CHAPTER 1

Introduction

Quality of Service (QoS) features let you manage traffic intelligently across your enterprise network and optimize resource utilization.

The following topics introduce you to QoS and CiscoWorks QoS Policy Manager:

What Is Quality of Service?

Quality of Service (QoS) is a set of capabilities that allow you to deliver differentiated services for network traffic, thereby providing better service for selected network traffic. QoS expedites the handling of mission-critical applications, while sharing network resources with noncritical applications.

QoS also ensures the available bandwidth and minimum delays required by time-sensitive multimedia and voice applications. This allows you to use expensive network connections more efficiently, and to establish service level agreements with customers of the network.

QoS features provide better and more predictable network service by:

- Supporting dedicated bandwidth for critical users and applications
- Controlling jitter and latency (required by real-time traffic)
- Avoiding and managing network congestion
- Shaping network traffic to smooth the traffic flow
- Setting traffic priorities across the network

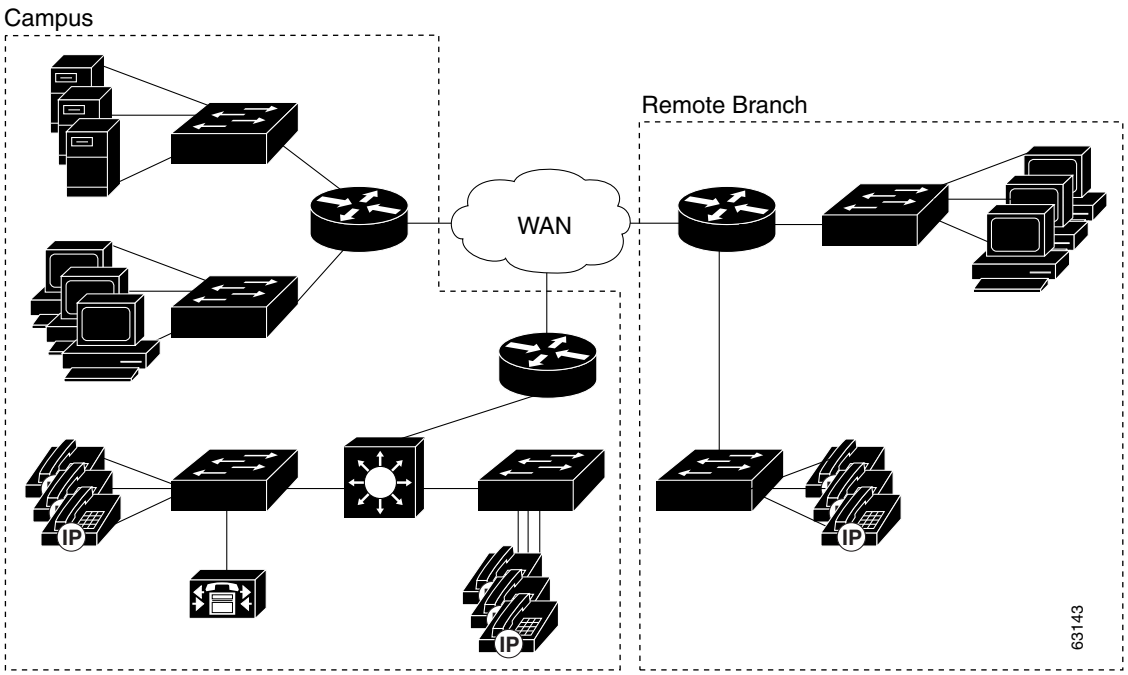
The WAN devices can limit the bandwidth available to the traffic, or give the traffic priority, or even change the classification of the traffic. In this way, you can provide end-to-end QoS in your network.

If you control the WAN and the LAN, you can control all aspects of the traffic's priority.

You can also use QoS techniques within the Campus to minimize loss and delay in real-time traffic, such as IP telephony traffic.

Figure 1-1 shows an example of an enterprise network. Typically, you classify traffic in the LAN before sending it to the WAN. The devices on the WAN then use the classification to determine the service requirements for the traffic.

Figure 1-1 Example of an Enterprise Network



What Is CiscoWorks QoS Policy Manager?

CiscoWorks QoS Policy Manager (QPM) provides a scalable platform for defining, applying, and monitoring QoS policy on a system-wide basis for Cisco devices, including routers and switches.

QPM enables you to baseline profile network traffic, create QoS policies at an abstract level, control the deployment of policies, and then monitor QoS to verify intended results. As a centralized tool, QPM is used to monitor and provision QoS for groups of interfaces and devices.

QPM provides a web-based intuitive user interface to define QoS policies, and translates those policies into the device's command line interface (CLI) commands.

QPM runs on the CiscoWorks Common Services server, which provides the infrastructure required by QPM to run from the CiscoWorks Homepage environment, and also provides management of user roles and privileges, allowing you to control who gets access to specific tasks in QPM.

The following topics provide details about the capabilities of QPM:

Overview of QoS Policy Manager

QoS Policy Manager (QPM) lets you analyze traffic throughput by application or service class, and then leverage that information to configure QoS policies to differentiate traffic and to define the QoS functions to be applied to each type of traffic flow.

By simplifying QoS policy definition and deployment, QPM makes it easier for you to create and manage end-to-end differentiated services in your network, thus making more efficient and economical use of your existing network resources.

For example, you can deploy policies that ensure that your mission-critical applications always get the bandwidth required to run your business.

QPM is suitable for large-scale enterprise deployments, and IP telephony deployments, consisting of hundreds or thousands of devices. QPM facilitates management of large networks by providing advanced user authorization capabilities through integration with Cisco Access Control Server (ACS).

You can partition the network into administrative and deployment domains. QPM allows you to organize groups of policies in separate policy groups, and supports best practices for phased deployments.

Using separate policy groups, you can also use QPM to test what-if scenarios, and run time-based deployment.

QPM includes the following management applications:

- Monitoring, page 1-3
- Provisioning, page 1-4
- Deployment, page 1-4
- QoS Configuration for IP Telephony, page 1-5
- Device Management, page 1-5
- Administration, page 1-5

Monitoring

QPM allows you to baseline profile the distribution of traffic before you change the QoS configuration, and to analyze the efficiency of the traffic going through the interfaces in your network after deploying your QoS policies.

You can schedule monitoring tasks, and generate monitoring reports displaying detailed QoS statistics for multiple interfaces, during the scheduled period.

You can also use the NBAR PD (Protocol Discovery) feature in QPM, to monitor the interfaces based on the protocols in the inbound or outbound traffic. This helps you to apply QoS on the interfaces based on specific protocol traffic.

You can view a real time QoS report for every device that you want to monitor. This helps you in obtaining the policy information attached to a device even while the device is being deployed with policies.

After you deploy the policies on the devices, the monitoring data can be collected on a real-time or on a periodic (historical) basis in QPM. You can use the Real Time Monitoring feature and the Historical Monitoring feature to view charts, based on the traffic rules that are assigned to various device interfaces. QPM supports both class-based monitoring and port-QoS monitoring.

In this way, you can obtain feedback about your QoS policy configurations, and decide whether they are working as expected.

You can also assign Threshold Sets (which are created by assigning water mark levels to class metrics) to the interfaces of a device. This helps you to make use of the Event Browser feature which generates real time reports of threshold violations in the traffic flow through the interface.

Provisioning

The QPM Provisioning application lets you define, maintain, and deploy scalable end-to-end QoS policies for your network devices.

You can define QoS properties that are suitable for specific sets of devices, interface types, and interface properties, including VLANs. You can then assign interfaces to your policies.

For example, you can define a set of properties and traffic rules to police LAN edge traffic on switches, and then assign the appropriate switch interfaces to this policy.

QPM contains global libraries of policy building blocks, to simplify policy definition. The IP Alias library contains definitions of groups of IP addresses and host names, and the Application Alias library contains protocol and port definitions for applications.

QPM lets you create policy templates to share common properties and traffic rules across different device groups and policy groups. Policy templates are policies without network assignments, and they are stored in a global library, so that they can be used in any policy group, or device group.

If you have already defined QoS configurations on your devices using the CLI, you can import them into QPM. QPM translates the QoS configurations into QoS properties and traffic rules , and generates reports summarizing the import process.

QPM also provides a Cisco TelePresence compatible QoS policy, which you can configure to receive notifications for threshold violations in your TelePresence circuit. This helps you to optimize your TelePresence circuit by offering differentiated services.

Deployment

When you deploy your QoS policies to their assigned network devices, QPM translates your policies into device commands and enters the commands through the device's command line interface (CLI).

Your QoS policies are organized in policy groups. You can deploy an entire policy group, or you can specify a set of devices, and QPM will deploy the appropriate policies within the policy group to those devices.

The time to complete a deployment depends on the number of devices to which you are concurrently deploying. QPM lets you control the number of devices for a deployment, so that the total deployment time remains within acceptable limits.

You can schedule the deployment of policies in QPM by specifying the server time and date for deployment.

Through QPM, you can preview the commands that will be used to configure the devices. During policy distribution, you can view device log messages as QPM configures each device, so that you can identify configuration successes and failures.

You can verify the device configuration to ensure that your policy definitions match the actual device configurations.

You can restore a previously distributed policy group and then redeploy it. This is especially important when certain unexpected errors occur in a deployment, and there is an immediate need to go back to a previous deployment.

Logging and web-based reporting capabilities help you maintain records of policy deployments.

QoS Configuration for IP Telephony

QPM includes an IP telephony wizard to help you configure end-to-end QoS for converged networks. The wizard automatically assigns the QoS policies required for switch and router interfaces in your IP network. The wizard is flexible enough so that you can accept or reject the automatic assignments.

The wizard uses voice policy group templates based on the Cisco IP Telephony QoS Design Guide recommendations.

You can modify voice policy groups, by changing QoS properties or policies, as for any policy group.

QPM generates various voice reports that help you troubleshoot your IP telephony network.

You can monitor IP telephony traffic and then adjust your QoS configuration, if required. See Monitoring, page 1-3 for more information about the Performance Analysis application.

Device Management

QPM includes a global device inventory for all the devices on which you want to define QoS configurations. You can add devices to the device inventory by importing the devices from the Device Credentials Repository (DCR) in CiscoWorks Common Services. The DCR is the central credentials repository for QPM.

You can also import virtual devices from a virtual device file created by QPM.

QPM connects to the devices to discover their interfaces and other information. You can view and manage device properties in the device inventory.

If ACS is installed on your network, you can use the ACS device groups with their user permissions, to facilitate the management of your network. QPM synchronizes device group information with ACS.

Administration

The administration options in QPM are:

- Audit

  This application provides information about changes made to the policies in a policy group, and any policy group actions. It registers the modification time and the login name of the user who made the modifications.

- SNMP

  You can change the default SNMP settings for devices in the QPM inventory using this application.

- User Permissions Report

  You can view how QPM user permissions relate to CiscoWorks user permissions using this application.

  If you are using ACS to control authorization, this matrix does not represent your user permissions configuration; it only shows the default authorizations for CiscoWorks authorization levels.

- License

  You can obtain a product license and license your application, view details of your current software licenses or install a new license using the License application.

  You can upgrade an existing installation of QPM 4.0 and QPM 4.0.x to version QPM 4.1 while retaining the inventory and preserving as much of the configuration of the application.

QPM 4.1 provides an evaluation license, three types of base licenses and three types of incremental device update licenses or device packs.

- Notification Groups

  In QPM, you can create Notification Groups to receive notifications for threshold violations in your Cisco TelePresence circuit. You can configure Notification Groups by the type of notification (email or trap) you require.

  Later you can select these Notification Groups and configure thresholds for the traffic rules present in the TelePresence compatible policy available in QPM.

QPM Features

Table 1-1 describes the main features of QPM.

Table 1-1 QPM Features

Feature	Description
Policy abstraction from device commands	You define policies through QPM's user interface, and then QPM converts your policies to device commands. You do not have to know the device commands to create policies. QPM hides the complexity of tedious and error prone device configuration.
Simplified policy definition	QPM's policy definition interface simplifies the creation of policies. You can create basic and complex traffic classifiers to define the traffic you are targeting, and you can define aliases for host groups and application services. You can save alias definitions in global libraries, and use them when defining policies. QPM lets you prioritize traffic rules by changing the order in which they appear in the policy's list of traffic rules.
Policy definition	Policies contain a constrained set of QoS properties and traffic rules, and an assigned set of network elements. Defining traffic rules within a policy, instead of independently per device, reduces repetitive policy definition. QPM lets you define only QoS properties and traffic rules that are supported by the device constraints specified for the policy.
Import of existing device configuration	If you have already defined QoS configuration on your devices using the CLI or other application, you can import them into QPM. QPM creates policy groups containing the imported policies, and assigns them to the devices.
QoS configuration for IP telephony traffic	QPM supports QoS features that ensure reliable delivery of voice, with low latency, resulting in minimal delay, jitter, and packet loss. QPM includes a wizard and predefined templates to automatically configure end-to-end QoS policies for voice in your IP telephony network. You can modify the voice templates and add new policies to fine-tune your IP telephony QoS configuration.
AutoQoS	QPM supports AutoQoS features simplifies QoS deployment by automating Cisco IOS QoS features.

Table 1-1 QPM Features (continued)

Feature	Description
Scalability	QPM can be used in large networks containing hundreds and thousands of devices. You can use multiple device groups, each of which contains a subset of network devices, and can be managed separately.
Device querying	QPM queries devices you add to the QPM device inventory to determine the software version, device type, and available interfaces. Because the information is obtained directly from the device, it is reliable.
CiscoWorks integration	QPM runs on the CiscoWorks Common Services server, and is installed as an add-on to the CiscoWorks Home Page. The CiscoWorks Home Page requires a single login for all products installed on the same server as CiscoWorks Common Services. QPM is accessed through the CiscoWorks Homepage. The Device Credentials Repository (DCR) in CiscoWorks Common services is the central credentials repository for QPM. You can also import device inventories from DCR. This simplifies the task of adding devices to QPM.
Web-based reporting	QPM produces reports of historical monitoring tasks to help you troubleshoot QoS problems in your network. You can store these HTML reports on your intranet, and manipulate them as you require, or print them from the browser.
Audit trail	QPM maintains logs of job and device policy distributions, and maintains a history of these logs. This ensures there is an audit trail of policy configuration actions. The job log also specifies the user that made the changes and the time of the changes.
Ability to view device commands	Allows you to view the device commands that will be used to configure your devices. You can view these commands before and after you deploy the QoS configuration to the devices.
Deployment control	You can deploy the QoS configuration to the network devices, or to an output configuration file. QPM lets you define the ranges of ACL numbers to be used when translating policies to CLI. You can also redeploy a previous job. When distributing policies, QPM distributes only the policies that have changed. QPM lets you halt policy distributions when you are distributing policies to devices. You can resume the deployment of a job that you previously stopped.
Verification of device configuration	Allows you to check whether changes have been made on your devices by comparing the policies configured on the devices with the policies defined in your QoS policy group.
Ability to restore a previously deployed policy group	Allows you to restore a previously deployed policy group. This feature is very useful when unexpected errors occur as a result of the deployment of a policy group and there is an immediate need to go back to a previous version of that policy group.

Table 1-1 QPM Features (continued)

Feature	Description
Performance analysis	Supports QoS monitoring. You can baseline profile traffic by top applications or DiffServ classes, select devices and interfaces for policy validation, schedule monitoring tasks, and generate monitoring reports.
Independent QoS Monitoring	Monitors a device's interfaces using the CISCO-CLASS-BASED-QOS MIB and the CISCO-CAR MIB, even when the policies on the interfaces are not configured and deployed by QPM. This allows you to monitor policies configured via other mechanisms.
Enhanced Monitoring Workflow	Provides an object selector with devices and monitorable interfaces, for easy launch of real-time charts.
Nested Policies	Enables you to create hierarchical policies, so that you can create multiple levels of policy groups and attach these to child policies which in turn can be attached to the interface. This feature of QPM enables you to segregate traffic based on flow source or destination, and apply different policing/shaping and service policies on each class of traffic.
TelePresence compatible policy	Provides a Cisco Telepresence-compatible QoS policy based on Cisco recommendations for QoS in a TelePresence circuit. You can configure circuit and class-based thresholds for the policy, and receive notifications for threshold violations. This helps you to optimize the network traffic in the TelePresence circuit.
Monitoring of policies defined through Nested Policies	Supports the monitoring of policies defined through Nested Policies, if they are assigned to a device interface
Provisioning of VC Bundles	Supports configuring QoS on VC Bundles
Monitoring ATM VC Bundles	Allows you to monitor policies for the device interface where ATM VC Bundles are defined.
Provisioning and monitoring of NBAR	Allows you to configure NBAR applications that have been updated using the PDLMs.
Content networking support	Uses NBAR or dNBAR to recognize and classify specific applications for which network services can then be invoked.
Monitoring of NBAR PDLMs	One of the graph types available for selection in the enhanced monitoring workflow. This provides the capability for QPM to report on the amount of traffic hitting each class-map/published application (For example, Citrix tag).
NBAD PD monitoring	Allows you to monitor protocols in both inbound and outbound traffic through the interface.
Port-QoS Monitoring	Allows you to provide QoS statistical information on a per-port basis.
VLAN Monitoring	Allows you to monitor VLAN interfaces that are based on CBQoS MIB. QPM supports both real time and historical monitoring tasks for VLAN interfaces.

Table 1-1 QPM Features (continued)

Feature	Description
Threshold Monitoring	Provides the capability for QPM to deploy RMON alarms and events to devices, so that devices can monitor QoS MIB objects locally, without the need for QPM to poll the device. This allows QoS performance monitoring to scale to significantly higher numbers. The specified MIB object will be checked against a high and low threshold. If the high threshold is exceeded, an SNMP trap will be sent to the QPM server. No additional traps will be sent until the low (reset) threshold is crossed. The delta (difference from previous) values are used to determine whether the high or low water mark is crossed. An Event Browser is provided to view live and snapshot events for the threshold crossing events.
Import and Export utilities	Includes an export utility and an import utility, which enable you to: • Migrate and upgrade QPM 4.0 database, configuration information, and other data to QPM 4.1. • Migrate QPM database, configuration information, and other data from one QPM server to another.
Provisioning QoS configuration employing time-based ACLs	Allows you to specify a time range for the ACL to be applied while creating In/Out policies.
Device upgrade drop-ins	Supports incremental device upgrade (IDU). This will enable existing users of QPM to purchase device upgrades for new versions of devices and IOS and add them incrementally to their existing installation.
Tiered License structure	Provides an SMB license, two types of base licenses, three types of incremental device update licenses or device packs, and two upgrade licenses.

Basic Concepts in QPM

This section describes basic terms and concepts used in QPM.

QoS Properties

QoS Properties define the settings such as congestion management and avoidance, shaping, and traffic control.

In Traffic Rule and Out Traffic Rule

Rules that are applied to a selected traffic flow. A traffic rule includes a traffic classifier, which defines the characteristics of the traffic flow, and the QoS actions to be applied to the selected traffic.

Traffic Rules are managed within a Policy.

Policy	Policies are defined with device constraints, such as device model, OS type and version, interface type, card type, and network element type (device, interface, subinterface, and so on). A policy must have assigned device elements before deployment, for its policies to be applied to the appropriate devices. Policies are managed within a Policy Group.
Voice Policy	Policy for defining QoS properties and policies for voice traffic in an AVVID (architecture for voice, video, and integrated data) network. A voice policy contains a Voice Role attribute.
Voice Role	Logical grouping of interface types according to their function, or location on the network, as appropriate for voice-related QoS. A voice role is defined as an internal attribute in a Voice Policy.
Policy Template	Policy containing a predefined set of QoS properties and policies for specified device constraints. A policy template can be used to share policies across policy groups. The policy template does not include preassigned devices.
Voice Template	A Policy Template for a Voice Policy. A voice template includes a Voice Role as an internal attribute.
Device Group	Subset of network devices defined in ACS, typically organized according to device function or network topology. QPM supports ACS device groups to facilitate management of large-scale networks.
Policy Group	A deployment unit containing a set of policies and any referenced global information. When you deploy a policy group, QPM saves a historical version, which you can later restore for policy editing and redeployment.
Performance Analysis	Scheduling monitoring tasks, and generating monitoring reports for QoS analysis. You can baseline profile traffic by top applications or DiffServ classes, select devices and interfaces for policy validation.

How Does QPM Interact with Other Network Management Products?

QPM interacts with other network management products as follows:

ACS 4.1.x and ACS 4.2—You can use ACS user permissions and device groups in QPM. QPM will integrate with ACS for authentication, authorization and device grouping.

Supported Devices and Software Releases

QPM supports a broad range of Cisco devices, including routers, and switches. For details of the devices and software releases that QoS Policy Manager supports, and the QoS techniques you can use on the supported platforms, see the following URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps2064/products_device_support_tables_list.html

Migrating From QPM 4.0

This section describes the main differences between this version of QPM (QPM 4.1) and QPM 4.0, and is intended for experienced QPM 4.0 users.

- QPM 4.1 is integrated with CiscoWorks Common Services 3.2.
- New User Interface based on CUES (Cisco User Experience Standards).
- Customization of QPM Dashboard—You can customize the Dashboard page in QPM by adding the available portlets and changing the layout of the content area of the portlets.
- Availability of QPM view in LMS Portal—If you have installed LMS Portal with Common Services 3.2, a separate view for QPM is available in LMS Portal. You can also create new views for specific features in QPM.
- Availability of Cisco TelePresence compatible policy—You can configure thresholds for circuit utilization and class utilization for the Cisco TelePresence compatible policy. You can receive notifications as SNMP trap or email, for the threshold violations. This helps you to optimize the traffic in the TelePresence circuit.
- Support for NBAR PD monitoring—NBAR PD (Protocol Discovery) monitoring helps you to separately monitor the protocols in the inbound and outbound traffic through device interfaces. This helps you to understand the protocol traffic before you deploy QoS policies on devices.
- Support for Port-QoS monitoring—QPM uses the Cisco Port QoS MIB to provide monitoring capabilities for each port. Both Real Time charts and Historical Monitoring charts are displayed to provide the QoS statistical information on a per port basis.
- SNMP v3 support—QPM allows you to discover the device using SNMP v3 credentials, if they are available on the device.
- Command Service Library support—QPM supports Command Service Library (CmdSvc) to enable you to select the login protocol among SSHv2, SSHv1, and Telnet, while re-discovering devices.
- Support for secondary DCR credentials such as Secondary Username, Secondary Password, Secondary Enable Password. This helps you to discover devices even if the primary credentials fail.
- Support for ATM PVC Monitoring—QPM 4.1 supports real time and historical monitoring of ATM multipoint sub-interfaces with VCs and PVCs. You can select VCs and PVC bundles configured on the interface for monitoring.
- Support for monitoring of child policies—You can monitor the interfaces based on the child policy available under a parent policy deployed on the interfaces.
- Support for VMware ESX Server 3.0.2 and 3.5.0.
- Support for Microsoft Windows Vista client.
- Support for Solaris 10 OS.
- Support for NCM Event Notification—You can integrate QPM with NCM to receive event notification in QPM for device configuration change and image upgrade. The event notifications from NCM to QPM help you synchronize the device level changes with QPM.
- Support for Integrating CUOM with QPM—You can use CUOM with QPM to exchange QoS-related metric data from routers, gateways, and IP phones.