1                       6
```

Deleting a Provisioned QoS Default Policy by Group ID

To delete a provisioned QoS default policy, enter the following command:

```
pqosdel
```

When no LDAP servers are available, the default policy applied to a group is based on priority [the higher the number the higher the priority]. Current Qos priorities per group:

```
 pqosdel command

Group IDProvisioned QoS priority
================================
9                       6
8                       6
7                       2
5                       6
1                       6

Group ID to delete? 9
Provisioned QoS entry for Group ID 9 removed.
```

Showing Policy Events

To show policy events by event date and description, enter the following command:

```
polevents
```

A list of events important enough to display is shown. Displayed events might look something like this shortened example:

```
/Networking/Policy %
/Networking/Policy % polevent
pyTasksList 0 - pyTaskPendingLIst 0 - pyQoSRequests 0 - pyActiveFlowList 0
Event DateEvent Description
00/02/10 09:43:52policy manager login
00/02/10 09:44:02policy cache loaded from 222.22.22.2/389 with 4 rules
00/02/10 09:50:41reapply policy rules to 0 flows
00/02/10 10:07:15LDAP server 172.19.33.4 state change to unavailable
00/02/10 10:11:10LDAP server 172.19.33.4 state change to available
00/02/10 10:36:15L3 Policy rules flushed
00/02/10 10:36:15Policy rule Entry2b deleted
00/02/10 10:39:38L3 Policy rule Entry3 loaded
00/02/10 10:43:29Policy cache loaded from 208.19.33.4/399 with 7 rules
/Networking/Policy %
```

Note

For the following four tasks only, values will typically be 0, since this information is normally all cached by the Policy Manager.

pyTasksList: Indicates how many outstanding tasks under the Policy Manager remain.

pyTaskPendingList: Indicates how many pending LDAP queries remain.

pyQosRequests: Indicates how many pending QoS requests between the Policy Manager and the QoS Manager remain.

pyActiveFlowList: Indicates number of active Layer 2 flows assigned to QoS rate queue.