Cisco Systems

User Guide for QoS Policy Manager 3.0

CiscoWorks

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7812542=
Text Part Number: 78-12542-01

User Guide for QoS Policy Manager 3.0

Preface

This manual describes CiscoWorks QoS Policy Manager, and provides instructions for using it.

Audience

This manual is for network architects and designers, network administrators, network management consultants, and integration partners.

To use QoS Policy Manager, you should have a basic understanding of network management, TCP/IP, and the configuration of your network. You should know how to use Microsoft Windows 2000.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font

Item	Convention
Menu items and button names	**boldface** font
Selecting a menu item	**Option>Network Preferences**

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Note Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review the QoS Policy Manager documentation on Cisco.com for any updates.

The following documentation is available:

PDF Files

The following PDF files are located on the QPM installation CD:

- User Guide for QoS Policy Manager 3.0
- Getting Started Guide for QoS Policy Manager 3.0
- Installation Guide for QoS Policy Manager 3.0

Note Adobe Acrobat Reader 4.0 or later is required.

Online Documentation

- Online help for CiscoWorks2000, Common Services, and QPM.

  In the CiscoWorks2000 desktop, select an option from the navigation tree, then click **Help.**

  The online help for QPM includes all the information in the QPM User Guide and QPM Getting Started Guide.

- Context-sensitive online help for QPM.

  In the QPM window, click the Help link at the top of each page.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

Cisco documentation is available in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquires are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

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:

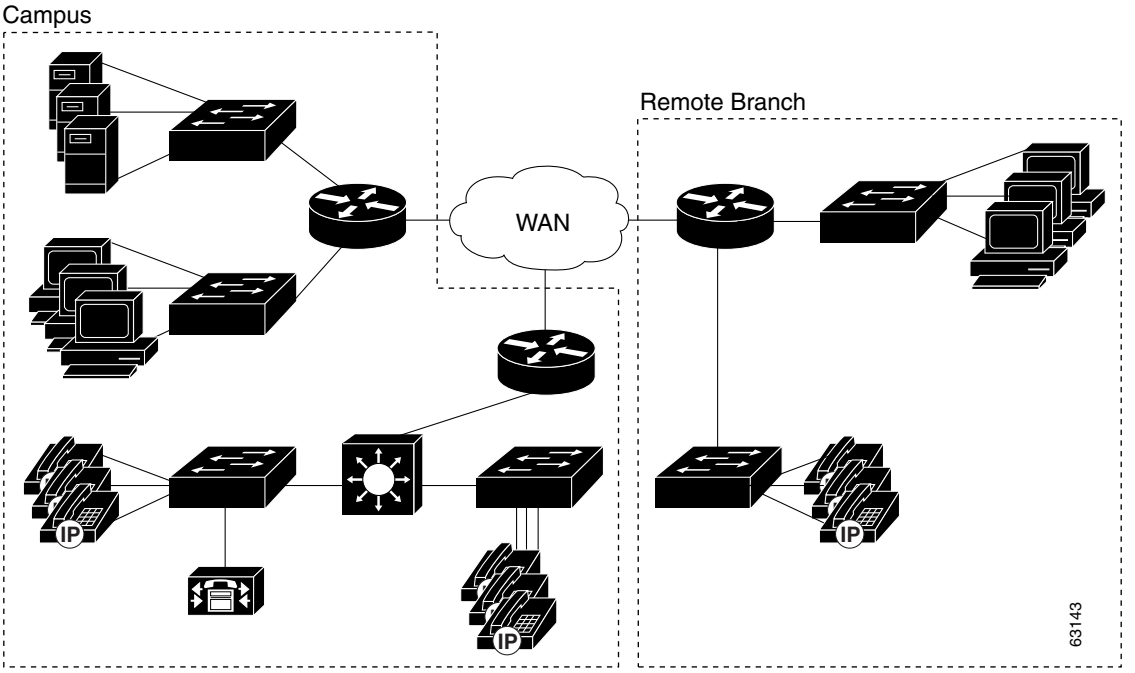
- Supporting dedicated bandwidth for critical users and applications
- Controlling jitter and latency (required by real-time traffic)
- Avoiding and managing network congestion

- Shaping network traffic to smooth the traffic flow
- Setting traffic priorities across the network

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. 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 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 can be installed as a standalone server, or as an add-on to CD One 5th Edition. CiscoWorks Common Services provides the infrastructure required by QPM to run from the CiscoWorks desktop 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 QPM's capabilities:

- Overview of QoS Policy Manager, page 1-4
- QPM Features, page 1-8
- Basic Concepts in QPM, page 1-10
- How Does QPM Interact with Other Network Management Products?, page 1-11
- Supported Devices and Software Releases, page 1-12

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 deployment groups, and supports best practices for phased deployments. Using separate deployment groups, you can also use QPM to test what-if scenarios, and run time-based deployment.

QPM includes the following management applications:

- QoS Analysis, page 1-5
- Policy Configuration, page 1-5
- QoS Configuration for IP Telephony, page 1-6
- Device Management, page 1-6
- Deployment, page 1-6
- Additional Administration Applications, page 1-7

QoS Analysis

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. The monitoring data can be collected on a real-time, or on a periodic (historical) basis. In this way, you can obtain feedback about your QoS policy configurations, and decide whether they are working as expected.

Policy Configuration

The QPM Policy Configuration application lets you define and maintain scalable end-to-end QoS policies for your network devices. You can define groups of QoS policies that are suitable for specific sets of devices, interface types, and interface properties, including VLANs. You can then assign interfaces to your policy groups. For example, you can define a group of policies to police LAN edge traffic on switches, and then assign the appropriate switch interfaces to this policy group.

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

If you have already defined QoS configurations on your devices using the CLI, you can upload them into QPM. QPM translates the QoS configurations into QoS policies and policy groups, and generates reports summarizing the upload process.

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, yet is flexible, so that you can accept or reject 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 QoS Analysis, page 1-5 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 manually, or you can import devices from the CiscoWorks Resource Manager Essentials (RME) application, or from a CSV file. 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.

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 deployment groups. You can deploy an entire deployment group, or you can specify a set of devices, and QPM will deploy the appropriate policies within the deployment 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 deploy your QoS configurations directly to network devices from QPM, or you can deploy to a configuration file, which can be deployed to the device using TFTP or any other application that downloads configuration files to the devices.

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 deployment 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.

Additional Administration Applications

- Audit—This application provides information about changes made to the policy groups in a deployment group, and any deployment group actions. It registers the modification time and the login name of the user who made the modifications.
- QPM 2.1.x Database Import—This application lets you import information from exported QPM 2.1.x databases, and converts them to QPM 3 format.
- Backup and Retrieve—This application lets you back up and retrieve all the QPM data on the QPM server. You can create full backups, and you can schedule regular incremental backups.

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 filters 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 policies by changing the order in which they appear in the policy group's list of policies.
Policy group definition	Policy groups contain a constrained set of QoS properties and policies, and an assigned set of network elements. Defining policies within a policy group, instead of independently per device, reduces repetitive policy definition. QPM lets you define only QoS properties and policies that are supported by the device constraints specified for the policy group.
Upload of existing device configuration	If you have already defined QoS configuration on your devices using the CLI or other application, you can upload them into QPM. QPM creates policy groups containing the uploaded 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.
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.

Table 1-1 QPM Features (continued)

Feature	Description
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, which can be installed as an add-on to the CiscoWorks2000 desktop. QPM is accessed through the CiscoWorks2000 desktop, and you can import device inventories from the CiscoWorks Resource Manager Essentials applications. This simplifies the task of adding devices to QPM.
Web-based reporting	QPM produces reports in HTML format to help you troubleshoot QoS problems in your network. You can store these 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	QPM lets you 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	QPM lets you check whether changes have been made on your devices by comparing the policies configured on the devices with the policies defined in your QoS deployment group.

Table 1-1 QPM Features (continued)

Feature	Description
Ability to restore a previously deployed deployment group	You can restore a previously deployed deployment group. This feature is very useful when unexpected errors occur as a result of the deployment of a deployment group and there is an immediate need to go back to a previous version of that deployment group.
Performance analysis	QPM 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.
Content networking support	QPM supports using NBAR or dNBAR to recognize and classify specific applications for which network services can then be invoked.

Basic Concepts in QPM

This section describes basic terms and concepts used in QPM.

QoS Policy

Also known as a QoS policy class, a QoS policy is a rule that is applied to a selected traffic flow. A policy includes a filter, which defines the characteristics of the traffic flow, and the QoS actions to be applied to the selected traffic. Policies are managed within a Policy Group.

Policy Group

Policy groups allow you to group policies according to their role in the network, for example, access policies, distribution policies, and so on. Policy groups 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). These device constraints define the types of network elements that can be assigned to the policy group, and the QoS features that can be configured by the policies in the group.

A policy group must have assigned device elements before deployment, for its policies to be applied to the appropriate devices. Policy groups are managed within a Deployment Group.

Voice Policy Group

A policy group for defining QoS properties and policies for voice traffic in an AVVID (architecture for voice, video, and integrated data) network. A voice policy group contains a Voice Role attribute.

Voice Role — A 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 Group.

Policy Group Template — A Policy Group containing a predefined set of QoS properties and policies for specified device constraints. A policy group template can be used to share policy groups across deployment groups. The policy group template does not include preassigned devices.

Voice Template — A Policy Group Template for a Voice Policy Group. A voice template includes a Voice Role as an internal attribute.

Device Group — A 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.

Deployment Group — A deployment unit containing a set of policy groups and any referenced global information. When you deploy a deployment 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 3.1 and higher—You can use ACS user permissions and device groups in QPM.
- RME 3.3 and higher—You can import devices directly from RME, or you can export a CSV file from RME, and then import it to QPM.

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/univercd/cc/td/doc/product/rtrmgmt/qos/qpm3_0/qpm30dev/index.htm

Migrating from QPM 2.1.x

This section describes the main differences between this version of QPM and QPM 2.x, and is intended for experienced QPM 2.x users.

- QPM is integrated with CiscoWorks2000, and all QPM applications are accessed from a single web interface, instead of the separate Policy Manager window and Distribution Manager window in QPM 2.x.
  - Databases are now called Deployment Groups. Deployment group and policy management options, which were accessed from the Policy Manager window, can be accessed from the Configure tab.
  - Device management options, which were accessed from the Policy Manager window, can be accessed from the Devices tab.
  - Deployment options, which were accessed from the Distribution Manager window, can be accessed from the Deploy tab.
  - Global settings options, such as Write Memory, Access Control, and NBAR Port Mapping, which were accessed from the Distribution Manager window, are now defined as device group properties in the Devices tab. These options can be overridden per device.
- All policies are now defined within policy groups. A policy group contains a constrained set of QoS properties and policies, and an assigned set of device elements, similar to a device group in QPM 2.x. (See the definition for a Policy Group, page 1-10.)

Note QPM 3 device groups are administrative device domains. They are *not* the same as QPM 2.x device groups.

- QPM's IP telephony configuration feature facilitates the QoS configuration for IP telephony. A configuration wizard guides you through the definition of your network topology, and then automatically assigns the relevant network points to the appropriate voice policy groups. You can modify the default voice policy groups.
- QPM supports policy monitoring. You can select policies and devices for monitoring, schedule monitoring tasks, and generate monitoring reports. You can access these features from the Performance Analysis option in the Reports tab.
- QPM contains a global inventory system. Devices can be added manually, or imported directly from RME. You access device import and device management options from the Devices tab.
- The Upload Device Configuration option uploads the device configuration into policy groups. If there are appropriate existing policy groups in the deployment group, these are used, otherwise QPM creates new policy groups. This option is now accessed from the Policy Groups page of the Configure tab.
- If you are running ACS on the network, you can use the ACS user permissions in QPM. When you use ACS user permissions, QPM synchronizes with ACS and organizes the devices in the device inventory according to the ACS device groups. Each device group can be managed separately, and a device group can contain multiple deployment groups (databases) as in QPM 2.x. Device groups are managed through the Devices tab.
- Additional devices and QoS features supported—see the list of supported devices and QoS features, at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/qos/qpm3_0/qpm30dev/index.htm

Note You can import into QPM 3, databases from QPM 2.1.x that have been exported to an XML file using the QPM 2.1.x export utility.

Planning for Quality of Service

Effective use of Quality of Service (QoS) capabilities requires careful planning. Before you deploy QoS to your network, carefully consider the types of applications used in the network and which QoS techniques might improve the performance of those applications. Then, use CiscoWorks QoS Policy Manager (QPM) to create and deploy your QoS policies to the network, and analyze QoS performance.

The following topics introduce you to QoS concepts and QoS capabilities supported by QPM:

Planning for QoS Deployment

The process of planning and implementing QoS is cyclical, and requires the following steps:

1. Identify the application traffic in your network:
   - Identify the applications in the network, and the traffic distribution of these applications. For example, you might identify the following applications—SAP (10% of traffic), HTTP (30%), FTP (20%), Voice over IP (VoIP) (30%), and other applications (10%).
   - Identify the business critical applications. In our example these might be SAP, Intranet HTTP, and VoIP.

- Evaluate the resources requirements for each application, for example, whether the application requires bulk traffic transfers, or streaming, and so on. For VoIP, calculate the bandwidth requirements.
- Based on these calculations, decide what level of service each application requires.

Note Use QPM monitoring to baseline profile your traffic. See Performing Baseline QoS Analysis, page 9-4.

2. Analyze your network:
   - Verify the capacity of your network devices (CPU, software, and so on).
   - Verify the capacity of your network links (link speeds, overhead, and so on).
   - Decide whether domain boundaries are trusted or untrusted. You can then decide where to classify traffic.
   - Analyze the network topology and traffic flow.
   - Analyze the network links in each layer of your network, and the possible QoS mechanisms that can be implemented on those links.

Note In converged networks, QPM's IP telephony wizard guides you through the definition of your network topology, and configures QoS on the relevant network points.

3. Use QPM to configure QoS policies throughout the network:
   - Define policies to mark traffic at the edge of the network.
   - Define policies based on markings for each network site.
   - Define policies for aggregate traffic at the WAN edge.
4. Use QPM to deploy your QoS policies:
   - Test deployment in the laboratory, or in a small section of the network.
   - In the network, deploy policies incrementally—start deployment at the edge, and continue towards the core.

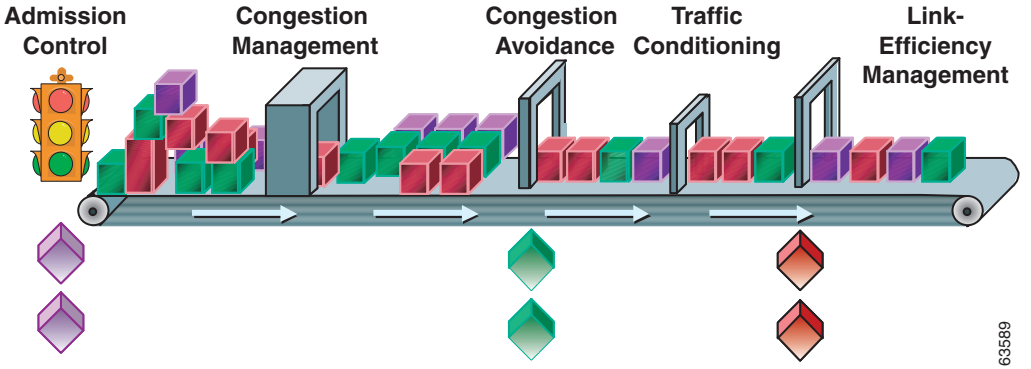
5. Use QPM to monitor QoS, and adjust QoS policies:
   - Check whether you achieved the desired QoS by measuring transmitted traffic and dropped traffic for different traffic classes.
   - Monitor application performance.
   - Adjust QoS policies where necessary, and redeploy.

What Types of Quality of Service Does QPM Handle?

QPM detects the QoS capabilities that are available on each of your devices, as defined by the device model, interface type, and the software version running on the device. You can choose different QoS techniques for different interfaces, as appropriate, to implement your overall networking policies.

Figure 2-1 shows the sequence a packet follows, and the QoS capabilities that might be activated when the packet reaches an interface.

Figure 2-1 QoS Capabilities for a Packet at an Interface



QPM policies let you define the following:

- Classification—Packet classification identifies traffic flows according to IP precedence or Diff-Serv Code Point (DSCP) values.
  - In QPM, you can filter traffic for conditional policies by identifying traffic flows according to their classification, source, destination, or application.

  - In QPM, you can classify traffic by defining marking policies. Marking is generally applied to inbound traffic on its first interface.
- Traffic Conditioning—Policing and Shaping:
  - Policing—The rate of traffic allowed to enter or exit an interface. On routers, you can police aggregate flows. On Catalyst switches, you can police single flows or aggregate flows. Out-of-profile traffic is discarded or its precedence value is marked down.
  - Shaping—How to smooth the rate of traffic. Shaping can only be defined on outbound interfaces.
- Congestion Management and Congestion Avoidance—Scheduling and drop preferences to be applied to packets for congestion management and avoidance. Some queuing methods queue packets according to their ToS values; for other queuing methods you might need to specify queuing priorities.
- Link-Efficiency Management—Traffic control mechanisms for management of voice traffic, such as (Compressed Real-time Protocol) CRTP and Link Fragmentation and Interleaving (LFI), and Frame Relay Fragmentation (FRF). They are used in the WAN for voice traffic.

The QoS features supported by any specific device depends on the device type and OS software version. For information about the devices and software versions that are supported by QPM, see the device support tables at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/qos/qpm3_0/qpm30dev/index.htm

The following topics describe the types of QoS capabilities you can implement with QPM:

- Packet Marking, page 2-5
- Traffic Policing for Limiting Bandwidth and Marking Traffic, page 2-6
- Traffic Shaping for Controlling Bandwidth, page 2-8
- Queuing Techniques for Congestion Management for Outbound Traffic, page 2-10
- Queuing Techniques for Congestion Avoidance on Outbound Traffic, page 2-21
- Management of Voice and Other Real-Time Traffic, page 2-23

- Managing Traffic Through Access Control, page 2-27
- Signaling Techniques, page 2-27

Related Topics

- More Information About Quality of Service, page 2-30

Packet Marking

Packet marking (also known as classification, or coloring) is used to partition network traffic into multiple priority levels, or classes of service. Because the classification value is embedded in the packet, changing it can affect the way the packet is handled on its entire path through the network.

In QPM, you can define marking policies to mark packets, using the following techniques:

- IP precedence value, or DiffServ Code Point (DSCP) value—Sets the IP precedence bits, or the IP differentiated services code point (DSCP) in the IP type of service (ToS) byte.
- Class of Service (CoS) value—Sets the layer 2 CoS value. This value can be used by layer 2 devices to determine the packet classification.
- MultiProtocol Label Switching (MPLS) Experimental value—Specifies the CoS for an MPLS packet; the IP packet's CoS is not changed as the packet travels through the MPLS network.
- Frame Relay Discard Eligibility (DE) Bit value—Determines the priority of a frame in a congested frame relay network. Frames with the DE bit set to 1 are dropped before frames with the DE bit set to 0.
- Trust state—The trust state of a port determines how it marks received traffic from connected devices. All frames received through untrusted ports are marked with the port CoS value (the default is zero). Frames received through trusted ports retain their CoS or ToS values. Trust extension values let you extend the trust boundary beyond the connected device.

QPM implements marking policies using policy-based routing (PBR), or modular QoS CLI (MQC) marking, depending on the device type and OS software version.

Note Packet marking can also be defined as part of a policing policy. In these cases, QPM uses Committed Access Rate (CAR) or MQC policing. See Traffic Policing for Limiting Bandwidth and Marking Traffic, page 2-6 for more information.

After you mark packets, you can define queuing, shaping, and policing policies that filter by marking value to create differentiated services.

Note Some scheduling methods automatically prioritize traffic according to packet marking, and you do not need to deploy specific queuing policies for interfaces using those queuing methods.

Related Topics

- Traffic Policing for Limiting Bandwidth and Marking Traffic, page 2-6

Traffic Policing for Limiting Bandwidth and Marking Traffic

Traffic policing allows you to control the rate of traffic sent or received on an interface. Traffic policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network.

You can specify one of the following actions for traffic that conforms to or exceeds the specified rate (depending on the type of policing):

- Transmit—The packet is sent.
- Drop—The packet is discarded.
- Mark and transmit—The ToS bits in the packet header are rewritten. The packet is then sent.
- Markdown—This reduces the packets' IP precedence or DSCP values according to a predefined markdown mapping table.

One of the main uses for policing policies is to ensure that traffic coming into your network does not exceed agreed-upon rates. If you define a policing policy for inbound traffic, you can throttle misbehaving traffic before it gets into your network. Because you control the traffic's rate at the inbound interface, the traffic should be well-behaved while it is in your network.

Because rate limiting does not smooth or shape traffic, it does not buffer packets, and therefore, unlike shaping, it does not add any delay to transmission of packets that conform to the rate limits.

The traffic policing feature works with a token bucket mechanism. For a description of a single token bucket algorithm, see:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart4/qcpolts.htm

In QPM, you can define the following types of policing policies:

- Microflow policing—QoS applies the specified bandwidth limit separately to each flow in matched traffic.
- Policing for aggregate flows on the same interface—QoS applies the specified bandwidth limit to all matched traffic on the interface.
- Policing for cross-interface aggregate flows—QoS applies the specified bandwidth limit to matched traffic from all the interfaces in the device group.

QPM supports the following policing techniques:

- CAR Policing—Uses a single token bucket algorithm based on the following three parameters:
  - Average rate—The average rate determines the long-term average transmission rate. Traffic that falls under this rate will always conform.
  - Normal burst size—The normal burst size determines how large traffic bursts can be before some traffic exceeds the rate limit.
  - Excess burst size—The excess burst (Be) size determines how large traffic bursts can be before all traffic exceeds the rate limit. CAR provides managed discard between the excess burst and extended excess burst parameters. Traffic that falls between the normal burst size and the excess burst size exceeds the rate limit with a probability that increases as the burst size increases.
- MQC Policing—Uses a single token bucket algorithm and a two token bucket algorithm. A single token bucket system is used when the violate action option is not specified, and a two token bucket system is used when the violate action option is specified.
- Two-rate policing on Catalyst switches—Uses a two token bucket algorithm with a normal rate and an excess rate:
  - Normal rate—Packets exceeding this rate are marked down.

- Excess rate—Packets exceeding this rate are either marked down or dropped as specified by the violate action.

Note You can create policies to mark packets without the traffic policing feature, using packet marking policies. See Packet Marking, page 2-5 for more information.

Related Topics

- Packet Marking, page 2-5
- Traffic Shaping for Controlling Bandwidth, page 2-8

Traffic Shaping for Controlling Bandwidth

Traffic shaping controls how much of the interface's bandwidth should be allocated to traffic flows.

Traffic shaping attempts to smooth the traffic flow to meet your rate requirements by buffering the packets. This puts a cap on the bandwidth available to that traffic, ensuring that the remainder of the interface's bandwidth is available to other kinds of traffic. Traffic shaping affects flows even during times of little congestion, and because it buffers the packets, adds some delay to transmission time.

You set a target average transmission rate for traffic. You can also define a burst size and an exceed burst size to further model the flow. These values define how much data is sent from the buffer per time interval. When the buffer is full, packets are dropped.

Some types of shaping support two types of shaping commands: average and peak. When shape average is configured, the interface sends no more than the committed burst (Bc) in each interval. When shape peak is configured, the interface sends the committed burst (Bc) plus the excess burst (Be) bits in each interval.

In a link layer network such as Frame Relay, the network sends messages with the forward explicit congestion notification (FECN) or backwards explicit congestion notification (BECN), if there is congestion. With some shaping methods, the traffic shaping adaptive mode takes advantage of these signals and adjusts the traffic descriptors. This approximates the rate to the available bandwidth along the path.

In QPM, you can configure the following types of shaping:

- Generic traffic shaping (GTS)—GTS shapes traffic by reducing outbound traffic flow to avoid congestion by constraining traffic to a particular bit rate using the token bucket mechanism.
- Frame relay traffic shaping (FRTS)—Lets you specify an average bandwidth size for Frame Relay virtual circuits (VC), defining an average rate commitment for the VC. FRTS uses a buffer to hold packets while it transmits the flow at the specified committed information rate (CIR). You can also define a burst size and an exceed burst size to further model the flow. These values define how much data FRTS can send from the buffer per time interval. After the buffer is full, packets are dropped.

  FRTS supports adaptive shaping. When congestion occurs, the default minimum CIR (minCIR) is used, which is half of the CIR. QPM allows you to override this default by specifying a minimum rate to be used when there is congestion.
- Distributed traffic shaping (DTS)—DTS supports all functionality provided by both GTS and FRTS. DTS uses queues to buffer traffic surges that can congest a network. Data is buffered and then sent into the network at a regulated rate. This ensures that traffic will behave according to the configured descriptor, as defined by the Committed Information Rate (CIR), Committed Burst (Bc), and Excess Burst (Be). DTS provides two types of shape commands—average and peak. DTS supports adaptive shaping.
- Modular shaping—Operates on all traffic flows on an interface. This type of shaping uses DTS on versatile interface processor (VIP) interfaces, or GTS on other types of interfaces. Modular traffic shaping can be used on VIP interfaces on devices that do not support FRTS.

Related Topics

- Traffic Policing for Limiting Bandwidth and Marking Traffic, page 2-6

Queuing Techniques for Congestion Management for Outbound Traffic

You can set a queuing technique on a device's interface to manage how packets are queued to be sent through the interface. Some queuing techniques use the packet marking, while others ignore them.

Queuing techniques are primarily used for managing traffic congestion on an interface, that is, they determine the priority in which to send packets when there is more data than can be sent immediately:

Class-Based QoS Queuing: Multiple-Action, Class-Based Policies

On devices with IOS software versions that support modular QoS CLI (MQC), you can create multiple-action, class-based QoS policies, including a class-based QoS queuing policy. If class-based QoS is available for an interface, Cisco recommends that you use it instead of other scheduling methods.

Class-based QoS queuing uses WFQ processing to give higher weight to high priority traffic, but derives that weight from classes that you create. These classes are similar to custom queues—they are policy-based, identify traffic based on the traffic's characteristics (protocol, source, destination, and so forth), and allocate a percentage of the interface's bandwidth to the traffic flow.

With class-based QoS queuing, you can create up to 64 classes for an interface. (Unlike WFQ, queues are not automatically based on the packet's ToS value.) Class-based QoS queuing also lets you control the drop mechanism used when congestion occurs on the interface. You can use WRED for the drop mechanism, and configure the WRED queues, to ensure that high-priority packets within a class are given the appropriate weight. If you use tail drop, all packets within a class are treated equally, even if the ToS values are not equal.

An effective use of class-based QoS queuing would be to guarantee bandwidth to a few critical applications to ensure reliable application performance.

The queues you define constitute a minimum bandwidth allocation for the specified flow. If more bandwidth is available on the interface due to a light load, a queue can use the extra bandwidth. This is handled dynamically by the device.

Unclassified packets that do not match any filters defined for class-based policies are processed according to the settings in the default class. The default behavior for unclassified traffic is weighted fair queuing.

If you use WRED as the drop mechanism for a class, WRED automatically considers the packet's ToS value when determining which packet to drop. Tail drop does not consider a packet's ToS value.

If you use WFQ on the default class policy, WFQ automatically considers the packet's ToS value when queuing, dropping, and sending packets in the default queues.

Class-based QoS can be used with additional QoS capabilities to enable efficient management of voice and other real-time traffic.

- Traffic Shaping for Controlling Bandwidth, page 2-8
- Low Latency Queuing (LLQ): Strict Priority Queuing, page 2-24

- IP RTP Priority: Providing Strict Priority to Voice Traffic, page 2-24
- Link Fragmentation and Interleaving (LFI): Reducing Delay and Jitter on Lower Speed Links, page 2-25
- Compressed Real-Time Protocol (CRTP): RTP Header Compression to Reduce Delay, page 2-26
- Frame Relay Fragmentation (FRF): Preventing Delay on Frame Relay Links, page 2-26

Related Topics

- Management of Voice and Other Real-Time Traffic, page 2-23
- Distributed Weighted Fair Queuing (DWFQ): High Speed WFQ for VIP Interfaces, page 2-12
- Fair Queuing (FQ): Flow-Based Queuing, page 2-13
- First In, First Out (FIFO) Queuing: Basic Store and Forward on Routers, page 2-17
- Priority Queuing (PQ): Basic Traffic Prioritization on Routers, page 2-14
- Custom Queuing (CQ): Advanced Traffic Prioritization on Routers, page 2-15
- Weighted Fair Queuing (WFQ): Intelligent Traffic Prioritization on Routers, page 2-16

Distributed Weighted Fair Queuing (DWFQ): High Speed WFQ for VIP Interfaces

On devices with IOS software versions that do not support class-based QoS, class-based queuing features are implemented through distributed WFQ (DWFQ).

With DWFQ, packets are assigned to different queues based on their QoS group or the IP precedence in the ToS field. QoS groups allow you to customize your QoS policy. A QoS group is an internal classification of packets used by the router to determine how packets are treated by certain QoS features, such as DWFQ and committed access rate (CAR).

Like class-based QoS queuing, DWFQ uses WFQ processing to give higher weight to high priority traffic, but derives that weight from classes that you create. These classes are similar to custom queues—they are policy-based, identify traffic based on the traffic's characteristics (protocol, source, destination, and so forth), and allocate a percentage of the interface's bandwidth to the traffic flow.

An effective use of DWFQ would be to guarantee bandwidth to a few critical applications to ensure reliable application performance.

QPM does not support ToS-based DWFQ.

Related Topics

- Class-Based QoS Queuing: Multiple-Action, Class-Based Policies, page 2-11
- Fair Queuing (FQ): Flow-Based Queuing, page 2-13
- First In, First Out (FIFO) Queuing: Basic Store and Forward on Routers, page 2-17
- Priority Queuing (PQ): Basic Traffic Prioritization on Routers, page 2-14
- Custom Queuing (CQ): Advanced Traffic Prioritization on Routers, page 2-15
- Weighted Fair Queuing (WFQ): Intelligent Traffic Prioritization on Routers, page 2-16

Fair Queuing (FQ): Flow-Based Queuing

Fair queuing gives all packets an equal weight, and all queues are allocated equal bandwidth.

With FQ, packets are classified by flow. Packets with the same source IP address, destination IP address, source TCP or User Datagram Protocol (UDP) port, destination TCP or UDP port, protocol, and ToS field belong to the same flow. (All non-IP packets are treated as flow 0.) Each flow corresponds to a separate output queue. When a packet is assigned to a flow, it is placed in the queue for that flow.

Related Topics

- Class-Based QoS Queuing: Multiple-Action, Class-Based Policies, page 2-11
- Distributed Weighted Fair Queuing (DWFQ): High Speed WFQ for VIP Interfaces, page 2-12
- First In, First Out (FIFO) Queuing: Basic Store and Forward on Routers, page 2-17
- Priority Queuing (PQ): Basic Traffic Prioritization on Routers, page 2-14

- Custom Queuing (CQ): Advanced Traffic Prioritization on Routers, page 2-15
- Weighted Fair Queuing (WFQ): Intelligent Traffic Prioritization on Routers, page 2-16

Priority Queuing (PQ): Basic Traffic Prioritization on Routers

Priority queuing (PQ) is a rigid traffic prioritization scheme: if packet A has a higher priority than packet B, packet A always goes through the interface before packet B.

An effective use of priority queuing would be for placing time-critical but low-bandwidth traffic in the high queue. This ensures that this traffic is transmitted immediately, but because of the low-bandwidth requirement, lower queues are unlikely to be starved.

The disadvantage of priority queuing is that the higher queue is given absolute precedence over lower queues. For example, packets in the low queue are only sent when the high, medium, and normal queues are completely empty. If a queue is always full, the lower-priority queues are never serviced. They fill up and packets are lost. Thus, one particular kind of network traffic can come to dominate a priority queuing interface.

Packets that do not match any filter are placed in the normal queue.

Related Topics

- Class-Based QoS Queuing: Multiple-Action, Class-Based Policies, page 2-11
- Distributed Weighted Fair Queuing (DWFQ): High Speed WFQ for VIP Interfaces, page 2-12
- Fair Queuing (FQ): Flow-Based Queuing, page 2-13
- First In, First Out (FIFO) Queuing: Basic Store and Forward on Routers, page 2-17
- Custom Queuing (CQ): Advanced Traffic Prioritization on Routers, page 2-15
- Weighted Fair Queuing (WFQ): Intelligent Traffic Prioritization on Routers, page 2-16

Custom Queuing (CQ): Advanced Traffic Prioritization on Routers

Custom queuing (CQ) is a flexible traffic prioritization scheme that allocates a minimum bandwidth to specified types of traffic. You can create up to 16 of these custom queues.

For custom queue interfaces, the device services the queues in a round robin fashion, sending out packets from a queue until the byte count on the queue is met, then moving on to the next queue. This ensures that no queue gets starved, in comparison to priority queuing.

An effective use of custom queuing would be to guarantee bandwidth to a few critical applications to ensure reliable application performance.

The custom queues you define constitute a minimum bandwidth allocation for the specified flow. If more bandwidth is available on the interface due to a light load, a queue can use the extra bandwidth. This is handled dynamically by the device.

If you do not create queuing policies for a Custom Queuing interface, all traffic is placed in a single queue (the default queue), and is processed first in, first out, in the same manner as a FIFO queuing interface.

Related Topics

- Class-Based QoS Queuing: Multiple-Action, Class-Based Policies, page 2-11
- Distributed Weighted Fair Queuing (DWFQ): High Speed WFQ for VIP Interfaces, page 2-12
- Fair Queuing (FQ): Flow-Based Queuing, page 2-13
- First In, First Out (FIFO) Queuing: Basic Store and Forward on Routers, page 2-17
- Priority Queuing (PQ): Basic Traffic Prioritization on Routers, page 2-14
- Weighted Fair Queuing (WFQ): Intelligent Traffic Prioritization on Routers, page 2-16

Weighted Fair Queuing (WFQ): Intelligent Traffic Prioritization on Routers

Weighted fair queuing (WFQ) acknowledges and uses a packet's priority without starving low-priority packets for bandwidth. Weighted fair queuing divides packets into two classes: interactive traffic is placed at the front of the queue to reduce response time; noninteractive traffic shares the remaining bandwidth proportionately.

Because interactive traffic is typically low-bandwidth, its higher priority does not starve the remaining traffic. A complex algorithm is used to determine the amount of bandwidth assigned to each traffic flow. Packet marking is considered when making this determination.

Weighted fair queuing is very efficient and requires little configuration. To implement weighted fair queuing, you define Weighted Fair Queuing for the interface. You do not need to define queuing policies because WFQ automatically prioritizes the packets according to their IP precedence or DSCP value.

When you apply WFQ automatically, consider marking all traffic that enters the device (or mark the traffic at the point where it enters your network, to ensure that packets receive the service level you intend. Otherwise, the originator of the traffic, or another network device along the traffic's path, determines the service level for the traffic.

Related Topics

- Class-Based QoS Queuing: Multiple-Action, Class-Based Policies, page 2-11
- Distributed Weighted Fair Queuing (DWFQ): High Speed WFQ for VIP Interfaces, page 2-12
- Fair Queuing (FQ): Flow-Based Queuing, page 2-13
- First In, First Out (FIFO) Queuing: Basic Store and Forward on Routers, page 2-17
- Priority Queuing (PQ): Basic Traffic Prioritization on Routers, page 2-14
- Custom Queuing (CQ): Advanced Traffic Prioritization on Routers, page 2-15

First In, First Out (FIFO) Queuing: Basic Store and Forward on Routers

First In, First Out (FIFO) queuing is the basic queuing technique. In FIFO queuing, packets are queued on a first come, first served basis: if packet A arrives at the interface before packet B, packet A leaves the interface before packet B. This is true even if packet B has a higher IP precedence than packet A since FIFO queuing ignores packet characteristics.

FIFO queuing works well on uncongested high-capacity interfaces that have minimal delay, or when you do not want to differentiate services for packets traveling through the device.

The disadvantage of FIFO queuing is that when a station starts a file transfer, it can consume all the bandwidth of a link to the detriment of interactive sessions. This phenomenon is referred to as a *packet train* because one source sends a "train" of packets to its destination and packets from other stations get caught behind the train.

You do not need to define any queuing parameters for FIFO queuing.

Related Topics

- Class-Based QoS Queuing: Multiple-Action, Class-Based Policies, page 2-11
- Distributed Weighted Fair Queuing (DWFQ): High Speed WFQ for VIP Interfaces, page 2-12
- Fair Queuing (FQ): Flow-Based Queuing, page 2-13
- Priority Queuing (PQ): Basic Traffic Prioritization on Routers, page 2-14
- Custom Queuing (CQ): Advanced Traffic Prioritization on Routers, page 2-15
- Weighted Fair Queuing (WFQ): Intelligent Traffic Prioritization on Routers, page 2-16

Weighted Round Robin (WRR): Managing Layer 3 Switch Congestion

Weighted round robin (WRR) scheduling is used on layer 3 switches. WRR queuing is handled differently on the Catalyst 8500 family and on other layer 3 switches.

Weighted round robin (WRR) scheduling is used automatically on layer 3 switches on egress ports to manage the queuing and sending of packets. WRR places a packet in one of four queues based on the packet's IP precedence, from which it derives a delay priority. Table 2-1 shows the queue assignments based on the IP precedence value and derived delay priority of the packet, and the weight of the queue if you do not change it.

Table 2-1 WRR Queue Packet Assignments

IP Precedence	Delay Priority	Queue Assignment	Default Queue Weight (Catalyst 8500)	Default Queue Weight (Other Layer 3 Switches)
0, 1	0	0	1	1
2, 3	1	1	2	2
4, 5	2	2[1]	4	3
6, 7	3	3	8	4

1. Queue 2 is the queue typically used for voice traffic.

With WRR, each queue is given a weight. This weight is used when congestion occurs on the port to give weighted priority to high-priority traffic without starving low priority traffic. The weights provide the queues with an implied bandwidth for the traffic on the queue. The higher the weight, the greater the implied bandwidth. The queues are not assigned specific bandwidth, however, and when the port is not congested, all queues are treated equally.

Devices that use WRR automatically create the four queues with default weights for each interface. You need only define policies if you want to change the queue weights. For the Catalyst 8500, these policies are assigned to the device. For other layer 3 switches, policies are assigned to the destination ports.

Managing Congestion on Switch Ports

Queuing methods on switch ports use a packet's precedence setting to determine how that packet is serviced on the port. The queuing methods use multiple queues of different priority, with one or more thresholds for each queue, to determine the bandwidth allowed for traffic based on each Class of Service (CoS) value.

These queues and thresholds are serviced using weighted round robin (WRR) techniques to ensure a fair chance of transmission to each class of traffic. These queuing methods favor high-priority traffic without starving low-priority traffic.

QPM supports the following queuing methods for switch ports:

- 2 Queues, 2 Thresholds (2Q2T), page 2-19
- 1 Priority Queue, and 2 Queues 2 Thresholds (1P2Q2T), page 2-20
- 2 Queues, 1 Threshold (2Q1T), page 2-20
- 4 Queues, I Threshold (4Q1T), page 2-20
- 4 Queues, 2 Thresholds (4Q2T), page 2-21

2 Queues, 2 Thresholds (2Q2T)

2Q2T queuing uses two queues, one high priority, the other low priority, with two thresholds for each queue, to determine the bandwidth allowed for traffic based on each Class of Service (CoS) value. 2Q2T assigns each precedence to a specific queue and threshold on that queue.

For example, packets with CoS value of 0 (the lowest priority) are placed in the low priority queue and use the lower threshold by default. This ensures that the least important traffic gets less service than any other traffic.

2Q2T queuing comes with a default configuration for the queues, thresholds, and traffic assignments based on CoS settings. You can change this configuration if it does not suit your requirements. You can change the size of the queues, their relative WRR weights, the sizes of their thresholds, and the assignment of precedence values to the appropriate queue and threshold. You do not need to define queuing policies for ports with 2Q2T queuing.

1 Priority Queue, and 2 Queues 2 Thresholds (1P2Q2T)

1P2Q2T queuing uses three queues:

- One strict priority queue, usually used for voice traffic
- One high priority queue with two thresholds
- One low priority queue with two thresholds

1P2Q2T assigns each precedence to a specific queue and threshold on that queue.

You can mark voice traffic so that it will be assigned to the strict priority queue. On 1P2Q2T interfaces, the switch services traffic in the strict priority queue before servicing the standard queues. When the switch is servicing a standard queue, after transmitting a packet, it checks for traffic in the strict priority queue. If the switch detects traffic in the strict priority queue, it suspends its service of the standard queue and completes service of all traffic in the strict priority queue before returning to the standard queue.

2 Queues, 1 Threshold (2Q1T)

2Q1T queuing uses two queues, with one threshold for each queue. Each pair of CoS values is associated with either queue 1 or queue 2. For each pair of CoS values, you can define the queue to which packets with those CoS values will be directed.

4 Queues, I Threshold (4Q1T)

4Q1T queuing uses four queues, with one threshold for each queue, to determine the bandwidth allowed for traffic based on each Class of Service (CoS) value.

4Q1T queuing comes with a default configuration for the queues, and traffic assignments based on CoS settings. You can change this configuration if it does not suit your requirements. You can change the relative WRR weights of the queues, and the assignment of precedence values to the appropriate queue and threshold. You do not need to define queuing policies for ports with 4Q1T queuing.

4 Queues, 2 Thresholds (4Q2T)

4Q2T queuing uses four queues, with two thresholds for each queue, to determine the bandwidth allowed for traffic based on each Class of Service (CoS) value. 4Q2T assigns each precedence to a specific queue and threshold on that queue.

4Q2T queuing comes with a default configuration for the queues, thresholds, and traffic assignments based on CoS settings. You can change this configuration if it does not suit your requirements. You can change the size of the queues, their relative WRR weights, the sizes of their thresholds, and the assignment of precedence values to the appropriate queue and threshold. You can also choose the drop method for each queue. You do not need to define queuing policies for ports with 4Q2T queuing.

You can define Queue 4 as a strict priority queue, which transmits traffic whenever it is detected.

Queuing Techniques for Congestion Avoidance on Outbound Traffic

Weighted random early detection (WRED) is a queuing technique for congestion avoidance, meaning, it manages how packets are handled when an interface starts to be congested.

With WRED, when traffic begins to exceed the interface's traffic thresholds, but before congestion occurs, the interface starts dropping packets from selected flows. If the dropped packets are TCP, the TCP source recognizes that packets are getting dropped, and lowers its transmission rate. The lowered transmission rate then reduces the traffic to the interface, thus avoiding congestion. Because TCP retransmits dropped packets, no actual data loss occurs.

WRED drops packets according to the following criteria:

- RSVP flows are given precedence over non-RSVP flows, to ensure that time-critical packets are transmitted as required.
- The IP precedence or DSCP value of the packets. Packets with higher precedence are less likely to be dropped. You can control how WRED determines when and how often to drop packets based on precedence value if you are not satisfied with the default settings.
- The amount of bandwidth used by the traffic flow. Flows that use the most bandwidth are more likely to have packets dropped.

- The weight factor you have defined for the interface determines how frequently packets are dropped.

WRED chooses the packets to drop after considering these factors in combination, the net result being that the highest priority and lowest bandwidth traffic is preserved.

WRED differs from standard random early detection (RED) in that RED ignores IP precedence, and instead drops packets from all traffic flows, not selecting low precedence or high bandwidth flows.

By selectively dropping packets before congestion occurs, WRED prevents an interface from getting flooded, necessitating a large number of dropped packets. This increases the overall bandwidth usage for the interface.

On devices with a versatile interface processor (VIP), when you configure an interface to use WRED, it automatically uses distributed WRED. Distributed WRED takes advantage of the VIP.

An effective use of weighted random early detection would be to avoid congestion on a predominantly TCP/IP network, one that has minimal UDP traffic and no significant traffic from other networking protocols. It is especially effective on core devices rather than edge devices, because the traffic marking you perform on edge devices can then affect the WRED interfaces throughout the network.

The disadvantage of WRED is that only predominantly TCP/IP networks can benefit. Other protocols, such as UDP or NetWare (IPX), do not respond to dropped packets by lowering their transmission rates, instead retransmitting the packets at the same rate. WRED treats all non-TCP/IP packets as having precedence 0. If you have a mixed network, WRED might not be the best choice for queuing traffic.

Weighted random early detection interfaces automatically favor high priority, low bandwidth traffic flows. No specific policies are needed. However, because WRED automatically uses the IP precedence settings in packets, consider marking all traffic that enters the device (or mark the traffic at the point where it enters your network). By marking all traffic, you can ensure that packets receive the service level you intend. Otherwise, the originator of the traffic, or another network device along the traffic's path, determines the service level for the traffic.

You can also create class-based QoS policies that use WRED as the drop mechanism for the class-based queues.

Related Topics

- Class-Based QoS Queuing: Multiple-Action, Class-Based Policies, page 2-11

Management of Voice and Other Real-Time Traffic

Real-time-based applications, such as voice applications, have different characteristics and requirements from those of other data applications. Voice applications tolerate minimal variation in the amount of delay affecting delivery of their voice packets. Voice traffic is also intolerant of packet loss and jitter, both of which degrade the quality of the voice transmission delivered to the recipient end user. To effectively transport voice traffic over IP, mechanisms are required that ensure reliable delivery of packets with low latency.

To simplify the process of defining end-to-end QoS for voice traffic, QPM provides you with a voice application. This includes a wizard, which guides you through the process of defining your IP network topology, and then automatically creates the required QoS configuration at each relevant network point. QPM also includes predefined IP telephony templates, which contain the QoS configurations and policies required at each relevant point in the network. All you must do is add your devices to the device inventory, assign their interfaces to the relevant policy groups, and deploy. For detailed information, see Chapter 5, "Configuring QoS for IP Telephony."

The following features can be used to manage voice traffic:

- Low Latency Queuing (LLQ): Strict Priority Queuing, page 2-24
- IP RTP Priority: Providing Strict Priority to Voice Traffic, page 2-24
- Link Fragmentation and Interleaving (LFI): Reducing Delay and Jitter on Lower Speed Links, page 2-25
- Compressed Real-Time Protocol (CRTP): RTP Header Compression to Reduce Delay, page 2-26
- Frame Relay Fragmentation (FRF): Preventing Delay on Frame Relay Links, page 2-26

On Catalyst switches, the following is available for management of voice traffic:

- 1 Priority Queue, and 2 Queues 2 Thresholds (1P2Q2T), page 2-20
- 4 Queues, 2 Thresholds (4Q2T), page 2-21

Low Latency Queuing (LLQ): Strict Priority Queuing

Low latency queuing (LLQ) is used with class-based QoS for strict priority queuing. Strict priority queuing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic. LLQ is not limited to UDP port numbers, as is IP RTP priority.

Using LLQ reduces delay and jitter in voice conversations. LLQ is enabled when you configure the priority status in a class-based QoS queuing policy. When several types of traffic on an interface are configured as priority classes, all these types of traffic are enqueued to the same, single, strict priority queue.

Related Topics

- Class-Based QoS Queuing: Multiple-Action, Class-Based Policies, page 2-11

IP RTP Priority: Providing Strict Priority to Voice Traffic

IP RTP Priority creates a strict priority queue for real-time transport protocol (RTP) traffic. The IP RTP Priority queue is emptied before other queues are serviced. This is typically used to provide absolute priority to voice traffic, which uses RTP ports. Because voice traffic is delay-sensitive and low bandwidth, you can typically give it absolute priority without starving other data traffic. This ensures that voice quality is adequate.

IP RTP Priority is especially useful on slow-speed WAN links, including Frame Relay, Multilink PPP (MLP), and T1 ATM links. It works with WFQ and class-based QoS. For class-based QoS interfaces, you can configure custom class-based queues for other types of traffic. The bandwidth allocated to the IP RTP Priority queue counts as part of the total allocated class-based QoS queue bandwidth. IP RTP priority cannot be configured on the interface when FRTS is enabled. IP RTP priority is not available on VIP cards.

IP RTP Priority ignores compression, treating a compressed 12 kbps flow as a 24 kbps flow.

Related Topics

- Weighted Fair Queuing (WFQ): Intelligent Traffic Prioritization on Routers, page 2-16
- Class-Based QoS Queuing: Multiple-Action, Class-Based Policies, page 2-11

Link Fragmentation and Interleaving (LFI): Reducing Delay and Jitter on Lower Speed Links

Voice over IP is susceptible to increased latency and jitter when the network processes large packets, such as LAN-to-LAN FTP Telnet transfers traversing a WAN link. This susceptibility increases as the traffic is queued on slower links. LFI was designed especially for lower-speed links in which serialization delay is significant.

LFI reduces delay and jitter on slower speed links by breaking up large data packets so that they are small enough to satisfy the delay requirements of real-time traffic. The low-delay traffic packets, such as voice packets, are interleaved with the fragmented packets. LFI also provides a special transmit queue for the smaller, delay-sensitive packets, enabling them to be sent earlier than other flows.

QPM cannot detect or implement MLP and will assume that the multilink PPP command is enabled on the interface. QPM will configure only the interleave and fragmentation commands. When LFI is defined on an interface group, it is only deployed to the interfaces that support it.

Related Topics

- Compressed Real-Time Protocol (CRTP): RTP Header Compression to Reduce Delay, page 2-26

Compressed Real-Time Protocol (CRTP): RTP Header Compression to Reduce Delay

Real-Time Protocol (RTP) is a host-to-host protocol used for carrying multimedia application traffic, including packetized audio and video, over an IP network. RTP provides end-to-end network transport functions intended for applications sending real-time requirements, such as audio and video.

To avoid the unnecessary consumption of available bandwidth, CRTP, the RTP header compression feature, is used on a link-by-link basis. CRTP compresses the IP/UDP/RTP header in an RTP data packet from 40 bytes to approximately 2 to 5 bytes resulting in decreased consumption of available bandwidth for voice traffic. A corresponding reduction in delay is realized.

Related Topics

- Link Fragmentation and Interleaving (LFI): Reducing Delay and Jitter on Lower Speed Links, page 2-25

Frame Relay Fragmentation (FRF): Preventing Delay on Frame Relay Links

Frame Relay fragmentation (FRF) ensures predictability for voice traffic, by aiming to provide better throughput on low-speed Frame Relay links. FRF allows long data frames on one virtual circuit (VC) to be fragmented into smaller pieces and interleaved with delay-sensitive voice traffic on another VC utilizing the same interface. In this way, real-time voice and non-real-time data frames can be carried together on lower-speed links without causing excessive delay to the real-time traffic.

VoIP packets should not be fragmented. However, VoIP packets can be interleaved with fragmented packets. If some PVCs are carrying voice traffic, you can enable fragmentation on all PVCs. The fragmentation header is only included for frames that are greater than the fragment size configured.

Managing Traffic Through Access Control

You can control traffic access by permitting or denying transport of packets into or out of interfaces.

You can define access control policies, which will deny or permit traffic that matches the filter definition in the specified direction. You can also define a filter condition to deny specific types of traffic as part of a QoS policy definition.

The access control feature can be used as a security feature, and can be enabled or disabled globally for all databases in your system. You can overwrite the global configuration on a per-domain or per-device basis.

You cannot create Access Control policies for the Cisco 8500 family of devices or for Catalyst switches.

Signaling Techniques

To implement end-to-end quality of service, a traffic flow must contain or use some type of signal to identify the requirements of the traffic. With QPM, you can control these types of signaling techniques:

- IP Precedence and DSCP Values: Differentiated Services, page 2-27
- Resource Reservation Protocol (RSVP): Guaranteed Services, page 2-28

IP Precedence and DSCP Values: Differentiated Services

The simplest form of signal is the IP precedence or DSCP setting in data packets: the packet's color or classification.

This signal is carried with the packet, and can affect the packet's handling at each node in the network. Queuing techniques such as WFQ and WRED automatically use this signal to provide differentiated services to high-priority traffic.

To use the IP precedence or DSCP setting effectively, ensure that you mark traffic at the edges of your network so that the marking affects the packet's handling throughout the network. See Packet Marking, page 2-5, for information on how to change a packet's IP precedence or DSCP setting.

IP precedence and DSCP can only provide differentiated services on interfaces that use a queuing technique that is sensitive to the precedence setting in the packet. For example, WFQ, WRED, WRR, 1P2Q2T, and 2Q2T automatically consider the precedence settings.

Related Topics

- Packet Marking, page 2-5
- Queuing Techniques for Congestion Management for Outbound Traffic, page 2-10
- Queuing Techniques for Congestion Avoidance on Outbound Traffic, page 2-21

Resource Reservation Protocol (RSVP): Guaranteed Services

A more sophisticated form of signaling than IP precedence is the resource reservation protocol (RSVP). RSVP is used by applications to dynamically request specific bandwidth resources from each device along the traffic flow's route to its destinations. After the reservations are made, the application can start the traffic flow with the assurance that the required resources are available.

RSVP is mainly used by applications that produce real-time traffic, such as voice, video, and audio. Unlike standard data traffic, such as HTTP, FTP, or Telnet, real-time applications are delay sensitive, and can become unusable if too many packets are dropped from a traffic flow. RSVP helps the application ensure there is sufficient bandwidth so that jitter, delay, and packet drop can be avoided.

RSVP is typically used by multicast applications. With multicasting, an application sends a stream of traffic to several destinations. For example, the Cisco IP/TV application can provide several audio-video programs to users. If a user accesses one of the provided programs, IP/TV sends a stream of video and audio to the user's computer.

Network devices consolidate multicast traffic to reduce bandwidth usage. Thus, if there are ten users for a traffic flow behind a router, the router sees one traffic flow, not ten. In unicast traffic, the router sees ten traffic flows. Although RSVP can work with unicast traffic (one sender, one destination), RSVP unicast flows can quickly use up RSVP resources on the network devices if a lot of users access unicast applications. In other words, unicast traffic scales poorly.

To configure RSVP on network devices, you must determine the bandwidth requirements of the RSVP-enabled applications on your network. If you do not configure the devices to allow RSVP to reserve enough bandwidth, the applications will perform poorly. See the documentation for the applications to determine their bandwidth requirements.

When an RSVP request is made, RSVP calculates the bandwidth request by considering the mean data rate, the amount of data the interface can hold in the queue, and the minimum QoS requirement for the traffic flow. The interface determines if it can meet the request, and replies to the requesting application.

When the traffic flow begins, RSVP can dynamically respond to changes in routes, switching reservations to new devices and releasing reservations for devices no longer on the path. After the flow is complete, all reservations are removed and the bandwidth on the interfaces released.

RSVP with WFQ or class-based QoS provides guaranteed rate service, providing an absolute rate even during congestion events. This is good for delay-sensitive real-time applications like voice over IP.

RSVP with WRED provides controlled load service, providing low delay and high throughput during congestion events. This is good for adaptive real-time applications such as the playback of a recorded conference call. With WRED advanced properties, you can control the WRED thresholds for RSVP traffic.

Related Topics

- Weighted Fair Queuing (WFQ): Intelligent Traffic Prioritization on Routers, page 2-16
- Class-Based QoS Queuing: Multiple-Action, Class-Based Policies, page 2-11
- Queuing Techniques for Congestion Avoidance on Outbound Traffic, page 2-21

More Information About Quality of Service

This publication cannot cover everything you might want to know about quality of service. This section provides pointers to more information available on the web.

For pages that require a cisco.com login, you can register at the cisco.com web site at:

http://www.cisco.com/register/.

The references are broken down into the following categories:

General QoS Information

- **Cisco IOS Quality of Service**—Links to QoS resources including white papers:

  http://www.cisco.com/warp/customer/732/Tech/qos/

- **Cisco IOS Enabling Network Services: QoS Services**—QoS overview with links to white papers on all major QoS technologies:

  http://www.cisco.com/warp/customer/732/net_enabled/qos.html

- **Quality of Service (Internetworking Technology Overview)**—Detailed overview of QoS capabilities:

  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm

Voice over IP Information

- **IP Telephony QoS Design Guide**—Provides a blueprint for implementing the end-to-end Quality of Service (QoS) that is required for successful deployment of Cisco AVVID solutions in today's enterprise environment:

  http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/avvidqos/index.htm

- **Quality of Service for Voice over IP**—Information on QoS methods for voice over IP:

  http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/qossol/qosvoip.htm

IOS Software Release 12.x Documentation

- **QoS Solutions Configuration Guide**—Includes information on QoS mechanisms supported by IOS 12.2:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/index.htm

- **QoS Solutions Configuration Reference**—Commands for configuring QoS:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_r/index.htm

- **Wide-Area Networking Configuration Guide**—Includes information on FRTS:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/index.htm

- **New Features in IOS 12.2**—Includes information about the latest QoS methods supported by IOS 12.2:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/cgft14.htm

IOS Software Release 11.1cc Documentation

- **Committed Access Rate (CAR)**—For release 11.1cc:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/car.htm

- **Distributed WRED**—For release 11.1cc:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/wred.htm

- **Distributed WFQ**—For release 11.1cc:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/dwfq.htm

Catalyst Documentation

- **Catalyst 8500 Quality of Service Feature Summary**—Information on WRR:

  http://www.cisco.com/univercd/cc/td/doc/product/l3sw/8540/rel_12_0/w5_6f/softcnfg/5cfg8500.htm

- **Catalyst 4908 Quality of Service Feature Summary**—Information on WRR:

  http://www.cisco.com/univercd/cc/td/doc/product/l3sw/4908g_l3/ios_12/7w515d/config/qos_cnfg.htm

- **Configuring Quality of Service (Software Configuration Guide)**—For the Catalyst 5000 family, software release 6.3. Information on Catalyst classification:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_6_3/config/qos.htm

- **Configuring Quality of Service (Software Configuration Guide)**—For the Catalyst 6000 family, software release 6.3. Information on Catalyst classification, policing, and queuing methods:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_6_3/confg_gd/qos.htm

- **Configuring Quality of Service**—For the Catalyst 2950:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/1216ea2b/scg/swgqos.htm

- **Configuring Quality of Service**—For the Catalyst 3550:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/1219ea1/3550scg/swqos.htm

Getting Started

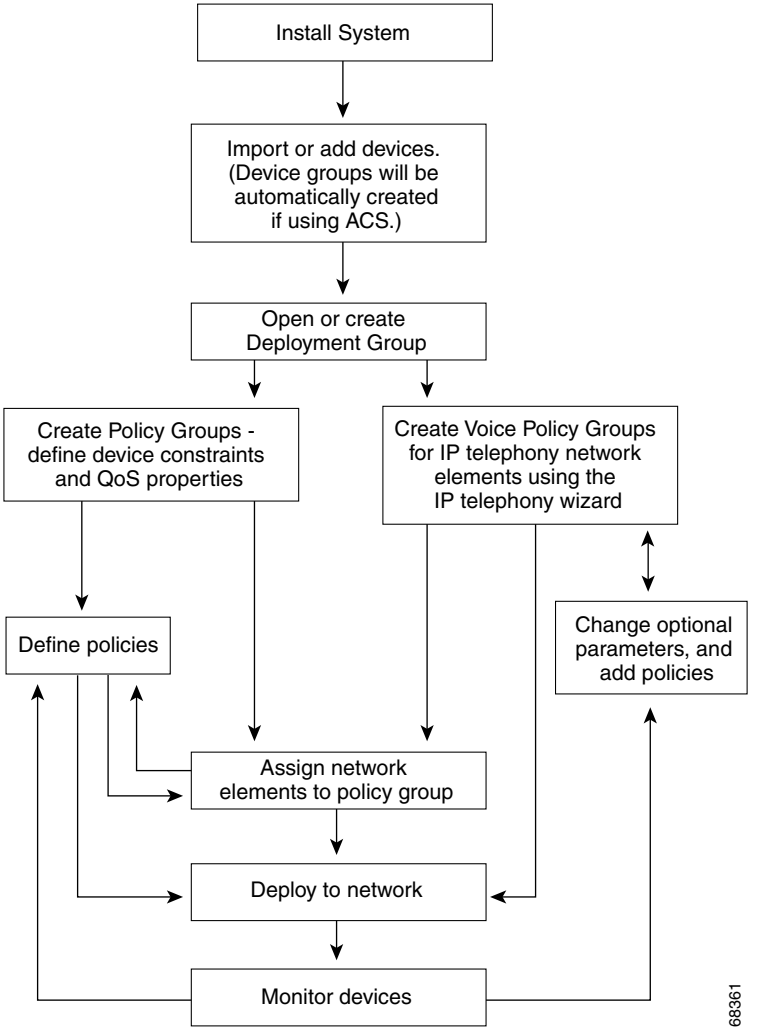
Before you begin to define your QoS policies, you should set up your QoS policy system.

The following topics describe how to start working with QPM.

Understanding the QPM Workflow

The QPM workflow is flexible and allows you to navigate between the QPM management applications. Figure 3-1 describes a common workflow for defining policies for data and IP telephony networks.

Figure 3-1 QPM Workflow



The main workflow tasks are:

- Installing QPM—QPM is installed over the Cisco Common Services application. See the *Installation Guide for QoS Policy Manager 3.0* for details.
- Adding and importing devices—You add and import devices into the QPM device inventory. You can add devices manually or from a CSV file, or you can import them directly from RME. See Chapter 4, "Managing Devices" for information about adding and importing devices.
- Open or create a deployment group—QPM QoS policies are defined within the framework of deployment groups. When you begin working with QPM, a default deployment group is automatically opened. You can create and manage multiple deployment groups for phased deployment, or for testing what-if scenarios. See Chapter 8, "Working with Deployment Groups" for more information.
- Create policy groups—Policy groups are constrained sets of QoS policies. You must define the device constraints and QoS properties for your policy groups before you can begin to define policies. See Chapter 6, "Working with Policy Groups and Policies" for information about defining policy groups. You can upload the existing QoS configuration on your devices into policy groups. See Uploading Device QoS Configurations to Policy Groups, page 6-16.
- Define policies—Policies contain filters and actions. The policy filter defines the traffic to which the policy actions will be applied. The policy actions can include marking, policing, queuing, and other traffic control techniques. (This step is optional, a policy group's properties will be deployed to the devices, even when there are no policies). See Chapter 6, "Working with Policy Groups and Policies" for information about defining policies.
- Assign network elements to policy group—You can assign network elements in the device inventory to a policy group. On deployment, the policy group's policies will be downloaded to the assigned network elements. You can assign network elements to policy groups before or after defining policies. See Chapter 6, "Working with Policy Groups and Policies" and Chapter 4, "Managing Devices" for information about assigning network elements to policy groups.
- Create voice policy groups for IP telephony networks—QPM provides an IP telephony wizard, which automatically creates the QoS policies required at each network point in your IP telephony network, according to the IP

telephony network topology that you define. The QoS policies are defined using voice policy group templates that follow the Cisco IP Telephony QoS Design Guide recommendations. See Chapter 5, "Configuring QoS for IP Telephony" for information about defining QoS for IP telephony networks.

- Deploy to network—After you have defined devices, policy groups, and policies, you can distribute the policies to devices in the network. See Chapter 7, "Deploying QoS Policies" for more information.
- Perform QoS Monitoring—After you have deployed your QoS configuration to the network, you can validate the effectiveness of your policies. Based on the monitoring results, you can refine your QoS policies to achieve optimum performance. See Chapter 9, "Using QoS Analysis" for more information.

Note You can use QoS monitoring, as a starting point for defining QoS policies, to profile traffic by critical applications, or DiffServ classes.

Related Topics

- Starting QPM, page 3-4

Starting QPM

QoS Policy Manager is accessed from the CiscoWorks2000 desktop.

Procedure

Step 1 In your web browser, start CiscoWorks. The default URL is http://<*QPMinstall*>:1741, where <*QPMinstall*> is the name of the computer with the QPM installation.

The CiscoWorks2000 desktop is displayed.

Note The first time you start CiscoWorks2000 on a CiscoWorks2000 server or a client machine, the Java Runtime Environment is automatically installed.

Note Verify on the front page that Java, JavaScript, and cookies are enabled. If they are not enabled, change your browser preferences to enable them, then continue to the next step.

Step 2 Log into CiscoWorks with your username and password.

The CiscoWorks navigation tree appears in the left pane.

Step 3 Click **QoS Policy Manager** in the navigation tree.

Step 4 Click **QPM** under the QoS Policy Manager drawer.

A Security Alert window opens. Click **Yes** to proceed.

QPM opens in a separate browser window.

Related Topics

- Working with the QPM User Interface, page 3-5
- User Permissions, page 3-11
- Exiting QPM, page 3-12
- Problems Starting QoS Policy Manager, page 11-3

Working with the QPM User Interface

The following topics familiarize you with the QPM user interface:

- Understanding the QPM User Interface, page 3-6
- Using QPM Tables, page 3-8
- Using QPM Wizards, page 3-10
- Working with Multiple Users, page 3-11

Related Topics

- Starting QPM, page 3-4
- Exiting QPM, page 3-12
- Troubleshooting User Interface Problems, page 11-4

Understanding the QPM User Interface

All the pages in the web-based QPM user interface have a consistent look and feel. Figure 3-2 shows an example of a QPM page.

Figure 3-2 Example of a QPM Page

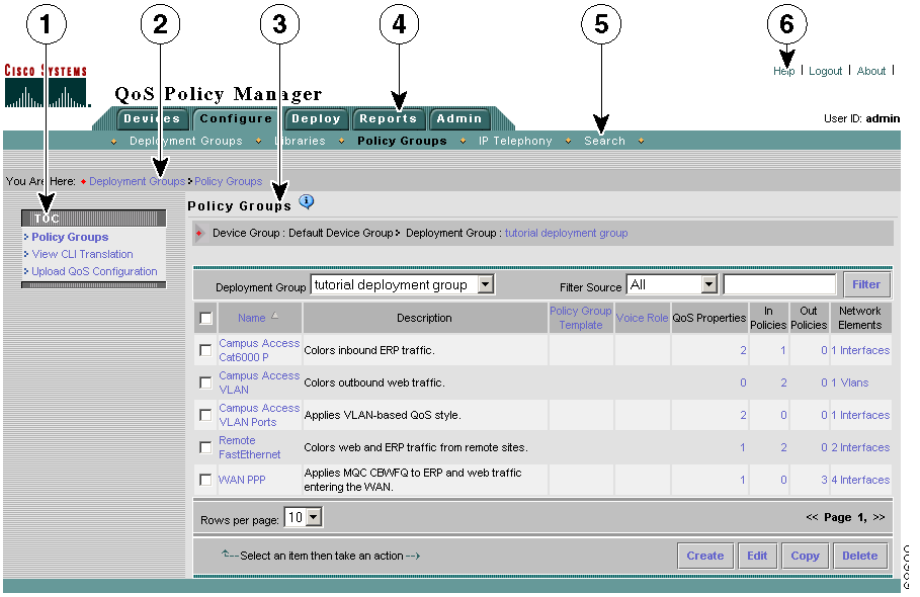


Table 3-1 describes the common elements in each page.

Table 3-1 Common GUI Elements in a QPM Page

Number	Area	Description
1	TOC	Provides up to two additional levels of navigation, if required: • A submenu for the selected option. • In a wizard context, this area displays the wizard steps.
2	Path bar	Provides a context for the displayed page. Indicates from which tab and option the current page is derived.
3	Content area	Displays the pages in which you perform application tasks.
4	QPM tabs	Contains tabs that provide access to QPM functionality. Click a tab to access its options: • Devices—Contains options for managing devices and device groups in the QPM inventory. • Configure—Contains options for defining policy groups and policies, and configuring QoS for IP telephony. This tab also includes options for working with global library policy components. • Deploy—Contains options for deploying QoS policies, and for previewing the CLI configuration on the devices. You can also view and restore previously deployed jobs through this tab. • Reports—Provides access to QPM reports, and to the Performance Analysis application. • Admin—Contains additional administration options.

Table 3-1 Common GUI Elements in a QPM Page (continued)

Number	Area	Description
5	Option bar	Displays the options available for the selected tab.
6	QPM banner	Contains the Help, Logout, and About buttons: • Click **Help** to open a window that displays context-sensitive help for the currently displayed page. The Help page also contains help contents, so that you can use this button to access any online help topic. • Click **Logout** to log out of QPM and close the QPM window. • Click **About** to display details about the version of the application.

Note It is not recommended to use the browser Back button to navigate in QPM.

Related Topics

- Using QPM Tables, page 3-8
- Using QPM Wizards, page 3-10
- Working with Multiple Users, page 3-11

Using QPM Tables

In QPM, lists of items are displayed in tables. A table consists of a table header with filtering criteria, column headers with the column titles, a table footer with the table action buttons, and one or more table pages containing the table contents.

In general, you must select a table item before you click an action button. (Some actions do not require any item selection, for example, creating a new item.)

When an action can apply to more than one item, for example, deleting items, you can select multiple items in a single page, and then click the action button. You can select all items in a table by selecting the check box in the column header row.

Note If you select items in a table page, and then attempt to open another table page without clicking an action button, a warning message appears.

You can change the table display in the following ways:

- Change the number of rows you want to appear on a table page. Select the number of rows in the Rows per page list box in the table footer. Select **All** to display all table rows in a single page.
- Display a subset of items using the Data Source list box in the table header. Choose a category in the Data Source list box. Items in the selected category only, are displayed.
- Display a subset of items using the filtering option in the table header:
  - Choose the item by which you want to filter in the Filter Source list box.
  - Enter the matching string in the field.
  - Click **Filter**.

  The filtering option operates on all pages in the table.
- Sort items in the entire table by clicking the column headers.

Related Topics

- Understanding the QPM User Interface, page 3-6
- Using QPM Wizards, page 3-10
- Working with Multiple Users, page 3-11

Using QPM Wizards

QPM wizards guide you through the steps required to complete configuration tasks in QPM.

Each step in a wizard can consist of one or more pages and dialog boxes. A step can also contain substeps. You can navigate through the wizard steps using either the Next and Back buttons, or the wizard navigation TOC in the left pane.

Note It is recommended not to use the browser Refresh button when working in a wizard. Using the browser Refresh button might result in loss of data.

When you open a wizard, some steps might be disabled depending on previous configurations you have made. As you progress through a wizard, some steps might become disabled depending on the choices you make in each step.

The configuration settings that you define in a wizard are saved only when you complete the wizard by clicking the Finish button. If you click the Cancel button in the wizard, or if you choose another QPM option while in the wizard, your wizard settings will not be saved.

Note In the IP Telephony wizard, new policy groups are saved when you complete each step.

Related Topics

- Understanding the QPM User Interface, page 3-6
- Using QPM Tables, page 3-8
- Working with Multiple Users, page 3-11

Working with Multiple Users

Multiple users can work with QPM at the same time. Whenever you save changes, for example, when you complete a wizard, or edit an item, QPM checks whether you are modifying the latest version of that item. An item might be a policy group, policy, global library item, and so on.

If you are not editing the latest version, meaning another user has saved changes to the item since you accessed it for editing, QPM displays a message informing you that you are not working with the latest version of the item, and will not let you save the changes. This mechanism prevents a user from unintentionally overwriting changes made by another user working at the same time.

Related Topics

- Understanding the QPM User Interface, page 3-6
- Using QPM Tables, page 3-8
- Using QPM Wizards, page 3-10

User Permissions

QPM can work with either Cisco Access Control Server (ACS) permissions or CiscoWorks permissions. QPM permissions for user authorization are mapped to CiscoWorks permission roles or ACS permissions as specified.

User permissions and authentications for QPM are handled by the Cisco Common Services application. Before you begin to work with QPM, you should ensure that you have the appropriate permissions. Verify your user permissions in the CiscoWorks2000 desktop (**Server Configuration > Setup > Security**), or in ACS (depending on the method you are using for user authentication).

See the *Installation Guide for QoS Policy Manager 3.0* for more information about user permissions.

Exiting QPM

When you finish working with QPM, you must log out of CiscoWorks to close the application.

Procedure

Step 1 Click **Logout** in any open QPM windows to close them.

Step 2 Click **Logout** in the CiscoWorks2000 desktop window.

The CiscoWorks session ends.

Managing Devices

The device inventory is a collection of information about the network elements that QPM can manage.

The following topics describe how to manage devices in QPM:

Understanding the Device Inventory

The device inventory is a collection of information about the network elements that QPM can manage. Network elements are devices and components of devices on which QoS can be configured. Examples of network elements include devices (routers, switches, and layer 3 switches), cards, interfaces, subinterfaces, and VLANs. For more information about network elements, see Working with Network Elements, page 4-25.

Using Device Folders To Organize Your Inventory

Device folders are groups of devices that you can create for organizational purposes, for example, to distinguish edge routers from core routers. For more information, see Working with Network Elements, page 4-25.

Using Device Groups

Device groups are groups of devices that are created and administered using ACS. You can use multiple device groups only if you use ACS to manage device access. For more information, see Working with Device Groups, page 4-34.

Default Device Group

The inventory always contains one device group named the default device group. If you are not using ACS device groups to group devices, your inventory will contain only the default device group.

The default device group (like all QPM device groups) has properties that are unique to QPM. You can edit some of these properties. For more information, see Editing Device Group Properties, page 4-37.

Communicating With Devices Using SSH

QPM can communicate with devices in the inventory using either Telnet or secure shell (SSH). SSH provides more security than Telnet because communication with SSH is encrypted and authenticated.

You must configure SSH on the device before QPM can communicate with it using SSH. When you configure SSH on devices, follow these guidelines:

- Configure a device public key size of 1024 bits or more.
- Define a username on the device.

Use one of the following methods to configure QPM to use SSH to communicate with a device:

- Select the Enable SSH check box in the Device Properties page to enable SSH communication with that device. For more information, see Viewing and Editing Device Properties, page 4-14.
- Select the Enable SSH check box in the Device Group Properties page to enable SSH communication as the default for a device group. For more information, see Editing Device Group Properties, page 4-37.

Adding Devices to the Device Inventory

To manage the QoS configuration on a device or any of its elements with QPM, you must first add it to the inventory. When you add a device to the inventory, QPM discovers the device on the network to obtain the properties that it stores about the device. Therefore, devices must be running and accessible on the network before you can add them to the inventory.

You can only add a device to the inventory if you have sufficient access permissions to it. The Import Devices Wizard shows you which devices you cannot import because of insufficient permissions.

When you add a device to the inventory, all of its network elements that QPM supports are automatically added. For more information about network elements, see Working with Network Elements, page 4-25.

Device Group Assignment

If you use ACS for user authentication, QPM assigns each imported device to the same QPM device group to which it is assigned in ACS. If a device is not assigned to an ACS device group, it is assigned to the QPM default device group.

If you are using CiscoWorks Common Services for user authentication, all devices you import are added to the QPM default device group.

OS Detection and IOS Mapping

QPM uses the device model type and operating system (OS) version number to load device capabilities to the inventory. All subversions of a certain version are translated to the major version, unless QPM explicitly supports the minor version. In QPM, new minor versions are mapped to the last supported minor version and not to the major version.

Both the device software version and the mapped software version are displayed in the Device Table page:

- OS Version—OS version that QPM detected.
- Mapped OS Version—OS version to which the detected OS version is mapped.

If QPM does not support an imported device's Cisco IOS version, the device is assigned the status "Unsupported," and no Mapped OS version is assigned to it. You cannot perform any tasks on devices that have the status Unsupported. If the

device model is supported by QPM but the Cisco IOS version is not, you can upgrade the device to a supported Cisco IOS version and then rediscover the device to make it available in QPM.

Device Model Discovery

If QPM does not support an imported device model, then the device is assigned the status "Unsupported" and the model appears as "Unknown" in the Device Table. You cannot perform any tasks on devices that have the status Unsupported. The device's interfaces are not discovered or imported.

Device System Name

You can add a device to the inventory by providing either its IP address or its DNS name (if it is registered in DNS). Whichever of these values you provide becomes the device's primary name in QPM.

If the device has a system name configured, it is detected when QPM discovers the device. The device system name is added to the Device Table, as another method for you to identify the device.

You cannot use device DNS names that contain the backslash (\) character.

Device Access Parameters

Device access parameters are the passwords and community strings that QPM needs to log into and configure devices. QPM obtains device access parameters for devices you add to the inventory in the following ways:

- When adding a device manually, you can either enter the device access parameters, or you can use the destination device group's default access parameters. To use default access parameters, leave the access parameters fields blank.
- When importing from a CSV file, QPM obtains each device's access parameters from the following sources, in this order:
  - The device's record in the CSV file.
  - The default access parameters configured in the CSV file.
  - The destination device group's default access parameters.
- When importing from RME, the device access parameters are taken from RME. If RME does not provide access parameters, the destination device group's default access parameters are used.

For more information about default device access parameters, see Configuring Default Device Access Parameters, page 4-12.

The following topics describe how to add devices to the inventory:

Adding a Single Device

To add a single device you enter the required device information, then QPM discovers the device on the network to obtain the rest of the device information.

Before You Begin

Obtain the following information for each device you are adding:

- DNS name of the device or IP address of the device or one of its interfaces.
- If you are not using the device group default access parameters to connect to the device, you must obtain the device access parameters necessary to connect to it.

For more information about default device access parameters, see Configuring Default Device Access Parameters, page 4-12.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select **Add Device** from the TOC. The Import Devices Wizard - General page appears.

Step 3 Do the following in the Import Devices Wizard - General page:

a. Select the Manual radio button.

b. Enter the device IP address in the Device IP field.

c. If you are not using the default device access parameters, enter the necessary device access parameters in the corresponding fields.

d. Click **Next**. The Import Devices Wizard - Select Devices page appears.

For more information about the Import Devices Wizard - General page, see Import Devices Wizard - General Page, page A-23.

Step 4 In the Import Devices Wizard - Select Devices page, select the check box next to the device you are adding, then click **Finish**.

The Discovery Status page appears, where you can monitor the progress of the add operation. For more information, see Viewing Device Discovery Status, page 4-13.

Related Topics

- Adding Devices to the Device Inventory, page 4-3
- Using QPM Tables, page 3-8
- Using QPM Wizards, page 3-10
- Troubleshooting Device Management Problems, page 11-5

Importing Devices from a Device Inventory CSV File

You can add multiple devices simultaneously to the inventory by importing them from a comma-separated value (CSV) device inventory file created using CiscoWorks2000 Resource Manager Essentials (RME).

During the import process, QPM presents a listing of QPM-supported devices in the CSV file. It does not include devices that are not supported by QPM. You select which devices to import.

You can import a particular device from a CSV file or directly from RME only once. After you import a device, you update its information and properties in QPM. QPM also tracks which devices you choose not to import from CSV files

and RME during the import process. If you re-import from a CSV file or RME again in the future, you can choose to import only those devices that have never been imported before.

When you import from a CSV file, QPM discovers all devices in the file.

QPM assigns access parameters to the devices based on the following sources:

- The CSV file.
- The QPM default access parameters. For more information about default access parameters, see Configuring Default Device Access Parameters, page 4-12.

Before You Begin

Export a device inventory CSV file using RME.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select **Add Device** from the TOC. The Import Devices Wizard - General page appears. For information about this page, see Import Devices Wizard - General Page, page A-23.

Step 3 Do the following in the Import Devices Wizard - General page:

a. Select the Import from CSV file radio button.

b. Enter the path to the CSV file in the File field, or click **Browse** to navigate to the file.

c. Select the Import only new RME devices check box to import only the devices that have not been previously imported from RME.

d. Click **Next**. The Import Devices Wizard - Select Devices page appears.

Step 4 In the Import Devices Wizard - Select Devices page, select the check boxes next to the devices you want to add, then click **Finish**.

The Discovery Status page appears, where you can monitor the progress of the add operation. For more information, see Viewing Device Discovery Status, page 4-13.

Tip Common causes of device discovery failure include incorrect Telnet or SNMP passwords, incorrect IP addresses, and unavailable devices.

Related Topics

- Adding Devices to the Device Inventory, page 4-3
- Using QPM Tables, page 3-8
- Using QPM Wizards, page 3-10
- Troubleshooting Device Management Problems, page 11-5

Importing Devices from RME

You can add multiple devices to the inventory by importing them from a supported release of Resource Manager Essentials (RME) directly, without saving the RME device inventory to a file.

During the import process, QPM presents a listing of QPM-supported devices in the RME inventory. It does not include devices that are not supported by QPM. You select which devices to import.

You can import a particular device from RME or a CSV file only once. After you import a device, you update its information and properties in QPM. QPM also tracks which devices you choose not to import from RME or CSV files during the import process. If you re-import from RME or a CSV file again in the future, you can choose to import only those devices that have never been imported before.

When you import a device from RME, QPM checks the device model to see whether it is a supported by QPM. If it is supported, QPM starts the discovery process, and it is imported. If the model is not supported, QPM does not start the discovery process and it is not imported.

For information about defining device access parameters during import, see Adding Devices to the Device Inventory, page 4-3.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select **Add Device** from the TOC. The Import Devices Wizard - General page appears.

Step 3 Do the following in the Import Devices Wizard - General page:

a. Select the Import from RME radio button.

b. Enter the IP address of the RME server in the Host Location field.

c. Enter a valid RME username in the User Name field.

d. Enter the password for the username in the Password field.

e. Select the Import only new RME devices check box to import only the devices that have not been previously imported from RME.

f. Click **Next**. The Import Devices Wizard - Select Devices page appears.

Step 4 In the Import Devices Wizard - Select Devices page, select the check boxes next to the devices you want to add, then click **Finish**.

The Discovery Status page appears, where you can monitor the progress of the add operation. For more information, see Viewing Device Discovery Status, page 4-13.

Related Topics

- Adding Devices to the Device Inventory, page 4-3
- Using QPM Tables, page 3-8
- Using QPM Wizards, page 3-10
- Troubleshooting Device Management Problems, page 11-5

Importing Virtual Devices

You can import virtual devices from a file for testing and demonstration purposes. Virtual devices are not physical devices, but rather are defined in a file that contains the same device information required to import a physical device.

You create a file containing a virtual device by exporting device inventory information. For more information, see Exporting Device Information, page 4-15.

Each device in the inventory must have a unique IP address. If the virtual device file you want to import contains a virtual device with an IP address that is already in the inventory, you must edit the IP address in the file (which is in XML format) before you can import the virtual device.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select **Add Device** from the TOC. The Import Devices Wizard - General page appears.

Step 3 Do the following in the Import Devices Wizard - General page:

a. Select the Import Virtual Devices from File radio button.

b. Enter the path to the virtual devices file in the File field, or click **Browse** to navigate to the file.

c. Click **Next**. The Import Devices Wizard - Select Devices page appears.

Step 4 In the Import Devices Wizard - Select Devices page, select the check boxes next to the devices you want to add, then click **Finish**.

The Discovery Status page appears, where you can monitor the progress of the add operation. For more information, see Viewing Device Discovery Status, page 4-13.

Related Topics

- Adding Devices to the Device Inventory, page 4-3
- Using QPM Tables, page 3-8
- Using QPM Wizards, page 3-10

Importing Devices from QPM 2.1x

You can import devices from a QPM 2.1x database that was exported to an XML file.

During the import process, QPM presents a listing of QPM-supported devices in the import file. It does not include devices that are not supported by QPM. You select which devices to import.

Before You Begin

Export a QPM 2.1x database using the QPM 2.1x export utility. See the *Installation Guide for QoS Policy Manager 3.0* for more information.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select **Add Device** from the TOC. The Import Devices Wizard - General page appears. For information about this page, see Import Devices Wizard - General Page, page A-23.

Step 3 Do the following in the Import Devices Wizard - General page:

a. Select the Import from QPM 2.x radio button.

b. Enter the path to the file in the File field, or click **Browse** to navigate to the file.

c. Click **Next**. The Import Devices Wizard - Select Devices page appears.

Step 4 In the Import Devices Wizard - Select Devices page, select the check boxes next to the devices you want to add, then click **Finish**.

The Discovery Status page appears, where you can monitor the progress of the add operation. For more information, see Viewing Device Discovery Status, page 4-13.

Tip Common causes of device discovery failure include incorrect Telnet or SNMP passwords, incorrect IP addresses, and unavailable devices.

Related Topics

- Adding Devices to the Device Inventory, page 4-3
- Using QPM Tables, page 3-8
- Using QPM Wizards, page 3-10

Configuring Default Device Access Parameters

Device access parameters are the passwords and community strings that QPM needs to log into, import, and configure devices. These parameters include TACACS and Telnet passwords.

When QPM connects to a device, it logs into the device using TACACS authentication. If this fails, it uses local authentication. This login process is used for both communication methods—SSH and Telnet.

You can configure default device access parameters that are assigned to devices when you import them into the inventory.

Note If you are using ACS and multiple device groups, each device group has its own set of default device access parameters.

When you add devices to the inventory, the default device access parameters are used to import the devices unless you override them. Each method of importing devices has its own method of overriding the defaults; see the related topics for more information.

You can configure device access parameters for an individual device, or for all devices in a device group.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 To change parameters for a single device, click the name of the device. The Device Properties page appears:

To change parameters for a device group:

a. Select **Device Groups** from the TOC. The Device Groups page appears.

b. In the Device Groups page, click the name of the device group you want to modify. The Device Group Properties page appears.

Step 3 Do the following in the Device Properties page, or the Device Group Properties page:

a. Open the Default Access Parameters area by clicking the arrow next to its heading.

b. Modify the access parameters by entering new values. For more information about the fields in these pages, see Device Group Properties Page, page A-35 or Device Properties Page, page A-7.

c. Click **Save**.

Related Topics

- Adding Devices to the Device Inventory, page 4-3
- Adding a Single Device, page 4-5
- Importing Devices from a Device Inventory CSV File, page 4-6
- Updating Device Access Parameters from RME, page 4-23
- Using QPM Tables, page 3-8
- Troubleshooting Device Management Problems, page 11-5

Viewing Device Discovery Status

When you import devices, you can use the Discovery Status report to see the status of each device discovery task (for example, tasks can be finished, in progress, or failed because of incorrect device access parameters).

You can define the refresh interval for this page.

If you add more devices while the previous add device operation is still in progress, the Discovery Status page will display a separate record for each add operation, in order from newest to oldest.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select **Discovery Status** from the TOC. The Discovery Status page appears.

Step 3 Do the following in the Discovery Status page:

a. View the status of active device discovery operations. For information about this page, see Discovery Status Page, page A-29.

b. Optionally, you can select a different refresh interval from the list box below the table.

Related Topics

- Adding Devices to the Device Inventory, page 4-3
- Using QPM Tables, page 3-8
- Troubleshooting Device Management Problems, page 11-5

Working with Devices

The following topics describe working with devices:

- Viewing and Editing Device Properties, page 4-14
- Setting Device Policy Groups Assignments, page 4-17
- Rediscovering Device Information, page 4-18

Viewing and Editing Device Properties

You can view a device's properties and edit some of them. Examples of the properties you can edit include:

- Device role assignment
- Device folder assignment
- Device access parameters (passwords and community strings)

You can view and edit device properties from any device list, whether it is in the main device table, or accessed from the device folders, device groups, or search results pages.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 In the Device Table page, do one of the following to select the device to edit:

- Click the device name in the Sys Name column.
- Select the check box next to the device name, then click **Edit**.

The Device Properties page appears.

Step 3 Do the following in the Device Properties page:

a. Edit any of the device properties that are available for editing. For more information about the fields in this page, see Device Properties Page, page A-7.

b. Click **Save**.

The following topics describe other tasks you can perform on devices:

- Exporting Device Information, page 4-15
- Connecting to a Device Using Telnet, page 4-16
- Viewing Device Configuration, page 4-17

Exporting Device Information

You can export a device's information to a file on your client system that can then be used to import the device back into QPM as a virtual device. This process allows you to test and demonstrate QoS policies without affecting real devices.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 In the Device Table page, do one of the following to select the device to edit:

- Click the device name in the Sys Name column.
- Select the check box next to the device name, then click **Edit**.

The Device Properties page appears.

Step 3 In the Device Properties page, click **Export**.

The browser file download process begins.

Step 4 Use the browser file download process to save the file to your client system.

Related Topics

- Importing Virtual Devices, page 4-9
- Using QPM Tables, page 3-8

Connecting to a Device Using Telnet

You can connect to a device in the device inventory from within QPM using Telnet. QPM starts the default Telnet program on your client system and automatically connects to the device. If there is no Telnet program installed on your client system, this feature will not work.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 In the Device Table page, do one of the following to select the device to edit:

- Click the device name in the Sys Name column.
- Select the check box next to the device name, then click **Edit**.

The Device Properties page appears.

Step 3 Click **Telnet**.

A Telnet application opens and connects to the device.

Related Topics

- Using QPM Tables, page 3-8
- Troubleshooting Device Management Problems, page 11-5

Viewing Device Configuration

You can view a device's running software configuration from within QPM. This is useful if you are deciding whether to upload the device's configuration into the QPM inventory.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 In the Device Table page, do one of the following to select the device to edit:

- Click the device name in the Sys Name column.
- Select the check box next to the device name, then click **Edit**.

The Device Properties page appears.

Step 3 Click **Show run**.

The Display show run report appears, displaying the device's running configuration.

Related Topics

- Using QPM Tables, page 3-8

Setting Device Policy Groups Assignments

To configure QoS policies on a device, you assign it to a policy group. You can do this in the following ways:

- By accessing a policy group's properties and assigning the device to the policy group. For more information, see Setting Network Element Assignments, page 6-13.
- By accessing a device's properties and assigning it to a policy group. The following procedure describes this process.

This procedure describes how to:

- Assign devices to policy groups.
- Remove devices from policy groups.
- Change device policy group assignment.

Procedure

Step 1 Select **Devices > Manage.** The Device Table page appears.

Step 2 Select the check box next to the devices you want to add to or remove from a policy group, then click **Set Policy Group**.

The Policy Group Assignment dialog box opens.

Step 3 Do the following in the Policy Group Assignment dialog box:

a. Set and remove policy group assignments. For information about the fields in this page, see Policy Group Assignment Dialog Box, page A-6.

b. Click **OK** to save the policy group assignment changes you have made and close the dialog box.

Related Topics

- Setting Network Element Policy Group Assignments, page 4-26
- Using QPM Tables, page 3-8

Rediscovering Device Information

Rediscovering a device's information causes QPM to connect to the device on the network and obtain its device information again. You should do this when you make configuration changes to a device to ensure that the device can still support the policies and configurations you assigned to it using QPM.

During the rediscover process, QPM will delete any policy group device or network element assignments that are no longer valid because of changes to the device's information. A report of deleted policy group assignments is generated. For more information see Assignment Conflicts Reports Page, page D-32.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select the check boxes next to the devices you want to rediscover, then click **Rediscover**.

The Device Table page refreshes. The rediscovery status is displayed in the Status column.

Step 3 Run the Assignments report by selecting **Reports > Conflicts > Assignments** to see if any policy group assignments were deleted as a result of the rediscovery.

For more information, see Assignment Conflicts Reports Page, page D-32.

Related Topics

- Updating Device Access Parameters from RME, page 4-23
- Using QPM Tables, page 3-8
- Troubleshooting Device Management Problems, page 11-5

Working with Device Folders

You can create device folders to organize the inventory for administrative purposes. For example, you might create a device folder for each building on your corporate campus and assign the devices in each building to their corresponding device folder.

Device folders are contained within device groups. If you are not using ACS and multiple device groups, all device folders are contained within the default device group.

Unlike device groups, you cannot assign access privileges to device folders. Device folders are used primarily to group devices into related groups for the purpose of more easily searching for devices and filtering and sorting lists of devices.

When you use the device folders table to browse device folders, you can perform the same actions on the listed devices that you can perform from the device table. See Working with Devices, page 4-14, for more information about these actions.

The following topics describe how to work with device folders:

- Creating Device Folders, page 4-20
- Organizing Devices with Device Folders, page 4-21
- Editing Device Folders, page 4-21
- Deleting Device Folders, page 4-22

Creating Device Folders

Create device folders to organize your inventory.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select **Device Folders** in the TOC. The Device Folders page appears.

Step 3 Click **Create**. The Device Folder Properties page appears.

Step 4 Do the following in the Device Folder Properties page:

a. Create the new device folder. For more information about the fields in this page, see Device Folder Properties Page, page A-39.

b. Click **Save**.

The Device Folders page appears. The new device folder appears in the table.

Related Topics

- Working with Device Folders, page 4-19

Organizing Devices with Device Folders

You can use device folders to organize your inventory. The procedure describes how to add devices to device folders, remove devices from devices folders, and move devices between device folders.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select the check box next to the devices you want to assign to or remove from a device folder, then click **Set Device Folder**. The Device Folders Assignment dialog box opens.

Step 3 Do the following in the Device Folders Assignment dialog box:

a. Set and remove device folder assignments. For more information about the fields in this page, see Device Folder Properties Page, page A-39.

b. Click **OK** to save the policy group assignment changes you have made and close the dialog box.

Related Topics

- Working with Device Folders, page 4-19
- Using QPM Tables, page 3-8

Editing Device Folders

Edit a device folder to change properties such as its name and description.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select **Device Folders** in the TOC. The Device Folders page appears.

Step 3 Do one of the following to select a device folder:

- Click the name of the device folder.
- Select the check box next to a device folder name, then click **Edit**.

The Device Folder Properties page appears.

Step 4 Do the following in the Device Folder Properties page:

a. Edit the device folder. For more information about the fields in this page, see Device Folder Properties Page, page A-39.

b. Click **Save**.

Related Topics

- Working with Device Folders, page 4-19
- Using QPM Tables, page 3-8

Deleting Device Folders

Delete a device folder when you no longer want to use it to organize your inventory. Devices assigned to the device folder are not deleted from the inventory, and are no longer assigned to any device folder.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select **Device Folders** in the TOC. The Device Folders page appears.

Step 3 Select the check box next to the device folders you want to remove, then click **Delete**.

The Device Folders page refreshes. The deleted device folders do not appear in the table.

Related Topics

- Working with Device Folders, page 4-19
- Using QPM Tables, page 3-8

Using Additional Device Functions

The following topics document the additional device functions that are available:

- Updating Device Access Parameters from RME, page 4-23
- Importing Device Roles, page 4-23

Updating Device Access Parameters from RME

You can update device access parameters in the device inventory with device access parameters from RME. This is a convenient way to update the device inventory when device access parameters change.

Procedure

Step 1 Select **Devices > Options**. The Update Passwords (RME) page appears.

Step 2 Enter information about the RME server in the page. For more information about these fields, see Update Passwords (RME) Page, page A-62.

Step 3 Select the check box next to the devices you want to update, then click **Update Passwords**.

Related Topics

- Using QPM Tables, page 3-8

Importing Device Roles

A device role is a device property that specifies the network point for a device in the AVVID network, For example, a device role might identify a device as campus access, campus distribution, or WAN aggregation. Device roles are used by the IP telephony wizard to help automatically identify which interfaces should be assigned to which policies. You can import device roles from a file generated by an application that manages device roles.

Procedure

Step 1 Select **Devices > Options > Import Device Roles**. The Import Device Roles page appears.

Step 2 Enter the path to the file from which you want to import device roles in the File field, or click **Browse** and browse to the file.

Step 3 Click **Import**.

Removing Devices

If you no longer want to manage QoS on a device, you can remove it from the inventory. When you remove a device, all of its elements are also removed.

Removing Devices That Are Being Monitored

If you remove a device that contains network elements that are being monitored by a QoS analysis task, QPM continues to monitor these network elements. To stop QPM from monitoring these network elements, you must stop or delete the QoS analysis task. For more information, see the following topics:

- Performing Historical QoS Analysis, page 9-6
- Performing Real-Time QoS Analysis, page 9-17

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select the check box next to the devices you want to remove, then click **Delete**. The Device Table refreshes, with the deleted devices removed.

Related Topics

- Using QPM Tables, page 3-8

Working with Network Elements

The following topics describe how to work with network elements:

Overview of Network Elements

QPM supports both physical and logical network elements. A physical network element physically exists on a device and can be read or calculated using SNMP and Telnet. Examples include device, interface, VLAN, DLCI, and VC.

A user-supplied element is one that does not exist on a device, and its purpose is helping you manage your network elements. An example is source-destination pairs.

The interfaces on a device carry the network traffic. In QPM, the term interfaces refers to router interfaces and subinterfaces, and switch ports. QPM allows you to configure QoS on subinterfaces.

Viewing and Editing Network Element Properties

You can view and change network element properties. An example of the network element properties that you can edit is whether interfaces are ignored (hidden from display in QPM).

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Click the Interfaces icon in the table row of the device that contains the network element or elements that you want to view or edit. The Interfaces page appears.

Step 3 Click an interface name to edit it. The Interface Properties page appears.

Step 4 In the Interface Properties page:

a. Edit the interface properties if desired. For more information about the fields in this page, see Interfaces Page, page A-14.

b. Click **Save**.

Related Topics

- Hiding and Displaying Interfaces, page 4-30
- Using QPM Tables, page 3-8

Setting Network Element Policy Group Assignments

To configure QoS policies on the network, you assign network elements to policy groups. You can do this in the following ways:

- By accessing a policy group's properties and assigning network elements to the policy group. For more information, see Setting Network Element Assignments, page 6-13.
- By accessing a devices's network elements and assigning them to policy groups. The following procedure describes this method.

There are four types of network elements that you can assign to policy groups:

- Devices—See Setting Device Policy Groups Assignments, page 4-17.
- Interfaces.
- Interface subelements (VCs and DLCIs).
- User-supplied elements (VLANs and source-destination pairs).

The following procedure describes how to do the following to interfaces, interface subelements, and user-supplied elements:

- Assign them to policy groups.
- Remove them from policy groups.
- Change policy group assignments.

You only need to perform the steps required for the network element types you are working with.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Click the Interfaces icon in the table row of a device that contains network element or elements that you want to assign. The Interfaces page appears.

Step 3 Assign interfaces to policy groups, remove interfaces from policy groups, and change interface policy group assignments:

a. Select the check box next to the interfaces you want to assign to or remove from a policy group, then click **Set Policy Group**. The Policy Group Assignment dialog box opens.

b. Set and remove policy group assignments. For more information about the fields in this page, see Policy Group Assignment Dialog Box, page A-6.

Step 4 Assign subelements of an interface to policy groups, remove subelements of an interface from policy groups, and change subelements of an interface policy group assignments:

a. Click the name of an interface. The Interface Properties page appears.

b. Select any subelements of the interface (click the arrow icons to open or close the page subsections) that you want to assign, then click **Set Policy Group**. The Policy Group Assignment dialog box opens.

c. Set and remove policy group assignments. For more information about the fields in this page, see Policy Group Assignment Dialog Box, page A-6.

Step 5 Assign source-destination pairs and VLANs to policy groups, remove source-destination pairs and VLANs from policy groups, and change source-destination pairs and VLANs policy group assignments:

a. Click **Source-Dest Pairs** or **VLANs** in the TOC.

b. In the resulting page, select the source-destination pairs or VLANs that you want to assign, then click Set Policy Group. The Policy Group Assignment dialog box opens.

c. Set and remove policy group assignments. For more information about the fields in this page, see Policy Group Assignment Dialog Box, page A-6.

Related Topics

- Setting Device Policy Groups Assignments, page 4-17
- Using QPM Tables, page 3-8

Working with Source-Destination Pairs

Source-destination pairs are logical (not physical) user-supplied network elements. You define them for Catalyst 8400 and Catalyst 8500 switches, which have QoS features that allow you to configure QoS policies to inbound and outbound traffic on the same device. To do this, you must define source-destination pairs of interfaces on a device, to which you can apply this type of QoS policy.

The following topics describe how to work with source-destination pairs using QPM:

- Creating Source-Destination Pairs, page 4-28
- Editing Source-Destination Pairs, page 4-29
- Deleting Source-Destination Pairs, page 4-30
- Setting Network Element Policy Group Assignments, page 4-26

Creating Source-Destination Pairs

You can create source-destination pairs using QPM.

Procedure

Step 1 Choose **Devices > Manage**. The Device Table page appears.

Step 2 Click the device name of the device on which you want to create a source-destination pair. The Device Properties page appears.

Step 3 Click **Source-Dest Pair** in the TOC (a subentry of Device Information). The Source-Dest Pairs page appears.

Step 4 Click **Create**. The Source-Dest Pairs Properties page appears.

Step 5 Do the following in the Source-Dest Pairs Properties page:

a. Create a source-destination pair. For more information about the fields in this page, see Source-Dest Pair Properties Page, page A-19.

b. Click **Save**.

Related Topics

- Working with Source-Destination Pairs, page 4-28
- Using QPM Tables, page 3-8

Editing Source-Destination Pairs

You can edit source-destination pairs using QPM.

Procedure

Step 1 Choose **Devices > Manage**. The Device Table page appears.

Step 2 Click the device name of the device on which you want to edit a source-destination pair. The Device Properties page appears.

Step 3 Click **Source-Dest Pair** in the TOC (a subentry of Device Information). The Source-Dest Pairs page appears.

Step 4 Select the check box next to the source-destination pair you want to edit, then click **Edit**. The Source-Dest Pairs Properties page appears.

Step 5 Do the following in the Source-Dest Pairs Properties page:

a. Edit the source-destination pair. For more information about the fields in this page, see Source-Dest Pair Properties Page, page A-19.

b. Click **Save**.

Related Topics

- Working with Source-Destination Pairs, page 4-28
- Using QPM Tables, page 3-8

Deleting Source-Destination Pairs

You can delete source-destination pairs using QPM.

Procedure

Step 1 Choose **Devices > Manage**. The Device Table page appears.

Step 2 Click the device name of the device on which you want to delete a source-destination pair. The Device Properties page appears.

Step 3 Click **Source-Dest Pair** in the TOC (a subentry of Device Information). The Source-Dest Pairs page appears.

Step 4 Select the check box next to the source-destination pairs you want to delete, then click **Delete**.

Related Topics

- Working with Source-Destination Pairs, page 4-28
- Using QPM Tables, page 3-8

Hiding and Displaying Interfaces

When you import a device, QPM discovers and imports all of its elements that QPM supports. You can prevent interfaces (not other network elements) from being displayed in QPM by marking them as ignored. You can later redisplay interfaces if you want to see them again. DLCIs and VCs on ignored interfaces are also ignored.

The following topics describe hiding and displaying interfaces:

- Hiding Interfaces, page 4-31.
- Displaying Interfaces, page 4-31.

Hiding Interfaces

You can mark interfaces as ignored, preventing them from displaying in QPM.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Click the name of the device that contains the interfaces you want to ignore. The Device Properties page appears.

Step 3 Select **Interfaces** in the TOC (a subentry of Device Information). The Interfaces page appears.

Step 4 Select the check box next to the interfaces you want to ignore, then click **Mark as Ignore**. A confirmation dialog box opens.

Step 5 Click **Yes** in the confirmation dialog box.

The Interfaces page refreshes. The ignored interfaces are no longer displayed.

Related Topics

- Hiding and Displaying Interfaces, page 4-30
- Displaying Interfaces, page 4-31
- Using QPM Tables, page 3-8

Displaying Interfaces

You can redisplay interfaces that you previously marked as ignored.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Click the name of the device that contains the interfaces you want to unignore. The Device Properties page appears.

Step 3 Click the hyperlinked number in the Ignored Interfaces field. The Ignored Interfaces List dialog box opens.

Step 4 Select the check box next to the interfaces you want to unignore, then click **Cancel Ignore**.

Step 5 Click **Close** to close the dialog box.

Related Topics

- Hiding and Displaying Interfaces, page 4-30
- Hiding Interfaces, page 4-31
- Using QPM Tables, page 3-8

Searching for Devices and Network Elements

You can search the inventory to find devices and network elements that meet criteria that you specify.

The search criteria are divided into two categories:

- Network element criteria—Based on qualities of the network element. For example, you can search for all devices that are running Cisco IOS version 12.0, or all interfaces that have ATM VCs configured on them.
- Assignment criteria—Based on the network element policy group assignment. For example, you can search for all devices that are assigned to a particular policy group.

You can create multiple search criteria. You specify whether the search results must match all of the criteria statements (logical AND) or any of them (logical OR).

You can display the search criteria you have configured as a sentence, allowing you to more easily verify that the search will produce the results you want.

The devices and elements that match the search criteria are displayed in tables that allow you to perform all the tasks that QPM provides on these network elements.

Procedure

Step 1 Select **Devices > Search**. The Search For Devices page appears.

Step 2 If you want to search for a network element other than a device, select that network element in the TOC. The search page for that network element type appears.

Step 3 Enter search criteria using the page fields. For information about these fields, see the UI reference for the type of network element you are searching for:

- Search for Devices Page, page A-41
- Search for Interfaces Page, page A-46
- Search for VLANs Page, page A-49
- Search for VCs Page, page A-53
- Search for DLCIs Page, page A-56
- Search for Source-Dest Pairs Page, page A-59

Step 4 To see the search criteria expressed as a sentence, click **Refresh Summary**. The summary field refreshes.

Step 5 To clear all search criteria, click **Reset**.

Step 6 To run the search, click **Search Now**. A results page appears.

For information about the results page, see the UI reference for the type of network element you are searching for:

- Devices Search Result Page, page A-43
- Interfaces Search Result Page, page A-48
- VLANs Search Result Page, page A-52
- VCs Search Result Page, page A-55
- DLCIs Search Result Page, page A-58
- Source-Dest Pairs Search Result Page, page A-61

Related Topics

- Using QPM Tables, page 3-8

Working with Device Groups

This section is applicable only for users who use ACS permissions, and are working with ACS device groups. If you do not use ACS to create multiple device groups, only the default device group will be available in QPM.

The following topics describe how to work with device groups:

Understanding Device Groups

Device groups are groups of devices (and their network elements) within the inventory. They are created and maintained in ACS, but QPM assigns some properties to each device group that you can view and edit in QPM. For more information, see Editing Device Group Properties, page 4-37.

Each device group has its own set of access permissions, so they can be used to divide the network into administrative groups for purposes of controlling who can do what with which devices. Because you create policies in the context of a device group, you can assign policy groups only to devices in the same device group as the policy.

The inventory always contains one device group named the default device group. If you are not using ACS device groups to group devices, your inventory will contain only the default device group.

ACS Device Groups

If you are using multiple ACS device groups, QPM will automatically create the same device groups with the same user permissions that are defined in ACS. When you add a new device to the inventory, QPM assigns it to its ACS device group, with the same user permissions. If a device is not assigned to an ACS device group, it is assigned to the QPM default device group.

QPM automatically synchronizes the inventory with ACS in the following cases:

- When you import devices, QPM synchronizes with ACS to find out what device groups the devices belong to. Only the imported devices are synchronized with ACS.
- When you log into QPM, QPM automatically synchronizes with ACS to obtain and store your user permissions so it can check them before any user operations you attempt.

In addition, before you deploy a deployment job, QPM synchronizes with ACS to verify that the user permissions allow the job to proceed.

You can also manually refresh the QPM device group information, synchronizing it with ACS. See Synchronizing Permissions and Device Group Information, page 4-36.

Note If you are using ACS device groups, all devices used in QPM, including the QPM server, should be defined in ACS device groups, only as AAA clients, and not as AAA servers.

Related Topics

- User Permissions, page 3-11

Setting the Active Device Group

Only one device group at a time can be active. Throughout the QPM user interface, only the devices, deployment groups, and policy groups that are contained in the active device group are displayed. You must have sufficient user privileges to set the active device group.

Procedure

Step 1 Select **Devices > Manage**. The Device Table page appears.

Step 2 Select **Device Groups**. The Device Groups page appears.

Step 3 Select the device group that you want to make active by selecting the check box next to its name, then click **Set Active**.

Related Topics

- Using QPM Tables, page 3-8

Synchronizing Permissions and Device Group Information

You can manually synchronize the user permissions and device group information in the inventory with ACS or CiscoWorks Common Services (depending on which you are using to administer device groups and user permissions).

Typically you would synchronize in the following cases:

- When you know changes have been made to the ACS or CiscoWorks Common Services device group assignments or access privileges.
- When your CiscoWorks user role has changed since you logged into QPM.

The Sync Privileges page displays your permissions to the QPM device groups on the system so you can determine if you need to synchronize to update your QPM permissions.

If changes are made to the QPM device groups as a result of the synchronization, the Conflicts Assignment report shows which devices have been moved from the current device group, and all policy group assignments for those devices and their network elements will be deleted.

Note ACS and CiscoWorks Common Services device group and user permissions information is automatically synchronized each time you log into QPM.

Procedure

Step 1 Select **Devices > Options**. The Update Passwords (RME) page appears.

Step 2 Select **Sync Device Groups** in the TOC. The Sync Privileges page appears.

Step 3 Click **Sync**. A dialog box opens.

Step 4 Click **OK** in the dialog box.

Related Topic

- Assignment Conflicts Reports Page, page D-32
- Troubleshooting Device Management Problems, page 11-5

Editing Device Group Properties

Although you cannot change device group membership within QPM (you must make device group assignment changes in ACS), you can edit the device group properties that are unique to QPM.

Many of the device group properties are the same properties that QPM maintains for devices. These device group properties are assigned to all devices in the device group by default. You can override these defaults by entering different device properties for an individual device.

Examples of the device group properties that you can edit include:

- Description.
- Default device access parameters.
- Enabling/disabling NBAR port mapping.

Procedure

Step 1 Click **Devices > Manage**. The Device Table page appears.

Step 2 Select **Device Groups** from the TOC. The Device Groups page appears.

Step 3 Click the name of the device group you want to edit. The Device Group Properties page appears.

Step 4 Do the following in the Device Group Properties page:

a. Edit the device group. For more information about the fields in this page, see Device Group Properties Page, page A-35.

b. Click **Save**.

Related Topics

- Using QPM Tables, page 3-8
- Viewing and Editing Device Properties, page 4-14

Deleting Device Groups from QPM

QPM device groups are not automatically deleted from QPM when you delete them in ACS, even when you synchronize device group information with ACS. Instead, you must manually delete QPM device groups. Any deployment groups and policy groups contained in the device group are also deleted.

This feature is useful because device groups are not automatically deleted from QPM when you delete them in ACS, even when you synchronize device group information with ACS. This gives you the opportunity to edit your QPM deployment groups and policy groups before manually deleting the device group.

The following are the restrictions for deleting QPM device groups:

- You cannot delete the QPM default device group.
- You cannot delete a device group that still contains devices. To delete a device group, you must first do one of the following:
  - Remove all devices from the device group in ACS.
  - Delete all devices in the device group from the QPM inventory.

If you convert from using ACS to CiscoWorks Common Services for device management and user authentication, all devices in the inventory are moved to the default device group (because CiscoWorks Common Services does not support multiple device groups). You can then delete the remaining empty device groups.

Procedure

Step 1 Click **Devices > Manage**. The Device Table page appears.

Step 2 Select **Device Groups** from the TOC. The Device Groups page appears.

Step 3 Select the radio button next to the device group you want to delete.

Step 4 Click **Delete**.

Configuring QoS for IP Telephony

In an AVVID (Architecture for voice, video, and integrated data) network, you must configure QoS for IP telephony to ensure voice quality.

The following topics provide information about the need for configuring QoS in an IP telephony environment and the tools that enable you to do this.

Understanding QoS for IP Telephony

Real-time based applications in a network, such as voice applications, have different characteristics and requirements than those of data applications. Voice applications tolerate minimal variation in the amount of delay affecting delivery of their voice packets. Voice traffic is also intolerant of packet loss and jitter, both of which degrade the quality of the voice transmission delivered to the recipient end user. To effectively transport voice traffic over IP, mechanisms are required that ensure reliable delivery of packets with low latency.

In an enterprise environment, network congestion can occur at any time in any portion of the network campus, branch office, or WAN. For successful deployment of IP telephony, you must ensure end-to-end network quality for voice traffic.

To ensure voice quality, you must use QoS in all areas of the enterprise network. To make a proper QoS configuration, you must first identify the points where QoS is a concern, then choose the appropriate QoS tools to use, and deploy to the devices in the network.

QPM provides tools that can determine and configure the optimum QoS for a voice network. These include:

- Provisioning tools—Let you easily define the correct policies for interfaces on the voice paths. QPM provides voice policy groups—policy groups that contain the QoS configurations and policies required at each relevant point in the network that needs QoS for IP telephony.
- Deployment tools—Let you deploy these policies on the network and monitor the deployment process.
- Reports and troubleshooting tools—Help you identify faults and fix them.

Related Topics

- Network Model for Configuring QoS for IP Telephony, page 5-3
- Using QPM to Configure QoS for IP Telephony, page 5-4
- Viewing the Voice Ready Report, page 5-25
- Chapter 7, “Deploying QoS Policies”

Network Model for Configuring QoS for IP Telephony

Figure 5-1 shows a typical network model for configuring QoS for IP telephony in an enterprise environment. QPM supports the QoS methods required to configure IP telephony QoS for high-speed campus domains, branch offices, and WAN implementations.

Figure 5-1 IP Telephony Network Model

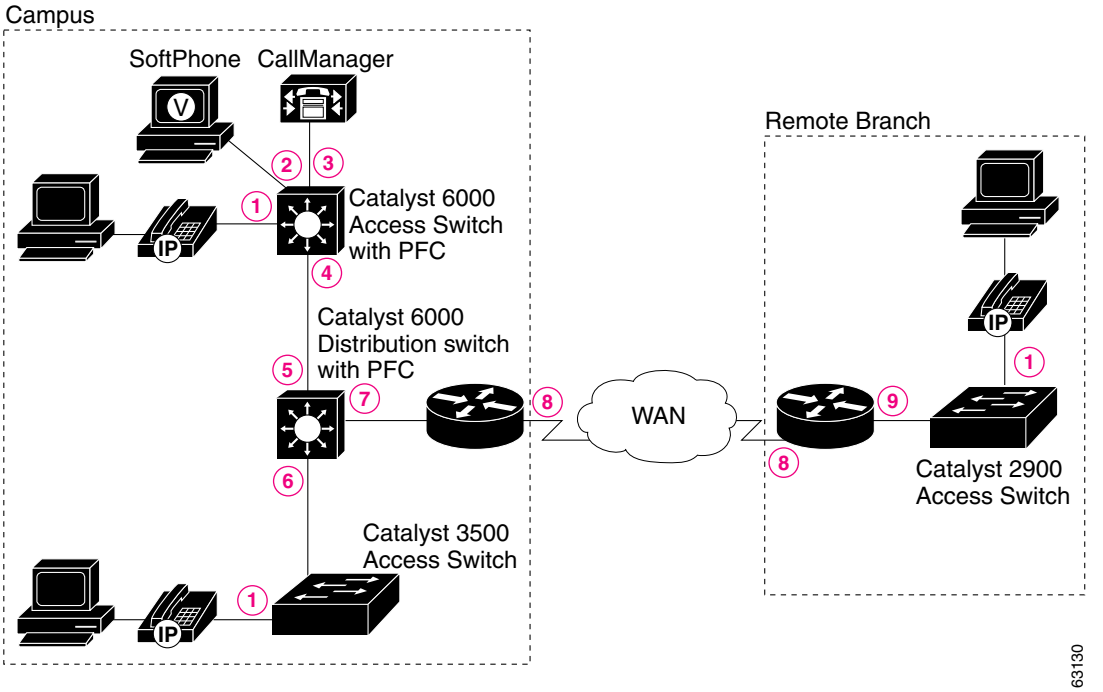


Table 5-1 lists the network points that require QoS configuration for IP telephony.

Table 5-1 Network Points Requiring QoS Configuration

Network Point in Figure 5-1	Description
1	Access switch - IP phone ports
2	Layer 3 QoS-aware access switch (with PFC) - SoftPhone port
3	Layer 3 QoS-aware access switch (with PFC) - CallManager port
4	Layer 3 QoS-aware access switch (with PFC) uplink port to distribution switch (with PFC)
5	Distribution switch (downlink) port to Layer 3 QoS-aware access switch (with PFC)
6	Distribution switch (downlink) port to Layer 2 QoS-aware access switch
7	Layer 3 distribution switch port to WAN router
8	WAN interface
9	Branch office router interface to Layer 2 QoS-aware switch

Related Topics

- Understanding QoS for IP Telephony, page 5-1
- Using QPM to Configure QoS for IP Telephony, page 5-4

Using QPM to Configure QoS for IP Telephony

The QPM IP Telephony application provides a solution for configuring QoS for voice traffic in an AVVID (architecture for voice, video, and integrated data) network.

The solution is an IP Telephony wizard that creates voice policy groups at each network point that requires IP telephony QoS configuration.

Voice policy groups are policy groups that contain the QoS properties and policies for each relevant point in the IP telephony network. A voice policy group contains a voice role attribute, which specifies the role of an interface, according to its type, function and location on the network, such as, IP phone, Switch to WAN Router. QPM allows you to modify properties and policies of certain voice policy groups created by the wizard, to suit specific network configurations, as required.

The IP Telephony wizard creates voice policy groups from voice policy group templates which are provided by QPM in the Policy Group Templates library. These templates follow the IP telephony QoS guidelines, described in the IP Telephony QoS Design Guide:

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/avvidqos/index.htm

If the required templates do not exist during IP telephony QoS configuration, they can also be generated by the wizard and stored in the library.

Some templates that are provided by QPM, such as ATM links, might not be used by the IP Telephony wizard.

Note You can also create voice policy groups without the wizard, using the voice policy group templates supplied by QPM. You assign the voice policy groups in the same way as you would data policy groups.

Related Topics

- Configuring QoS Using the IP Telephony Wizard, page 5-5
- Modifying Voice Policy Groups, page 5-24
- Working with Policy Group Templates, page 6-41

Configuring QoS Using the IP Telephony Wizard

The IP Telephony wizard allows you to configure QoS for voice traffic on the network. The wizard handles VoIP configuration in common IP telephony network topologies. It guides you through the steps required to define your IP telephony network topology. At each step, the wizard automatically creates the voice policy groups, that include the QoS policies required at each network point (interface) where QoS is a concern. The wizard presents only the interfaces on

which the relevant QoS can be configured. All you need to do is select the network elements that require QoS configuration at each network point. The wizard then automatically assigns the interfaces to the appropriate voice policy groups.

Note QPM allows you to import files which contain device role information about devices (see Importing Device Roles, page 4-23). Device role information is used by the IP Telephony wizard during the selection of interfaces to voice roles. For example, for the wizard to select an Ethernet 10/100 port on the switch to an IP phone voice role, the switch must be an access type switch (i.e., have an "access" device role). If the switch has a "distribution" device role, QPM will not select it. If the device role information imported from a file is not up-to-date, you can manually override it in the Device Properties page (see Viewing and Editing Device Properties, page 4-14).

The wizard automatically creates voice policy groups in the current deployment group. The deployment group may also contain previously created policy groups containing data policies. If required, you can change the current deployment group when you start working with the wizard. If the required voice policy groups already exist in the deployment group, the wizard uses them and assigns the required interfaces to them. If a required voice policy group does not exist in the deployment group, the wizard creates a new one from the relevant template.

Step-by-step procedures for configuring QoS using the IP Telephony wizard, are described in the following sections.

The steps of the wizard are as follows:

- Introduction
- Selecting Devices for QoS Configuration
- Selecting the IP Phone Connections
- Selecting the SoftPhone Connections
- Selecting the CallManager and Gateways Ready Ports
- Selecting the IntraLAN Connections
- Selecting Voice VLAN Devices
- Selecting the Switch to the WAN Router Connections
- Selecting the Router WAN to Switch Connections
- Selecting WAN Serial Point-to-Point Connections

- Selecting WAN Frame Relay Connections
- End

Before you Begin

To run the wizard, it is assumed that the following preconditions have been met:

- Voice VLANs have been configured on all the relevant ports of the devices to enable the wizard to attach QoS properties to these VLANs.
- All the relevant devices in your network were added or imported to QPM's device inventory.

Related Topics

- Using QPM to Configure QoS for IP Telephony, page 5-4
- Using the IP Telephony Wizard, page 5-7
- Adding Devices to the Device Inventory, page 4-3
- Working with Policy Group Templates, page 6-41

Using the IP Telephony Wizard

This topic describes the main features of the IP Telephony wizard pages and how to use them.

Description

Each configuration step page of the wizard includes a description of the QoS policies that will be configured on the interfaces for the selected voice role. You can view or hide this description by clicking the arrow button next to **Description**. By default, the description is hidden.

Advanced

The Advanced section of a configuration step page provides two buttons:

- Remove—Clicking this button opens a page in which you can remove network elements that were assigned for a voice role. This option allows you to change your selection of network elements after they have been assigned to voice policy groups. The wizard removes the assignment of selected elements from the voice policy group.

- Recommend—If QPM recommended rules are available for a specific voice role, clicking this button activates the wizard to accept the recommended selection of network elements for the current voice role. The network elements are selected but not assigned to voice policy groups. A list of the rules for the current voice role is displayed.

You can view or hide the Advanced section by clicking the arrow button next to **Advanced**. By default, this section is hidden.

Selection Table

In each configuration step, you select the network elements that require QoS configuration. The available network elements are presented in a table. You can hide this table by clicking the arrow button next to **Selection Table**. By default, the selection table is open. For information about using a selection table, see Using QPM Tables, page 3-8.

By selecting the Display Configuration Info. check box in the first configuration step, you can choose to view assignment summary information after each configuration step. The check box will remain selected in all the other steps. Similarly, you can deselect this check box in the first configuration step if you don't want to view the summary information. You can override the default selection at each step, if required.

Assignment Summary

As you work through the wizard, you can choose to view an assignment summary page that displays the voice policy groups that were created for the current voice role, and summary information about the assignment of network elements in the current configuration step.

The following assignments summary information may be displayed:

- The total number of network elements you selected in this configuration step.
- The number of network elements that were selected, but found to be previously assigned to voice policy groups with this voice role.
- The number of network elements that were newly assigned to a voice policy group with this voice role. (This may include elements that were previously assigned to voice policy groups with different voice roles.)
- The number of network elements that were selected in this configuration step, but were not assigned to the voice role because they have no policies for this voice role. These elements appear in the selection list because they have the same interface type as other elements that can be selected. For example,

although GigabitEthernet interfaces have the same interface type as FastEthernet interfaces, they cannot be connected to an IP phone. During IP phone configuration, these interfaces will not be assigned to voice policy groups for the IP Phones voice role.

- The number of related assignment elements. These are network elements that were not selected (or were not in the selection table), but were assigned to voice policy groups to complete the configuration correctly. For example, when you configure traffic shaping on a DLCI, you must also enable it on a main frame-relay interface.
- The number of reassigned network elements. If network elements were found to be already assigned to voice policy groups with different voice roles, the wizard overrides the previous assignment and assigns them to voice policy groups with the new voice role.

From this assignment summary page, you can also view detailed information about a voice policy group, and a list of the newly assigned network elements.

Saving Your Assignments

You work through each step of the wizard by clicking the Next button in each page, or you can use the Navigation TOC that is displayed on the left side of each page to move directly to the step you want to do. Clicking Next to move to the next configuration step, or selecting another step forward in the Navigation TOC, saves the voice policy groups and the assignments that were made for that voice role, to the deployment group. Clicking Cancel, Back, or selecting another step backward in the Navigation TOC, undoes any configuration changes you made in that step.

If the Display Configuration Info. check box is selected, clicking Next opens the assignments summary page for that configuration step. The voice policy groups will be saved in the deployment group, but the assignment of interfaces to them will not be saved. After reviewing your assignments summary, clicking Next in this page saves both the voice policy groups and the interface assignments, and opens the next step of the wizard.

Related Topics

- Configuring QoS Using the IP Telephony Wizard, page 5-5
- IP Telephony Wizard: Assignment Summary Page, page B-97
- Viewing Policy Group Information, page 6-18

Introduction

The first page is an introduction to the wizard. It includes an overview of why QoS configuration is necessary for VoIP networks, and how the wizard will guide you to configure QoS for IP telephony.

Before you run the wizard, ensure that all the required devices in your IP telephony network have been added to the device inventory. If not, you must exit the wizard and add or import them. After adding your devices, you can check that your devices support voice QoS, by running the Voice Ready report. The Voice Ready report shows all the devices in the current device group, and whether or not they support voice QoS.

This page also displays the name of the current deployment group that will be used by the wizard for defining the IP telephony policies. You can change the current deployment group, if required.

Procedure

Step 1 Select **Configure > IP Telephony**. The Introduction page appears.

Step 2 If you are running the wizard for the first time, click the Before you run the wizard for the first time link. A window opens, prompting you to check the following:

a. If you opened the wizard before adding or importing your devices into QPM's device inventory:

- Click **Cancel** to exit the wizard.
- Add/import your network devices to the device inventory.
- Select **Configure > IP Telephony** to reopen the Introduction page of the wizard.

b. Check if your devices support voice QoS by viewing the Voice Ready report. You can open this report in one of the following ways:

- Click the Voice Ready Report link in step 2 of the wizard.
- Select **Reports > IP Telephony**.

Step 3 To change the displayed deployment group, select the required one from the list box.

Step 4 Click **Next** to move to the first configuration step of the wizard.

Related Topics

- Selecting Devices for QoS Configuration, page 5-11
- Adding Devices to the Device Inventory, page 4-3
- Viewing the Voice Ready Report, page 5-25

Selecting Devices for QoS Configuration

In this step of the wizard, you select the devices that you want to participate in the current IP Telephony wizard session. All the devices in the device group that support IP telephony features (according to model and OS) are displayed in a table. The wizard will configure only the network elements from the selected devices. By default, the wizard selects all the devices.

Devices that do not support IP telephony are not displayed. If required, you can open the Voice Ready report to see all the devices in the current device group and whether or not they support QoS for voice.

Note If you opened the IP Telephony wizard before you added or imported your devices, no devices will be displayed in the table. In this case, you must add or import devices into the device inventory. Click **Cancel** to exit the wizard, and open the Add/Import Devices wizard (see Adding Devices to the Device Inventory, page 4-3).

Some devices, such as Catalyst 6000 and Catalyst 4000 switches, require global device configuration. If any of the selected devices require global device configuration, the wizard immediately assigns them to the appropriate voice policy groups with a Voice Device voice role. Clicking the link on this page opens an information window describing this feature.

Procedure

Step 1 In the table, select the check boxes next to the devices you want to configure for voice QoS.

For more information about the columns in this table, see IP Telephony Wizard: Select IP Telephony Devices Page, page B-96.

Step 2 To view the Voice Ready report, click the Voice Ready report link.

Step 3 Select/deselect to view the Assignment Summary page:

- If you want to view summary information about the assignments made at each configuration step of the wizard, select the Display Configuration Info. check box and click **Next**. The Assignment Summary page appears.

  For information about the Assignment Summary page, see IP Telephony Wizard: Assignment Summary Page, page B-97.

- If you don't want to view the assignments summary at each configuration step of the wizard, deselect the Display Configuration Info. check box.

Step 4 Click **Next**.

The voice policy groups and your network element assignments will be saved, and the next configuration step of the wizard appears (Selecting the IP Phone Connections).

Related Topics

- Using QPM Tables, page 3-8
- Adding Devices to the Device Inventory, page 4-3
- Using the IP Telephony Wizard, page 5-7
- Modifying Voice Policy Groups, page 5-24
- Viewing the Voice Ready Report, page 5-25
- Viewing Policy Group Information, page 6-18

Selecting the IP Phone Connections

This step of the wizard describes the QoS requirements for all catalyst ports to which IP phones are connected, and asks you to select the switch ports on which the wizard will configure the QoS settings for the IP phone connections (network points **1** in Figure 5-1).

Procedure

Step 1 In the selection table, select the switch ports on which to configure QoS for your IP phones by selecting the check boxes next to the appropriate Ethernet ports.

For more information about the columns in this table, see IP Telephony Wizard: Select IP Phone Connections Page, page B-99.

Step 2 To remove any ports that were previously assigned for this voice role:

a. Click the Remove button in the Advanced section of the page. A page appears, displaying the network elements assigned for the IP Phones voice role.

For more information about this page, see IP Telephony Wizard: Remove Network Elements Page, page B-101.

b. Select the ports you want to unassign and click **Remove**. The page closes.

Step 3 Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next**.

The voice policy groups and your IP phones ports assignments will be saved, and the next configuration step of the wizard appears (Selecting the SoftPhone Connections).

Related Topics

- Using QPM Tables, page 3-8
- Using the IP Telephony Wizard, page 5-7
- Viewing Policy Group Information, page 6-18

Selecting the SoftPhone Connections

This step of the wizard describes the QoS requirements for a Catalyst 6000 (with PFC) switch that is connected to a PC running a Cisco IP SoftPhone application. You should select the switch ports on which the wizard will configure QoS settings for the SoftPhone connections in your network (network point **2** in Figure 5-1).

Procedure

Step 1 In the selection table, select the switch ports on which to configure QoS for the SoftPhone connections in the network, by selecting the check boxes next to the appropriate Ethernet ports in the list.

For more information about the columns in this table, see IP Telephony Wizard: Select SoftPhone Connections Page, page B-103.

Step 2 To remove any ports that were previously assigned for this voice role:

a. Click the Remove button in the Advanced section of the page. A page appears, displaying the network elements assigned for the SoftPhones voice role.

For more information about this page, see IP Telephony Wizard: Remove Network Elements Page, page B-101.

b. Select the ports you want to unassign and click **Remove**. The page closes.

Step 3 Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next**.

The voice policy groups and your SoftPhones port assignments will be saved, and the next configuration step of the wizard appears (Selecting the CallManager and Gateways Ready Ports).

Related Topics

- Using QPM Tables, page 3-8
- Using the IP Telephony Wizard, page 5-7
- Viewing Policy Group Information, page 6-18

Selecting the CallManager and Gateways Ready Ports

This step of the wizard describes the QoS requirements for Catalyst ports to which CallManagers or Voice Gateways are connected, and asks you to select the switch ports on which the wizard will configure the QoS settings for these connections in your network (network point **3** in Figure 5-1).

Procedure

Step 1 Select the switch port on which to configure QoS for the CallManager connection in the network, by selecting the check box next to the appropriate Ethernet port in the selection table.

For information about the columns in this table, see IP Telephony Wizard: Select CallManager Connections Page, page B-105.

Step 2 To remove any ports that were previously assigned for this voice role:

a. Click the Remove button in the Advanced section of the page. A page appears, displaying the network elements assigned for the CallManager voice role.

For more information about this page, see IP Telephony Wizard: Remove Network Elements Page, page B-101.

b. Select the ports you want to unassign and click **Remove**. The page closes.

Step 3 Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next**.

The voice policy groups and your CallManager ports assignments will be saved, and the next configuration step of the wizard appears (Selecting the IntraLAN Connections).

Related Topics

- Using QPM Tables, page 3-8
- Using the IP Telephony Wizard, page 5-7
- Viewing Policy Group Information, page 6-18

Selecting the IntraLAN Connections

After QoS configuration of the access interfaces, QoS must be configured throughout the LAN.

In this step, the wizard helps you define the appropriate QoS for the internal LAN ports—the uplinks and downlinks (network points **4**, **5** and **6** in Figure 5-1).

Note No QoS configuration is required on the uplink port of the Layer 2 Catalyst 3500 switch to the Layer 3 distribution switch port.

The correct QoS configuration for LAN connections is to trust DSCP from Layer 3 devices and trust CoS from Layer 2 devices. The wizard will configure the QoS automatically according to the type of neighboring switch.

If QPM recognizes that the neighboring switch has Layer 3 QoS capabilities, it will trust DSCP from the Layer 3 switch. If there is no neighboring switch (or if the switch is of unknown type), QPM will configure QoS for a Layer 2 device.

Procedure

Step 1 Select the switch interfaces on which to configure QoS for the LAN connections in the network, by selecting the check boxes next to the appropriate interfaces in the selection table.

For more information about the columns in this table, see IP Telephony Wizard: Select IntraLAN Connections Page, page B-107.

Step 2 To remove any interfaces that were previously assigned for this voice role:

a. Click the Remove button in the Advanced section of the page. A page appears, displaying the network elements assigned for the IntraLAN voice role.

For more information about this page, see IP Telephony Wizard: Remove Network Elements Page, page B-101.

b. Select the interfaces you want to unassign and click **Remove**. The page closes.

Step 3 Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next**.

The voice policy groups and your LAN interfaces assignments will be saved, and the next configuration step of the wizard appears (Selecting Voice VLAN Devices).

Related Topics

- Using QPM Tables, page 3-8
- Using the IP Telephony Wizard, page 5-7
- Viewing Policy Group Information, page 6-18

Selecting Voice VLAN Devices

Since the IP phone ports are configured to use an auxiliary voice VLAN on the switches, and the QoS style on the IP phone ports is set to VLAN-based, it is important to attach the appropriate policies to the voice VLAN. In this step, the wizard configures VLAN-based QoS style for an auxiliary VLAN on the connection of the IP phones to the Catalyst 6000 access switch, and also on the Layer 2 switch to Layer 3 switch connection.

Procedure

Step 1 In the selection table, select the auxiliary VLANs on which to configure QoS on both the access and distribution layer switches.

For more information about the columns in this table, see IP Telephony Wizard: Select Voice VLAN Connections Page, page B-110.

Step 2 To remove any VLANs that were previously assigned for this voice role:

a. Click the Remove button in the Advanced section of the page. A page appears, displaying the VLANs assigned for the Voice VLAN voice role.

For more information about this page, see IP Telephony Wizard: Remove Network Elements Page, page B-101.

b. Select the VLANs you want to unassign and click **Remove**. The page closes.

Step 3 Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next**.

The voice policy groups and your Voice VLAN assignments will be saved, and the next configuration step of the wizard appears (Selecting the Switch to the WAN Router Connections).

Related Topics

- Using QPM Tables, page 3-8
- Using the IP Telephony Wizard, page 5-7
- Viewing Policy Group Information, page 6-18
- Troubleshooting the IP Telephony Network, page 11-15

Selecting the Switch to the WAN Router Connections

In this step, the wizard sets QoS for the distribution switch interfaces to the WAN router (network point **7** in Figure 5-1).

Because traffic coming from the WAN side is already classified, the QoS configuration for the distribution switch interface to the router will be to trust the layer 3 DSCP bits.

Procedure

Step 1 Select the switch interface on which to configure QoS for the distribution switch connection to the WAN router, by selecting the check box next to the appropriate port in the selection table.

For more information about the columns in this table, see IP Telephony Wizard: Select Switch to WAN Router Connections Page, page B-112.

Step 2 To remove any interfaces that were previously assigned for this voice role:

a. Click the Remove button in the Advanced section of the page. A page appears, displaying the interfaces assigned for the Switch to WAN Router voice role.

For more information about this page, see IP Telephony Wizard: Remove Network Elements Page, page B-101.

b. Select the interfaces you want to unassign and click **Remove**. The page closes.

Step 3 Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next**.

The voice policy groups and your Switch-to-WAN-Router interface assignments will be saved, and the next configuration step of the wizard appears (Selecting the Router WAN to Switch Connections).

Related Topics

- Using QPM Tables, page 3-8
- Using the IP Telephony Wizard, page 5-7
- Viewing Policy Group Information, page 6-18

Selecting the Router WAN to Switch Connections

In this step, the wizard sets QoS for the WAN router connection to the access (layer 2 QoS aware) switch in the branch office (network point **9** in Figure 5-1).

By default, a router trusts the interface to a distribution (layer 3 QoS aware) switch, so no special QoS is required on the router input direction. For example, in Figure 5-1, there is no need to set QoS for the router connection to the Catalyst 6000 distribution switch in the campus. In addition, no special QoS is required on the output direction, since the layer 3 switch knows to trust DSCP from the router and sets the CoS bits accordingly. However, if the switch has only layer 2 QoS capabilities, the router must classify traffic on input and set layer 2 CoS bits on output.

Procedure

Step 1 Select the switch interfaces on which to configure QoS for the router interfaces to the distribution and access switches, by selecting the check boxes next to the appropriate interfaces in the list.

For more information about the columns in this table, see IP Telephony Wizard: Select Router WAN to Switch Connections Page, page B-114.

Step 2 To remove any interfaces that were previously assigned for this voice role:

a. Click the Remove button in the Advanced section of the page. A page appears, displaying the interfaces assigned for the Router WAN to Switch voice role.

For more information about this page, see IP Telephony Wizard: Remove Network Elements Page, page B-101.

b. Select the interfaces you want to unassign and click **Remove**. The page closes.

Step 3 Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next**.

The voice policy groups and your Router-to-Switch interface assignments will be saved, and the next configuration step of the wizard appears (Selecting WAN Serial Point-to-Point Connections).

Related Topics

- Using QPM Tables, page 3-8
- Using the IP Telephony Wizard, page 5-7
- Viewing Policy Group Information, page 6-18

Selecting WAN Serial Point-to-Point Connections

This step of the wizard allows you to select the interfaces on which to configure QoS for the Serial Point-to-Point links in the WAN segment of your network. You should select all MLP and HDLC interfaces (from both the central and the remote

sites) that carry voice traffic. For Point-to-Point links with speeds equal to or less than 768 kbs, you should select Multilink interfaces—selecting a serial interface may cause a deployment failure.

The wizard will automatically configure QoS separately for groups of interfaces with link speeds greater than 768kbs, and those with link speeds equal to or less than 768kbs.

Procedure

Step 1 Select the interfaces on which to configure QoS for the WAN Serial Point-to-Point links, by selecting the check boxes next to the appropriate interfaces in the list.

For more information about the columns in this table, see IP Telephony Wizard: Select WAN Point to Point Connections Page, page B-116.

Step 2 To remove any interfaces that were previously assigned for this voice role:

a. Click the Remove button in the Advanced section of the page. A page appears, displaying the interfaces assigned for the WAN Point-to-Point voice role.

For more information about this page, see IP Telephony Wizard: Remove Network Elements Page, page B-101.

b. Select the interfaces you want to unassign and click **Remove**. The page closes.

Step 3 Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next**.

The voice policy groups and your WAN-Serial-Point-to-Point interface assignments will be saved, and the next configuration step of the wizard appears (Selecting WAN Frame Relay Connections).

Related Topics

- Using QPM Tables, page 3-8
- Using the IP Telephony Wizard, page 5-7
- Viewing Policy Group Information, page 6-18
- Troubleshooting the IP Telephony Network, page 11-15

Selecting WAN Frame Relay Connections

If the interface connections in the WAN segment of your network support Frame Relay configuration, this step of the wizard allows you to select the Frame Relay DLCI's WAN links. When you assign a role to a DLCI, the role will also be assigned to the interface to which the DLCI belongs. QPM will configure both the DLCIs and the interfaces.

Note The IP Telephony wizard currently supports only Frame Relay to Frame Relay network configuration, and not Frame Relay to ATM devices configuration.

The wizard describes the tools that will be used to configure the QoS settings for these interfaces.

You must select all the Frame Relay interfaces (from both the central and the remote sites) that carry voice traffic. The wizard will automatically configure QoS separately for groups of interfaces, according to their link speed.

Procedure

Step 1 Select the interfaces on which to configure QoS for the Frame Relay WAN links, by selecting the check boxes next to the appropriate Frame Relay interfaces in the list.

For more information about the columns in this table, see IP Telephony Wizard: Select WAN Frame Relay Connections Page, page B-118.

Step 2 To remove any interfaces that were previously assigned for this voice role:

a. Click the Remove button in the Advanced section of the page. A page appears, displaying the interfaces assigned for the WAN Frame Relay voice role.

For more information about this page, see IP Telephony Wizard: Remove Network Elements Page, page B-101.

b. Select the interfaces you want to unassign and click **Remove**. The page closes.

Step 3 Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next**.

The voice policy groups and your WAN-Frame-Relay interface assignments will be saved, and the last step of the wizard appears (End, page 5-23).

Related Topics

- Using QPM Tables, page 3-8
- Using the IP Telephony Wizard, page 5-7
- Viewing Policy Group Information, page 6-18
- Troubleshooting the IP Telephony Network, page 11-15

End

The final step of the IP Telephony wizard informs you that all the QoS settings have been completed and that the wizard has added and saved the policies in the current deployment group.

From this page, you can select to go to the Deployment wizard to deploy the deployment group directly, or to the Policy Groups page to view a detailed summary of all the voice policy groups that were created by the wizard. From the Policy Groups page, you can modify the properties and policies configured in the voice policy groups, if required.

Procedure

Step 1 Select the Yes or No radio button, depending on whether or not you want to deploy your QoS policies.

Step 2 Click **Finish** to close the wizard.

The Policy Groups page or the Deployment wizard appears.

Related Topics

- Modifying Voice Policy Groups, page 5-24
- Modifying a Policy Group, page 6-19
- Chapter 7, "Deploying QoS Policies"

Modifying Voice Policy Groups

After you have completed the IP Telephony wizard, you can modify properties and policies of the voice policy groups created by the voice wizard, to suit a specific network configuration. You can also add nonvoice policies to the default voice policy groups.

Note You cannot modify a voice policy group that is linked to a policy group template. You must disconnect the voice policy group from its template, or modify the template.

After you have completed the IP Telephony wizard and you selected not to deploy your QoS policies directly (see End, page 5-23), the Policy Groups page automatically appears. The Policy Groups page displays all voice policy groups together with non voice policy groups in the current deployment group. For each voice policy group, its associated voice role is displayed.

You can modify any of the properties and policies of a voice policy group, except for its device constraints. Changing the device constraints will cause the voice policy group to lose its voice role. In this case, the IP Telephony wizard will be unable to assign network elements to the voice policy group. You edit a voice policy group just like any policy group. The difference is that when saving, QPM checks the device constraints of the voice policy group. If any changes were made, you must save the voice policy group as a regular policy group without a voice role.

A full description of modifying policy groups is provided in Modifying a Policy Group, page 6-19.

Related Topics

- Using QPM to Configure QoS for IP Telephony, page 5-4

Viewing the Voice Ready Report

The Voice Ready report provides you with an overview of the system's readiness for voice, displaying a list of all the configurable and nonconfigurable devices in the current device group.

The report displays the voice ready status of each device, and the reason for nonvoice readiness, where relevant. For a device to be "voice ready", it must have all the required software and hardware to support QoS for voice and be supported by QPM. Nonconfigurable devices do not have the required software or hardware to support QoS for voice, and/or are not supported by QPM. From this report, you can also view the properties of the devices in the list.

Note Some devices that appear as "voice ready" in the report may not be supported by the IP Telephony wizard. They must be configured manually by QPM.

It is recommended that you view the Voice Ready report after adding or importing the devices in your IP telephony network to QPM's device inventory, so that you can check whether your devices support voice QoS.

In the second step of the IP Telephony wizard, only the devices that support IP telephony features are displayed in a table. Devices that do not support IP telephony are not displayed. By opening the Voice Ready report, you can see all the devices in the current device group, including those that do not support QoS for voice.

Procedure

Step 1 Select **Reports > IP Telephony**. The Voice Ready report appears, displaying the voice status of each device and the reason for non voice readiness, where relevant.

Note You can also open the Voice Ready report by clicking its link in Step 2 of the IP Telephony wizard (see Selecting Devices for QoS Configuration, page 5-11).

For more information about the columns in this table, see Voice Ready Report Page, page D-2.

Step 2 To view details about a device in the table, click the Sys Name link for the required device in the table. The Device Properties page appears for the selected device.

Related Topics

- Introduction, page 5-10
- Selecting Devices for QoS Configuration, page 5-11
- Using QPM Tables, page 3-8
- Viewing and Editing Device Properties, page 4-14

Working with Policy Groups and Policies

A major part of your Quality of Service (QoS) configuration is the definition of policy groups and policies. QoS policies define the QoS actions that will be applied to specific data packets. These policies are managed within policy groups, which are applied to a specified set of network elements.

The following topics provide information about creating and managing policy groups and policies:

Related Topics

- Basic Concepts in QPM, page 1-10

Working with Policy Groups

The following topics describe how to create and work with policy groups in QPM:

Related Topics

Understanding Policy Groups

Policy groups are constrained sets of QoS policies, and assigned network elements. A policy group consists of:

- Device constraints—These are defined by device properties, such as device model, operating system version, network element type, and so on. These constraints determine the QoS features that can be defined in the policy group, and the type of network elements on which the policies can be configured. You can define multiple device constraints in a policy group, but they must all be for the same network element type.
- QoS properties—These include the policy group's scheduling type, and other properties and QoS mappings that are applied to all traffic on the network elements to which they are deployed. The scheduling type can affect the QoS properties that can be defined for the policy group, for example, CRTP, LFI, trust state, and so on.

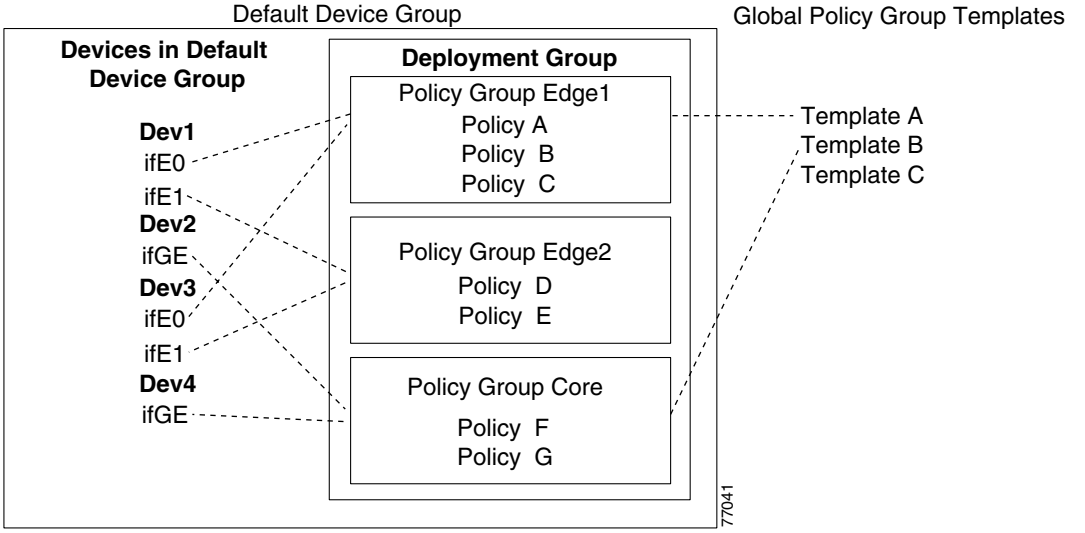
- Assigned network elements—These are the network elements to which the policy group's properties and policies are deployed. A network element can be assigned to only one policy group in a deployment group.
- QoS policies—QoS policies are applied to specific traffic flows entering or leaving the network elements on which they are deployed.

Note Voice policy groups contain the QoS properties and policies for each relevant point in the IP telephony network. Each voice policy group contains a voice role attribute, which specifies the role of an interface, according to its type, function, and location on the network. For more information about voice policy groups, see Chapter 5, "Configuring QoS for IP Telephony."

Policy groups are managed within deployment groups. You can define shared policies across deployment groups by either copying policy group definitions, or by using a global policy group template. Policy group templates are policy group definitions without network element assignments.

Figure 6-1 shows the relationship between a deployment group, its policy groups, policy group templates, and assigned network elements.

Figure 6-1 Relationship between Policy Groups, Policy Group Templates, and Assigned Network Elements



The example deployment group has been created in the San Jose device group. The deployment group contains three policy groups—Edge1, Edge2, and Core. Policy group Edge1 is linked to Policy Group Template A. This means that its policies and properties are inherited from Template A. Policy group Core is linked to Template B. Policy group Edge2 is not linked to a template.

Interfaces ifE0 on Dev1, and ifE0 on Dev3, are assigned to policy group Edge1. This means that the policies in policy group Edge1 will be deployed to those interfaces. Interfaces ifE1 on Dev1, and ifE1 on Dev3, are assigned to policy group Edge2. Different interfaces on a single device can be assigned to different policy groups. Interfaces ifGE on Dev2, and ifGE on Dev4 are assigned to policy group Core.

When working with a policy group, QPM presents you with only those QoS properties and policy actions, and network elements that are valid for the defined device constraints.

For information about the devices and QoS features supported by QPM, see the device support tables at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/qos/qpm3_0/qpm30dev/index.htm

Related Topics

- Creating a Policy Group, page 6-5
- Defining QoS Properties and Mappings, page 6-8
- Setting Network Element Assignments, page 6-13
- Working with Policies, page 6-24
- Copying Policy Groups, page 6-15
- Uploading Device QoS Configurations to Policy Groups, page 6-16
- Working with Policy Group Templates, page 6-41.
- Viewing Policy Group Information, page 6-18
- More Information on Policy Configuration, page 6-50
- Basic Concepts in QPM, page 1-10

Creating a Policy Group

Create a policy group when you want to define a group of QoS properties and policies for a set of device elements with common properties.

This topic describes how to use the Policy Group Definition wizard to create a new policy group in the following ways:

- **Define the policy group's device constraints using the Policy Group Definition wizard**—You can define device constraints manually, or from a set of selected network elements. When you use a set of network elements, QPM uses their common device properties to create one or more device constraint definitions. After you have defined the device constraints, you can continue to define QoS properties and policies, or assign network elements.
- **Link the new policy group to a policy group template**—The policy group you are creating will use the device constraint definitions, and the QoS properties and policies defined for the template. You cannot edit the policy group's properties or policies while it is linked to the template. You can disconnect the template, and then edit the policy group.

- **Copy the device constraints, QoS properties, and policies, from a policy group template**—The policy group is not linked to the template, and you can edit the policy group without affecting the template. Policy group templates do not include network element assignments, so you must assign network elements to the policy group.
- **Copy the device constraints and, optionally, QoS properties and policies, from another policy group**—The source policy group can reside in a different deployment group from the policy group you are creating. You can also copy the device assignments from the source policy group to the new policy group, if the policy groups are in different deployment groups in the same device group.

Procedure

Step 1 Select **Configure > Policy Groups**. The Policy Groups page appears displaying the policy groups for the current deployment group.

To create a policy group in a different deployment group, select the required deployment group in the Deployment Group list box.

Step 2 Click **Create**. The Policy Group Definition wizard opens.

Step 3 In the General Definition page:

a. Enter the name of the new policy group.

b. Enter a description for the policy group (optional).

c. To define device constraints using the wizard, go to step e. To define the policy group using advanced options, click on the triangle next to Advanced. The Advanced field expands.

d. Select how you want to create the policy group, and fill in the appropriate fields.

For more information about the General Definition page fields, see Policy Group Definition Wizard: General Definition Page, page B-40.

e. Click **Next**.

- If you are creating the policy group manually, the Device Constraints page appears. Continue with Step 4.
- If you are creating the policy group from a template, or other policy group, the Capabilities Report page appears. Continue with Step 5.

Note You can also navigate through the wizard using the wizard navigation TOC in the left pane.

Step 4 In the Device Constraints page, define the policy group's device constraint definitions. This determines the QoS features you can use, and the type of network elements that can be assigned to the policy group:

- Click **Define Manually** to define a new constraint manually. The Device Definitions page appears.
  - Define the device constraints. For more information about the fields in this page, see Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43.
  - Click **OK**. The Device Constraints page reappears displaying the new device constraint.
  - Repeat this step to create additional device constraints.

  Note The network element type is the same for all constraints in the policy group and cannot be changed.

- Click **Define from Inventory** to define a new constraint from network elements.
  - Select the device model, and type of network element you want to use to define the device constraint. Click **OK**.
  - In the page that appears, select the network elements you want to use to define the device constraints. For more information about the fields in this page, see Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43.
  - Click **Define Constraint**. The Device Constraints page reappears displaying the new device constraint.
  - Repeat this step to create additional device constraints.

In the Device Constraints page, click **Next**. The Capabilities Report page appears.

Step 5 In the Capabilities Report page, you can view a summary of the QoS features that can be configured for the policy group, according to the device constraints.

For more information about this page, see Policy Group Definition Wizard: Capabilities Report Page, page B-49.

- Click **Finish**. The QoS Properties page appears. See Defining QoS Properties and Mappings, page 6-8.

More Ways to Create Policy Groups

- Copy an existing policy group in the Policy Groups page. See Copying Policy Groups, page 6-15.
- Upload a device's existing QoS configuration into QPM. QPM will convert the device's QoS configuration into policies in new or existing policy groups. See Uploading Device QoS Configurations to Policy Groups, page 6-16.

Related Topics

- Understanding Policy Groups, page 6-2
- Defining QoS Properties and Mappings, page 6-8
- Setting Network Element Assignments, page 6-13
- Modifying a Policy Group, page 6-19
- Working with Policies, page 6-24
- Working with Policy Group Templates, page 6-41
- Viewing Policy Group Information, page 6-18
- More Information on Policy Configuration, page 6-50

Defining QoS Properties and Mappings

A policy group's QoS properties and mappings apply to all flows passing through the interface. QoS properties include scheduling properties, traffic control features, and other QoS features, depending on the device constraints for the policy group. Mappings include NBAR port mappings, DSCP to CoS, CoS to DSCP, IP precedence to DSCP, DSCP to markdown, and excess markdown values.

The following topics describe how to configure QoS properties and mappings for a policy group or a policy group template:

- Defining QoS Properties, page 6-9
- Defining Mappings, page 6-12

Defining QoS Properties

This topic describes how to define QoS properties using the QoS Properties wizard.

The following QoS properties can be configured for a policy group or policy group template (depending on the device constraints):

- Congestion Management—The type of scheduling and the scheduling parameters, if required.
- Shaping Settings:
  - Frame Relay Traffic Shaping (FRTS) parameters
  - Modular Shaping parameters
- Traffic Control Settings:
  - IP RTP priority parameters
  - IP RTP header compression (CRTP) parameters
  - Link Fragmentation and Interleaving (LFI) parameters
  - Voice configuration (FRF) parameters
  - Signaling parameters
  - Trust state parameters
  - QoS style—port-based or VLAN-based
  - Tx ring
  - Inline power—Implements inline power on power-enabled Ethernet line cards.
- Congestion Avoidance—Weighted Random Early Detect (WRED) parameters

After you create a policy group, or policy group template, and define its device constraints using the Policy Group Definition wizard, you can define its QoS properties using the QoS Properties wizard. The QoS Properties wizard lets you

configure only those QoS properties that conform to the device constraints of the policy group. Some QoS properties are inter-dependent, therefore the selection of available QoS properties might change as you proceed through the wizard.

Note When you create a policy group, or policy group template, from another policy group, or policy group template, its QoS properties are defined automatically.

Note The following procedure describes all the pages in the QoS Properties wizard. However, when you define QoS properties, some (or occasionally, all) of the pages or options might not appear, depending on the device constraints for the policy group, or policy group template.

Procedure

Step 1 Open the QoS Properties page in one of the following ways:

- After you finish the Policy Group Definition wizard, click **Finish**.
- In the Policy Groups page, or in the Policy Group Templates page, click the number in the QoS Properties column for the required policy group.
- In the Policy Group TOC, or in the Policy Group Template TOC, select **QoS Properties**.

Step 2 In the QoS Properties page, click **Edit** in the QoS Properties table.

The Scheduling page of the QoS Properties wizard appears.

Step 3 In the Scheduling page:

a. Choose the scheduling type from the list box.

b. Configure the queuing properties, if required. If you do not fill in the queuing property fields, the defaults on the device will be used. For more information about the fields in this page, see QoS Properties Wizard: Congestion Management Page, page B-51.

c. Click **Next** to proceed to the next available page.

Note You can also navigate through the wizard using the wizard navigation TOC in the left pane.

Step 4 In the Shaping Settings page:

a. Configure the FRTS properties, or modular shaping properties. For more information about the fields in this page, see QoS Properties Wizard: Shaping Settings Page, page B-59.

b. Click **Next** to proceed to the next available page.

Step 5 In the Traffic Control Settings page:

a. Configure the Traffic Control properties. For more information about the fields in this page, see QoS Properties Wizard: Traffic Control Settings Page, page B-61.

b. Click **Next** to proceed to the next available page.

Step 6 In the Congestion Avoidance Settings page:

a. Configure the WRED properties. For more information about the fields in this page, see QoS Properties Wizard: Congestion Avoidance Page, page B-66.

b. Click **Next** to proceed to the Summary page.

Step 7 Review the summary page. For more information about the fields in this page, see QoS Properties Wizard: Summary Page, page B-69.

After you are satisfied with the configuration, click **Finish**. The QoS Properties page reappears, displaying the QoS properties you have configured.

You can now do one of the following:

- Define mappings. See Defining Mappings, page 6-12.
- Define policies. See Creating a Policy, page 6-27.
- Assign the policy group to network elements. See Setting Network Element Assignments, page 6-13.

Related Topics

- Defining Mappings, page 6-12
- Viewing Policy Group Information, page 6-18
- Configuring FRTS Policies, page 6-56

Defining Mappings

The following mappings can be configured for a policy group or policy group template (depending on the device constraints):

- NBAR port mappings
- DSCP to markdown and excess markdown tables
- DSCP mapping tables

Procedure

Step 1 Open the QoS Properties page in one of the following ways:

- After you finish the Policy Group Definition wizard, click **Finish**.
- In the Policy Groups page, or in the Policy Group Templates page, click the number in the QoS Properties column for the required policy group.
- In the Policy Group TOC, or in the Policy Group Template TOC, select **QoS Properties**.

The available mappings are displayed in the Mappings table.

Step 2 To configure mappings, or to change the mapping settings, click **Edit** by a mapping. The corresponding Mappings page appears.

If the mapping has been configured, the current mapping settings are displayed.

If the mapping has not been configured, default mapping values are displayed.

See the following topics for more information about these pages:

- NBAR Port Mappings Page, page B-22
- DSCP to CoS Mappings Page, page B-24
- CoS to DSCP Mappings Page, page B-25
- IP Precedence to DSCP Mappings Page, page B-27
- DSCP to Markdown Mappings Page, page B-28
- Excess Markdown Mappings Page, page B-30

Step 3 To save the displayed default mappings, click **Save Defaults**. If the default mappings are not displayed, click **Reset**, then click **Save Defaults**.

Step 4 To configure or change a mapping, click **Create** (NBAR Port Mappings only), or select a mapping and click **Edit**. The corresponding Mapping dialog box opens.

Step 5 Set the mapping as required, and click **OK**.

See the following topics for more information about these dialog boxes:

- NBAR Port Mapping Dialog Box, page B-23
- DSCP to CoS Mapping Dialog Box, page B-25
- CoS to DSCP Mapping Dialog Box, page B-26
- IP Precedence to DSCP Mapping Dialog Box, page B-28
- DSCP to Markdown Mapping Dialog Box, page B-30
- Excess Markdown Mapping Dialog Box, page B-31

The Mappings page reappears displaying the new mapping. Repeat Step 4 and Step 5 to create or edit additional mappings.

Step 6 To delete an entire mapping configuration, click **Delete** in the Mappings page. The QoS Properties page appears.

Step 7 After you have finished configuring mappings, click **Done** in the Mappings page. to return to the QoS Properties page.

Related Topics

- Defining QoS Properties, page 6-9
- Viewing Policy Group Information, page 6-18

Setting Network Element Assignments

After you create a policy group and define its device constraints, you can assign network elements to it. QPM lets you assign only those network elements in the device group that match the policy group's device constraint definitions.

You can change network element assignments. When you assign network elements that are already assigned to a different policy group, QPM automatically removes the previous assignment and saves the new assignment.

You can also remove network element assignments.

Tip To delete the current QoS configuration on a network element, create a policy group with no configuration, and assign the network element to it.

This topic describes how to set network element assignments for the current policy group. You can also set network element assignments from the Device Table. See Setting Device Policy Groups Assignments, page 4-17, and Setting Network Element Assignments, page 6-13 for more information.

Procedure

Step 1 Open the Assigned Network Elements page in one of the following ways:

- In the Policy Groups page, or the Attached Policy Groups page, click in the Network Elements column for the required policy group.
- In the Policy Group TOC, select **Assigned Network Elements**.

The Assigned Network Elements page displays the network elements that have been assigned to the policy group.

Step 2 To assign network elements to the policy group:

a. Click **Add**. The Assignment window opens displaying the network elements in the current device group that match the policy group's device constraints.

b. Select the desired network elements, and click **Assign**. The Assigned Network Elements page reappears, displaying all the network elements assigned to the policy group.

Step 3 To remove network elements from the policy group assignment, select the assigned network elements in the Assigned Network Elements page, and click **Remove**.

See the following topics for more information about these pages:

- Assigned Network Elements Page, page B-35
- Add Assignment Dialog Box, page B-38

Related Topics

- Creating a Policy Group, page 6-5
- Defining QoS Properties and Mappings, page 6-8
- Working with Policies, page 6-24
- Viewing Policy Group Information, page 6-18

Copying Policy Groups

You can create new policy groups by copying existing policy groups. The new policy group contains the source policy group's device constraint definitions, and QoS properties, and, optionally, its policies. If you are copying to a different deployment group within the current device group, you can also copy the source policy group's network element assignments.

The new policy group is given the default name, "Copy of <*source policy group*>." You should rename the policy group with a more meaningful name.

Procedure

Step 1 Select **Configure > Policy Groups**. The Policy Groups page appears displaying the policy groups for the current deployment group.

To change deployment group, select the required deployment group in the Deployment Group list box.

Step 2 Select the check box next to the policy group you want to copy, and click **Copy**. The Copy Policy Group dialog box opens.

Step 3 Choose how to copy the policy group:

a. Select the device group and deployment group to which you want to copy the selected policy group.

b. To copy the properties and policies to the new policy group, select the Copy with policies and properties check box.

c. To copy the network element assignments to the new policy group, select the Copy with assignments check box. This check box is not available if you are copying within a deployment group, or to another device group.

d. Click **OK**. The Policy Groups page reappears.

See Copy Policy Group Dialog Box, page B-17 for more information about the fields in this dialog box.

Step 4 If you copied to a different deployment group, select the required deployment group in the Deployment Group list box, to view the new policy groups.

Related Topics

- Setting Network Element Assignments, page 6-13
- Viewing Policy Group Information, page 6-18
- Modifying a Policy Group, page 6-19

Uploading Device QoS Configurations to Policy Groups

You can upload the existing QoS configurations on devices into QPM policy groups. This is useful if you install QPM in a network where you already have QoS-configured devices.

The upload process incorporates the following steps for each device:

- The configuration that is running on the device is translated to QoS properties and policies.
- For each interface, QPM creates a new policy group containing the policies and properties configured on the interface, and assigns the interface to it.

  If the interface is already assigned to a policy group in the same deployment group, the assignment is deleted before the assignment to the new policy group is set.
- After the upload operation is complete, an HTML report is generated, which you can view in your browser. This report provides:
  - A summary of the new policy groups, and details of the network element assignments to those policy groups.
  - Details of the QoS configurations that were not successfully uploaded. Upload failure may be caused by incomplete configurations that exist on the router, or unsupported options.

Note On deployment, some uploaded QoS configurations might use a different CLI from the original, however the QoS capabilities remain unchanged.

Procedure

Step 1 Select **Configure > Policy Groups**. The Policy Groups page appears displaying the policy groups for the current deployment group.

To upload a device's configuration into a different deployment group, select the required deployment group in the Deployment Group list box.

Step 2 Select **Upload QoS Configuration** in the TOC. The Upload QoS Configuration page appears displaying the list of devices in the current device group.

Step 3 Select the check boxes next to the devices you want to upload, and click **Upload**.

A dialog box appears informing you that the upload process has started.

Step 4 In the Upload dialog box, do one of the following:

- View a report showing the status and other details of the upload process:
  - Click **View**. The Upload Reports page appears.
  - Select the report you want to view, and click **View**. The selected report is displayed in a separate window. See Upload Report, page D-4 for information about the Upload report.

  Note To view a report later, select **Reports > Upload** to display the Reports page.

- Click **Continue** to continue editing policies. The Policy Groups page appears.

Related Topics

- Modifying a Policy Group, page 6-19
- Working with Policies, page 6-24

Viewing Policy Group Information

You can view information about the properties, policies, and network element assignments for a specific policy group. You can then modify the policy group as required.

Procedure

Step 1 Select **Configure > Policy Groups**. The Policy Groups page appears displaying the policy groups for the current deployment group.

To modify a policy group in a different deployment group, select the required deployment group in the Deployment Group list box.

Step 2 To open policy group information pages from the Policy Groups page, do any of the following:

- Click the required policy group name. The General page appears, displaying general definitions for the selected policy group.
- Select a policy group, and click **Edit**. The General page appears, displaying general definitions for the selected policy group.
- Click the number of QoS properties for the required policy group. The QoS Properties page appears, displaying the QoS properties and mappings for the selected policy group.
- Click the number of In policies for the required policy group. The In Policies page appears, displaying the inbound policies for the selected policy group.
- Click the number of Out policies for the required policy group. The Out Policies page appears, displaying the outbound policies for the selected policy group.
- Click the network elements link for the required policy group. The Assigned Network Elements page appears, displaying the network elements that are assigned to the selected policy group.

After you have opened a policy group information page, the TOC changes to the Policy Group TOC.

Step 3 Open any policy group information page from the Policy Group TOC. In addition to the pages referred to in the previous step, you can also open the Device Constraints page, which displays device constraint definitions for the selected policy group.

You can modify policy group details from these information pages.

See the following topics for more information about these pages:

- General Page (Policy Group and Template), page B-17
- Device Constraints Page, page B-19
- QoS Properties Page, page B-20
- In Policies/Out Policies Page, page B-32
- Assigned Network Elements Page, page B-35

Related Topics

- Modifying a Policy Group, page 6-19
- Defining QoS Properties and Mappings, page 6-8
- Setting Network Element Assignments, page 6-13
- Working with Policies, page 6-24

Modifying a Policy Group

Modify a policy group when you want to modify:

- General definitions
- Device constraint definitions:
  - After you define the first device constraint in a policy group, you cannot change the network element type definition. All constraints in a policy group must be for the same network element type. If you want to change the network element type, you must create a new policy group.
  - A policy group must contain at least one constraint definition. You cannot delete a constraint definition if it is the only constraint definition for the policy group.
- QoS properties and mappings—See Defining QoS Properties and Mappings, page 6-8.

- QoS policies—You can add, remove, and edit policies. See Working with Policies, page 6-24.
- Network element assignments—You can add and remove network element assignments. See Setting Network Element Assignments, page 6-13.

Note You cannot modify a policy group that is linked to a policy group template. You must disconnect the policy group from the template, or modify the template. See Disconnecting Policy Groups from Policy Group Templates, page 6-48.

This topic describes how to change a policy group's general definitions, and device constraint definitions.

Procedure

Step 1 Select **Configure > Policy Groups**. The Policy Groups page appears displaying the policy groups for the current deployment group.

To modify a policy group in a different deployment group, select the required deployment group in the Deployment Group list box.

The Policy Groups page displays for each policy group, the number of QoS properties, and the number of QoS policies it contains, and the number of assigned network elements.

For policy groups that are linked to templates, the linked template name is displayed, and the properties and policies are shown as "inherited." For more information about the Policy Groups page, see Policy Groups Page, page B-14.

Step 2 To edit the general definitions for the policy group:

a. Click the required policy group name, or select the required policy group, and click **Edit**.

The General page appears for the selected policy group. The TOC changes to the Policy Group TOC.

b. Click **Edit** in the General page.

The Policy Group Definition wizard opens, displaying the General Definition page.

c. Edit the name and description in the General Definition page, as required.

Step 3 To add, edit, or remove device constraint definitions, open the Device Constraints page in the Policy Definition wizard in one of the following ways:

- If the Policy Group Definition wizard is open, continue to the Device Constraints Definition page.
- Select Device Constraints in the Policy Group TOC. The Device Constraints page appears. Click **Edit**. The Policy Group Definition wizard opens, displaying the Device Constraint Definition page.

Modify device constraint definitions as required:

- To edit an existing constraint:
  - Select the constraint definition, and click **Edit**. The Device Definitions page appears.
  - Edit the device constraints. For more information about the fields in this page, see Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43.

    Note You cannot change the network element type after it has been defined for the first device constraint in the policy group.

  - Click **OK**. The Device Constraints page reappears displaying the modified device constraint.
- To delete an existing constraint definition:
  - Select the constraint definition, and click **Delete**.

    Note A policy group must contain at least one constraint definition. You cannot delete a constraint definition if it is the only constraint definition for the policy group.

- To create a new constraint manually:
  - Click **Define Manually**. The Device Definitions page appears.
  - Define the device constraints. For more information about the fields in this page, see Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43.

Note You cannot change the network element type after it has been defined for the first device constraint in the policy group.

- Click **OK**. The Device Constraints page reappears displaying the new device constraint.

- To define a new constraint from network elements:
  - Click **Define from Inventory**.
  - Select the type and model of network element to use to define the device constraint. Click **OK**.

Note You cannot change the network element type after it has been defined for the first device constraint in the policy group.

  - Select the network elements you want to use to define the device constraints. For more information about the fields in this page, see Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43.
  - Click **Define Constraint**. The Device Constraints page reappears displaying the new device constraint.

Step 4 After you have completed your policy group definitions, click **Finish** to exit the Policy Group Definition wizard.

Related Topics

- Creating a Policy Group, page 6-5
- Viewing Policy Group Information, page 6-18
- Defining QoS Properties and Mappings, page 6-8
- Setting Network Element Assignments, page 6-13
- Working with Policies, page 6-24
- Working with Policy Group Templates, page 6-41

Deleting a Policy Group

Delete a policy group when you no longer want to apply its QoS properties and policies to any of the assigned devices.

Note When you delete a policy group, all its contents are deleted.

Procedure

Step 1 Select **Configure > Policy Groups**. The Policy Groups page appears displaying the policy groups for the current deployment group.

To delete a policy group in a different deployment group, select the required deployment group in the Deployment Group list box.

Step 2 Select the policy group you want to delete, and click **Delete**. A warning message appears.

Step 3 Click **OK** to confirm the deletion. The policy group and its contents are deleted.

Related Topics

- Viewing Policy Group Information, page 6-18
- Modifying a Policy Group, page 6-19

Viewing Policy Translations

You can view the CLI translations of the QoS configurations that will be deployed to devices assigned to policy groups in the current deployment group.

Procedure

Step 1 Select **Configure > Policy Groups**. The Policy Groups page appears displaying the policy groups for the current deployment group.

To view policy translations for a different deployment group, select the required deployment group in the Deployment Group list box.

Step 2 In the TOC, select **View CLI Translation**. The Policy Translation page appears, displaying the list of devices that have assigned network elements to policy groups in the current deployment group. See Policy Translation Page, page B-91 for more information about this page.

Step 3 Select the check box(es) next to the device(s) whose policy translation you want to view. Click **Translate**. The Translate page appears, displaying the CLI translation for the device(s). See Translation Report Page, page B-92 for more information about this page.

Related Topics

- Viewing Policy Group Information, page 6-18
- Modifying a Policy Group, page 6-19

Working with Policies

Your policies define the QoS actions that are to be applied to specific traffic flows.

The following topics describe how to create and manage policies:

Understanding Policies

After you have defined a policy group or policy group template with device constraints and QoS property definitions, you can add policies to it.

Using QPM, you can create the following types of policies:

- QoS policies—A *QoS policy* is a conditional statement that applies one or more specified QoS actions to a packet if the packet satisfies the conditions (filters) defined in the policy.
- Access control policies—An *access control policy* permits or denies the flow of data if the data packet satisfies the conditions (filters) defined in the policy. An access control policy does not have an associated QoS action.

Note You cannot create access control policies on all Cisco devices.

The filter you create for a policy can be broad, in which case the policy is applied to a high percentage of the traffic that travels through the device or interface, or it can be very narrow and selective. When the device determines that a packet satisfies the conditions of the policy, it applies the policy's action to it.

In general, if there is more than one policy defined on the interface or device, the device looks at the policies in order, top to bottom, until the first match is found, at which point it applies the policy and ignores remaining policies. (If you are creating an advanced policing policy, however, you can specify that additional policies be considered after the device applies a matching policy.)

When you define policies, QPM presents you with only actions and settings that are valid for the device constraints and QoS properties defined for the policy group.

You can enable and disable policies without deleting them, and you can change the order in which policies are checked on the interface.

Related Topics

- What Types of Quality of Service Does QPM Handle?, page 2-3
- Creating a Policy, page 6-27
- Modifying a Policy, page 6-34

Displaying the Policies Pages

Your starting point for working with policies, is the lists of policies in the policy group or policy group template. Inbound policies and outbound policies are displayed in separate pages.

The following topics describe how to display policies:

Displaying Policies in a Policy Group

You access the policies for a policy group from the Policy Groups page.

Procedure

Step 1 Select **Configure > Policy Groups**. The Policy Groups page appears displaying the policy groups for the current deployment group.

Step 2 To view policies in a different deployment group, select the required deployment group in the Deployment Group list box.

Step 3 In the Policy Groups page, click the number of In or Out policies for the required policy group.

The In Policies or Out Policies page appears, displaying the inbound or outbound policies in the current policy group.

Note If the Policy Group TOC is displayed, you can select **In Policies**, or **Out Policies**, as required.

Displaying Policies in a Policy Group Template

You access the policies for a policy group from the Policy Group Templates page.

Step 1 Select **Configure > Libraries**.

Step 2 In the Libraries TOC, select **Templates**. The Templates page appears displaying the policy group templates.

Step 3 In the Templates page, click the number of In or Out policies for the required template.

The In Policies or Out Policies page appears, displaying the inbound or outbound policies in the template.

Note If the Templates TOC is displayed, you can select **In Policies**, or **Out Policies**, as required.

Related Topics

- Creating a Policy, page 6-27
- Modifying a Policy, page 6-34
- Enabling and Disabling Policies, page 6-35
- Changing the Priority of Policies, page 6-36

Creating a Policy

Create a QoS policy to apply specific QoS actions to selected traffic flows. Create an access control policy to permit or deny specific classes of traffic. Access control policies do not contain any associated actions.

You can create policies in a policy group, or in a policy group template.

The QPM Policy wizard guides you through the following steps required to define policies in the inbound or outbound direction:

- General Policy Definition, page 6-28
- Defining a Policy Filter, page 6-29

- Defining QoS Policy Actions, page 6-31
- Viewing the Policy Summary, page 6-33

General Policy Definition

The general policy definition for inbound or outbound policies includes the following:

- Policy name
- Policy description
- Type of policy—QoS policy or access control policy (if relevant)

Procedure

Step 1 Open the In Policies or Out Policies page for the policy group or policy group template in which you want to create a new policy. See Displaying the Policies Pages, page 6-26.

Step 2 In the Policies page, click **Create**. The Policy wizard opens, displaying the Policy Wizard - General page.

Step 3 In the Policy Wizard - General page:

- Enter the policy name.
- Enter a description for the policy, if desired.
- Select the type of policy you want to create—QoS policy, or access control policy.

Step 4 Click **Next** to proceed to the Filter step in the wizard. See Defining a Policy Filter, page 6-29.

Related Topics

- Defining QoS Policy Actions, page 6-31
- Viewing the Policy Summary, page 6-33

Defining a Policy Filter

Define a filter to specify the traffic to which the policy should be applied. A filter can contain multiple filter *rules*. Each filter rule is a set of filter *conditions*—to satisfy the rule, a packet must satisfy *all* conditions of the rule. To match the filter, a packet must satisfy *any* one of the rules.

The available filter elements change according to the policy group's device constraints and congestion management properties. Typically, you can identify the traffic by any of the following characteristics:

- Source IP or destination IP. You can use IP aliases from the QPM component libraries.
- Source application or destination application. You can use application aliases from the QPM component libraries.
- Service—IP precedence or DSCP value.

In addition, you might be able to filter using:

- Network Based Application Recognition (NBAR) properties—NBAR is a classification engine that recognizes a wide variety of applications, including web-based and other difficult-to-classify protocols that utilize dynamic TCP/UDP port assignments. When an application is recognized and classified by NBAR, a network can invoke services for that specific application.
- IP RTP ports
- CoS value
- MPLS value

You can also define a class default filter for unclassified traffic that does not match any other filter condition.

The Policy wizard guides you through the process of defining filter conditions and rules for your policy.

Procedure

Step 1 Open the Policy Wizard - Filter page:

- If the Policy wizard is not open, open the relevant Policies page. See Displaying the Policies Pages, page 6-26. Select the policy whose filter you want to edit, and click Edit. The Policy wizard opens, displaying the Policy Wizard - General page.
- If the Policy wizard is open, click **Next** in the Policy Wizard - Filter page, or select **Filter** in the wizard navigation TOC.

Step 2 Enter a name for the filter, if desired. The filter name helps you identify the defined filter in the CLI translation.

Step 3 Select how to define the traffic type of the policy:

- Create New Filter—This policy is applied to traffic that matches any of the filter conditions. If you do not define filter rules, the policy is applied to all traffic.
- Class Default—This policy is applied to all traffic that does not match any of the filters. You do not create any filter conditions for this type of policy. Go to Step 8.

Step 4 Define a filter rule:

a. Click **Create** in the Filters table. The Rule Setting page appears, displaying the conditions you can define for each filter rule.

b. Click **Edit** next to the condition you want to define. A dialog box opens.

c. Define the condition as required.

See the following topics for information about these dialog boxes:

- Source IP / Destination IP Dialog Box, page B-77
- Application Dialog Box, page B-74
- Protocol Dialog Box, page B-75
- CoS Dialog Box, page B-78
- MPLS Dialog Box, page B-79
- Service Dialog Box, page B-78
- IP-RTP Port Range Dialog Box, page B-79

Note For IP and application conditions, you can choose a predefined alias. You can also save a defined condition as an alias in the QPM libraries for future use.

d. Click **OK** in the Condition dialog box. The Rule Setting table reappears.

e. Repeat steps b through d to create additional conditions for the filter rule.

f. After you have defined all the rules in the filter condition, click **Done**. The Filter page reappears displaying the filter rule you have defined.

Step 5 Repeat Step 4 to create additional filter rules.

Step 6 To edit a filter rule, select the filter rule in the Filter page, and click **Edit**. The Rule Setting page appears. Edit the rule conditions as required, and click **Done** to return to the Filter page.

Step 7 To delete a filter rule, select the filter rule in the Filter page, and click **Delete**.

Step 8 After you have completed your filter definitions, click **Next**.

- If you are defining a QoS policy, the Policy Wizard - Actions page appears. See Defining QoS Policy Actions, page 6-31.
- If you are defining an access control policy, the Summary page appears. See Viewing the Policy Summary, page 6-33.

Related Topics

- General Policy Definition, page 6-28
- Working with Aliases, page 6-38

Defining QoS Policy Actions

The Policy Actions step of the Policy wizard includes several substeps to define the actions to be applied to traffic that matches the filter definition:

- **Marking**—Defines a packet's relative importance. The marking can be used to identify and prioritize packets in subsequent policies.
- **Microflow Policing**—Limits the input transmission rate of traffic, and marks packets.

- **Policing**—Limits the rate of aggregate flows on a single interface or across interfaces.
- **Shaping**—Smooths the flow of outbound traffic.
- **Queuing**—Provides bandwidth guarantees and priority servicing for outbound traffic.
- **Congestion Avoidance**—Discards packets to avoid congestion.

Note Cisco Express Forwarding (CEF) must be enabled on a device if you want to deploy NBAR or class-based QoS policies. On VIP platforms, distributed CEF (dCEF) must be enabled.
The global CLI command to enable CEF or dCEF is:
ip cef [distributed] switch

The following procedure describes all the available actions in the Policy Wizard - Actions step. However, when you define actions for a policy, some of the options might not appear, depending on the device constraints and QoS properties of the policy group.

Procedure

Step 1 Open the Policy Wizard - Actions page:

- If the Policy wizard is not open, open the relevant Policies page. See Displaying the Policies Pages, page 6-26. Select the policy whose action you want to edit, and click Edit. The Policy wizard opens, displaying the Policy Wizard - General page.
- If the Policy wizard is open, click **Next** in the Policy Wizard - Filter page, or select **Actions** in the wizard navigation TOC. The Policy Wizard - Actions page for Marking appears.

Step 2 Use the Next button to navigate to the action pages you want to define, or select the actions in the wizard navigation TOC:

See the following topics for information about these dialog boxes:

- Policy Wizard: Marking Actions Page, page B-80
- Policy Wizard: Microflow Policing Actions Page, page B-81
- Policy Wizard: Policing Actions Page, page B-83

- Policy Wizard: Shaping Actions Page, page B-86
- Policy Wizard: Congestion Avoidance Actions Page, page B-90

Step 3 After you have completed defining the policy actions, click **Next** to proceed to the Summary step in the Wizard. See Viewing the Policy Summary, page 6-33.

Related Topics

- General Policy Definition, page 6-28
- Defining a Policy Filter, page 6-29

Viewing the Policy Summary

After you have finished defining your policy, review the policy definitions in the Summary page. You can go back and revise definitions before completing the Policy Definition wizard.

Procedure

Step 1 If the Policy Wizard - Summary page is not displayed, select **Summary** in the wizard navigation TOC.

Step 2 Review the policy definitions.

Step 3 To modify any of the settings, choose the relevant step in the wizard navigation TOC, or click the Back button.

Step 4 After you are satisfied with the policy definition, click **Finish** to complete the policy and exit the wizard.

Related Topics

- General Policy Definition, page 6-28
- Defining a Policy Filter, page 6-29
- Defining QoS Policy Actions, page 6-31

Modifying a Policy

You can modify a policy by changing its properties, filter, or actions. When you redeploy the policies, the modified policy replaces the old policy on the policy group's assigned network elements.

You cannot modify policies within a policy group that is linked to a policy group template. You must either disconnect the policy group template first, or modify the policy group template.

Procedure

Step 1 Open the In Policies or Out Policies page for the policy group or policy group template in which you want to modify a policy. See Displaying the Policies Pages, page 6-26.

Step 2 In the Policies page, select the check box next to the policy you want to edit, and click **Edit**. The Policy wizard opens, displaying the Policy Wizard - General page. Change the name or description of the policy if required.

Step 3 Navigate to pages you want to edit using the wizard Next button, or by choosing a step in the wizard navigation TOC:

- To modify the policy filter, see Defining a Policy Filter, page 6-29.
- To modify the policy actions, see Defining QoS Policy Actions, page 6-31.

Step 4 After you have finished editing the policy click **Finish**. The Policy Wizard - Summary page appears. See Viewing the Policy Summary, page 6-33.

Related Topics

- Working with Aliases, page 6-38
- Working with Policy Group Templates, page 6-41

Deleting Policies

When you no longer want to use a policy, you can delete it from the policy group or policy group template. When you redeploy the policies, the deleted policy is removed from the policy group's assigned network elements.

You cannot delete a policy in a policy group that is linked to a policy group template. You must either first disconnect the policy group template, or delete the policy in the linked policy group template.

Before You Begin

If you are not sure whether you will need a policy, consider disabling it instead of deleting it. See Enabling and Disabling Policies, page 6-35 for information on disabling a policy.

Procedure

Step 1 Open the In Policies or Out Policies page for the policy group or policy group template in which you want to delete a policy. See Displaying the Policies Pages, page 6-26.

Step 2 In the Policies page, select the check box(es) next to the policy or policies you want to delete. Click **Delete**.

Related Topics

- Enabling and Disabling Policies, page 6-35

Enabling and Disabling Policies

When you create a policy, it is enabled by default, so that when you deploy to the devices, the policy is distributed and takes effect. However, you can disable a policy, so that it exists in the policy group, but is not deployed to the network. This allows you to define policies before you want to make them effective, or temporarily remove a policy from the network without erasing it completely. You can also enable policies that have been disabled.

Procedure

Step 1 Open the In Policies or Out Policies page for the policy group or policy group template in which you want to work. See Displaying the Policies Pages, page 6-26.

Step 2 In the Policies page, select the check box(es) next to the policy or policies you want to enable or disable.

Step 3 Click **Enable** or **Disable** as required.

Changing the Priority of Policies

The device examines QoS policies in order until a match is found for the packet. Even if a packet satisfies more than one policy, it will be treated as satisfying only the first policy that the device encounters, unless you define your policy to include the Continue setting, in which case a subsequent match will be sought.

Policies on an interface are examined top-down according to the QPM display. Therefore the policies in a policy group should appear in order of importance, from top to bottom, to ensure that policies get the priority you require. If you are creating complex policy structures that include Continue settings (so that you can set multiple policies on a given packet), ensure that the statements with the Continue setting come before the subsequent policy statement you want applied.

Initially, policies are listed in the order in which they are defined. You can change the order of policies in the list.

Procedure

Step 1 Open the In Policies or Out Policies page for the policy group or policy group template in which you want to reorder policies. See Displaying the Policies Pages, page 6-26.

Step 2 In the Policies page, click **Reorder**. The Reorder dialog box opens.

Step 3 Select the policy that you want to reorder. Click the Up or Down button to reorder the policy as required.

Step 4 Change the order of policies as required. After you have finished, click **Reorder**. The Policies page appears displaying the new order.

Searching for QoS Properties and Policies

You can search for QoS properties and policies in policy groups or policy group templates. When searching for policy groups, you can search within a single deployment group, or across all deployment groups.

Procedure

Step 1 Select **Configure > Search**. The Policy/Properties Search page appears.

Step 2 Select whether to search in policy groups, or in policy group templates. To search in policy groups, select the deployment group in which you want to search, or select Select All to search in all deployment groups.

Step 3 Select the type of search:

- Select **Policy** to search for policies, according to policy name and/or policy action. Enter search criteria as required.
- Select **Properties** to search for QoS properties. Select the QoS property for which to search.

See Policy/Properties Search Page, page B-122 for more information about fields in this page.

Step 4 Click **Search**. After the search is complete, the Search Results page appears, displaying information for the policies or properties, that match the search criteria.

See Policy Search Results Page, page B-123 for information about fields in the Policy Search Results page.

See Properties Search Results Page, page B-124 for information about fields in the Properties Search Results page.

See Templates Policies Search Results Page, page B-125 for information about fields in the Templates Policies Search Results page.

See Templates Properties Search Results Page, page B-125 for information about fields in the Templates Properties Search Results page.

Working with Aliases

Definitions of IP aliases, and application aliases, can be stored in QPM libraries, and used in policy definitions across all your deployment groups. When you change the alias definition, all policies that reference the definition are affected.

When you deploy historical jobs with referenced alias definitions, QPM performs a validation check on the referenced definitions. See Chapter 7, "Deploying QoS Policies".

The following topics describe how to work with alias definitions:

- Defining IP Aliases, page 6-38
- Defining Application Aliases, page 6-39
- Modifying Aliases, page 6-40
- Deleting Aliases, page 6-41

Defining IP Aliases

An IP alias is an alias for a named group of IP addresses (including masks) or hostnames. It can be used for both source IP and destination IP conditions within a filter. IP aliases are stored in the IP Aliases library.

Procedure

Step 1 Select **Configure > Libraries**, or if you have been working with other library items, select **IP Aliases** in the Libraries TOC.

The IP Aliases page appears, displaying IP alias definitions in the IP Alias library.

Step 2 Click **Create**. The IP Alias dialog box opens.

Step 3 Enter the IP alias name in the Name field.

Step 4 For each IP address you want to add to the alias:

a. Enter the IP address and mask, or enter host name.

b. Click **Add** to add the IP address to the alias. The IP address and mask are displayed in the Alias list.

To remove an IP address that you added, select the IP address in the list, and click **Remove**.

For more details, see IP Alias Dialog Box, page B-5.

Step 5 After you have added all the IP addresses to the alias, click **OK**. The IP Alias page displays the new alias.

Related Topics

- Modifying Aliases, page 6-40
- Deleting Aliases, page 6-41

Defining Application Aliases

An application alias is an alias for a defined protocol and port (or group of ports). It can be used in a filter definition for source and destination application conditions. Application aliases are stored in the Application Aliases library.

Procedure

Step 1 Select **Configure > Libraries**.

Step 2 Select **Applications** in the Libraries TOC. The Applications page appears displaying application alias definitions in the Applications library.

Step 3 Click **Create**. The Application Alias dialog box opens.

Step 4 Enter the Application alias name in the Name field.

Step 5 Define the protocol, and TCP/UDP port or range, if appropriate.

For more details, see Application Alias Dialog Box, page B-7.

Step 6 Click **OK**. The Applications page reappears displaying the application alias.

Related Topics

- Modifying Aliases, page 6-40
- Deleting Aliases, page 6-41

Modifying Aliases

You can change IP aliases and application aliases. When you modify an alias, all policies that reference it, are modified.

Procedure

Step 1 Select **Configure > Libraries**.

Step 2 In the Libraries TOC, select the library that contains the alias you want to modify.

Step 3 Select the check box next to the alias you want to modify, and click **Edit**. The Alias dialog box opens, displaying details for the alias.

Step 4 Modify fields as required.

For more details, see:

- IP Alias Dialog Box, page B-5
- Application Alias Dialog Box, page B-7

Step 5 Click **OK** in the dialog box. The Alias page displays the modified alias.

Related Topics

- Defining IP Aliases, page 6-38
- Defining Application Aliases, page 6-39

Deleting Aliases

You can delete aliases if they are not currently being used in policies.

Procedure

Step 1 Select **Configure > Libraries**.

Step 2 In the Libraries TOC, select the library that contains the aliases you want to delete.

Step 3 Select the check boxes next to the alias(es) you want to delete.

Step 4 Click **Delete**.

Working with Policy Group Templates

Policy group templates contain QoS properties and policies, but do not contain network element assignments. Policy group templates can be used to create policy groups in any deployment group. You can create global policy group templates and store them in the Policy Group Templates library.

The following topics describe how to work with policy group templates:

Understanding Policy Group Templates

Policy group templates can be used to create and share policy groups across deployment groups and device groups. A policy group template contains a set of QoS properties and QoS policies for specified device constraints. It does not include any device assignments. Policy group templates are stored in the Policy Group Templates library.

You can create policy groups by copying policy group templates, or by attaching the policy group template to the policy group. When a policy group template is attached to policy groups, any change in the policy group template will affect the attached policy groups. You can disconnect policy groups from their attached policy group template at any time.

QPM generates voice policy group templates, which are used to create voice policy groups for IP telephony QoS configuration. You can edit the voice policy group templates created by QPM.

Related Topics

- Creating a Policy Group Template, page 6-43
- Modifying a Policy Group Template, page 6-45
- Viewing Policy Group Template Information, page 6-43
- Disconnecting Policy Groups from Policy Group Templates, page 6-48
- Deleting Policy Group Templates, page 6-50
- Chapter 5, “Configuring QoS for IP Telephony”

Creating a Policy Group Template

Create a policy group template when you want to share policies across deployment groups or device groups.

You create a new policy group template in the same way as you create a new policy group using the Policy Group Definition wizard. You can create a new template by copying another template or a policy group.

Procedure

Step 1 Create a new policy group template and define its device constraints. See Creating a Policy Group, page 6-5.

Step 2 Define the policy group template's QoS properties and mappings. See Defining QoS Properties and Mappings, page 6-8.

Step 3 Define policies for the policy group template. See Creating a Policy, page 6-27.

Related Topics

- Viewing Policy Group Template Information, page 6-43
- Modifying a Policy Group Template, page 6-45
- Deleting Policy Group Templates, page 6-50

Viewing Policy Group Template Information

You can view information about the QoS properties and policies for a specific policy group template. You can then modify the policy group template as required.

You can also view the policy groups that are attached to a policy group template, and you can then disconnect a policy group from its template.

Procedure

Step 1 Select **Configure > Libraries**.

Step 2 Select **Templates** in the Libraries TOC. The Templates page appears displaying the global policy group templates.

Step 3 To open policy group template information pages from the Templates page, do any of the following:

- Click the required template name. The General page appears, displaying general definitions for the selected policy group template.
- Click the number of QoS properties for the required policy group template. The QoS Properties page appears, displaying the QoS properties and mappings for the selected policy group template.
- Click the number of In policies for the required policy group template. The In Policies page appears, displaying the inbound policies for the selected policy group template.
- Click the number of Out policies for the required policy group template. The Out Policies page appears, displaying the outbound policies for the selected policy group template.

After you have opened a policy group template information page, the TOC changes to the Template TOC.

Step 4 Open any policy group template information page from the Template TOC. In addition to the pages referred to in the previous step, you can also open the Device Constraints page, which displays device constraint definitions for the selected policy group template.

You can modify policy group template details from these information pages.

Step 5 To view a template's attached policy groups, click the number of attached policy groups for the required policy group template. The Attached Policy Groups page appears, displaying the list of attached policy groups.

You can disconnect a policy group from its template in this page.

Related Topics

- Modifying a Policy Group Template, page 6-45
- Deleting Policy Group Templates, page 6-50
- Disconnecting Policy Groups from Policy Group Templates, page 6-48

Modifying a Policy Group Template

Modify a policy group template when you want to modify:

- General definitions
- Device constraint definitions:
  - After you define the first device constraint in a policy group template, you cannot change the network element type definition. All constraints in a policy group template must be for the same network element type. If you want to change the network element type, you must create a new policy group.
  - A policy group template must contain at least one constraint definition. You cannot delete a constraint definition if it is the only constraint definition for the policy group template.
- QoS properties and mappings—See Defining QoS Properties and Mappings, page 6-8.
- QoS policies—You can add, remove, and edit policies. See Working with Policies, page 6-24.

Note If a policy group template is attached to policy groups, any change in the policy group template will affect the attached policy groups. For information on disconnecting a policy group from its attached template, see Disconnecting Policy Groups from Policy Group Templates, page 6-48.

This topic describes how to change a policy group template's general definitions, and device constraint definitions.

Procedure

Step 1 Select **Configure > Libraries**.

Step 2 Select **Templates** in the Libraries TOC. The Templates page appears displaying the global policy group templates.

Step 3 To edit the general definitions for the policy group template:

a. Open the Policy Group Definition wizard in one of the following ways:

- Select the required policy group template, and click **Edit**.
- If you want to view general information first, click the required policy group template name. The General page appears for the selected template. The TOC changes to the Template TOC. Click **Edit** in the General page.

The Policy Group Definition wizard opens, displaying the General Definition page.

b. Edit the name and description in the General Definition page, as required.

Step 4 To add, edit, or remove device constraint definitions, open the Device Constraints page in the Policy Definition wizard in one of the following ways:

- If the Policy Group Definition wizard is open, continue to the Device Constraints Definition page.
- Select Device Constraints in the Policy Group TOC. The Device Constraints page appears. Click **Edit**. The Policy Group Definition wizard opens, displaying the Device Constraint Definition page.

Modify device constraint definitions as required:

- To edit an existing constraint:
  - Select the constraint definition, and click **Edit**. The Device Definitions page appears.
  - Edit the device constraints. For more information about the fields in this page, see Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43.

Note You cannot change the network element type after it has been defined for the first device constraint in the policy group.

  - Click **OK**. The Device Constraints page reappears displaying the modified device constraint.

- To delete an existing constraint definition:
  - Select the constraint definition, and click **Delete**.

    Note A policy group must contain at least one constraint definition. You cannot delete a constraint definition if it is the only constraint definition for the policy group.

- To create a new constraint manually:
  - Click **Define Manually**. The Device Definitions page appears.
  - Define the device constraints. For more information about the fields in this page, see Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43.

    Note You cannot change the network element type after it has been defined for the first device constraint in the policy group.

  - Click **OK**. The Device Constraints page reappears displaying the new device constraint.
- To define a new constraint from network elements:
  - Click **Define from Inventory**.
  - Select the type and model of network element to use to define the device constraint. Click **OK**.

    Note You cannot change the network element type after it has been defined for the first device constraint in the policy group.

  - Select the network elements you want to use to define the device constraints. For more information about the fields in this page, see Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43.
  - Click **Define Constraint**. The Device Constraints page reappears displaying the new device constraint.

Step 5 After you have completed modifying your policy group template definitions, click **Finish** to exit the Policy Group Definition wizard.

Related Topics

- Viewing Policy Group Template Information, page 6-43
- Deleting Policy Group Templates, page 6-50
- Modifying a Policy Group, page 6-19

Disconnecting Policy Groups from Policy Group Templates

You can disconnect an individual policy group from its template, and you can disconnect several policy groups from a policy group template.

The following topics describe how to disconnect policy groups from templates:

- Disconnecting an Individual Policy Group from its Template, page 6-48
- Disconnecting Several Policy Groups from a Template, page 6-49

Disconnecting an Individual Policy Group from its Template

This topic describes how to disconnect an individual policy group from its policy groups template.

Procedure

Step 1 Select **Configure > Policy Groups**. The Policy Groups page appears displaying the policy groups for the current deployment group.

Step 2 Click the policy group name, or select the required policy group, and click **Edit**.

The General page appears for the selected policy group. The TOC changes to the Policy Group TOC.

Step 3 In the Attached to Template field, click **Disconnect**.

Related Topics

- Disconnecting Several Policy Groups from a Template, page 6-49
- Modifying a Policy Group Template, page 6-45
- Deleting Policy Group Templates, page 6-50

Disconnecting Several Policy Groups from a Template

This topic describes how to disconnect one or more policy groups from the Policy Groups Templates page.

Procedure

Step 1 Select **Configure > Libraries**.

Step 2 Select **Templates** in the Libraries TOC. The Templates page appears displaying the global policy group templates.

Step 3 To view a template's attached policy groups, click the number of attached policy groups for the required policy group template. The Attached Policy Groups page appears, displaying the list of attached policy groups.

Step 4 Select the policy group to disconnect, and click **Disconnect**.

Related Topics

- Disconnecting an Individual Policy Group from its Template, page 6-48
- Modifying a Policy Group Template, page 6-45
- Deleting Policy Group Templates, page 6-50

Deleting Policy Group Templates

You can delete policy group templates that are not attached to any policy groups.

Procedure

Step 1 Select **Configure > Libraries**.

Step 2 In the Libraries TOC, select the Policy Group Templates. The Templates page appears.

Step 3 Select the check boxes next to the template or templates you want to delete.

Step 4 Click **Delete**.

Related Topics

- Disconnecting Policy Groups from Policy Group Templates, page 6-48

More Information on Policy Configuration

This section provides additional information about configuring QoS on different types of interfaces and devices:

- QoS Configuration on Network Element Types, page 6-51
- Configuring FRTS Policies, page 6-56
- Configuring VLAN Policies, page 6-58

QoS Configuration on Network Element Types

Policy groups can be assigned to only one type of network element. For some devices, you will need to define several policy groups to consolidate the QoS configuration on the device.

To create a complete QoS configuration for a single type of network element, you might need to define more than one policy group. For example, when configuring FRTS policies, and when configuring VLAN policies.

There are other cases, where you might need two policy groups. For example, you configure markdown in policing policies on Catalyst ports at the port level, but to change the default markdown mapping values, you must define an additional policy group at the device level.

This section provides tables listing the types of QoS configurations that can be configured for each network element type, for different device models:

- Types of QoS Configurations on IOS Devices
- Types of QoS Configurations on Catalyst Devices
- Types of QoS Configurations on Layer 2 Switches Running IOS
- Types of QoS Configurations on Layer 3 Devices

Table 6-1 Types of QoS Configurations on IOS Devices

	Network Element Type				
Device Model	**Device**	**Interface**	**VC**	**DLCI**	**VLAN**
1600	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
1720	No QoS configuration at device level.	Scheduling Properties, Actions	Not available	Scheduling Properties Actions	Not available
1750	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties: Actions	Not available

Table 6-1 Types of QoS Configurations on IOS Devices (continued)

	Network Element Type				
Device Model	**Device**	**Interface**	**VC**	**DLCI**	**VLAN**
2500	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
2600	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties: Actions	Not available
3600	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties: Actions	Scheduling Properties Actions	Not available
3800	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions:	Not available
4000	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
4500	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
4700	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
7100	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling: Properties Actions	Not available

Table 6-1 Types of QoS Configurations on IOS Devices (continued)

	Network Element Type				
Device Model	**Device**	**Interface**	**VC**	**DLCI**	**VLAN**
7200	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties: Actions	Not available
7400	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling: Properties Actions	Not available
7500	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
7600	DSCP Mappings NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Actions **Note:** VLAN scheduling is inherited from its ports.
7700	No QoS configuration at device level.	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling: Properties Actions	Not available
AS5300	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
AS5800	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
C4GWY	No QoS configuration at device level.	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available

Table 6-1 Types of QoS Configurations on IOS Devices (continued)

	Network Element Type				
Device Model	**Device**	**Interface**	**VC**	**DLCI**	**VLAN**
Cat3550	DSCP Mappings	Scheduling Properties Actions	Not available	Not available	DSCP Mappings Actions **Note:** VLAN scheduling is inherited from its ports.
Cat4200	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
Cat6000_PFC1 (IOS)	DSCP Mappings NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Actions **Note:** VLAN scheduling is inherited from its ports.
Cat6000_PFC2 (IOS)	DSCP Mappings NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Actions **Note:** VLAN scheduling is inherited from its ports.
MSFC (QoS is supported on the FlexWan module only)	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available

Table 6-1 Types of QoS Configurations on IOS Devices (continued)

Device Model	Network Element Type				
	Device	**Interface**	**VC**	**DLCI**	**VLAN**
RSM	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
VG200	No QoS configuration at device level.	Scheduling Properties Actions	Scheduling Properties Actions:	Scheduling Properties Actions:	Not available

Table 6-2 Types of QoS Configurations on Catalyst Devices

Device Model	Network Element Type		
	Device	**Interface**	**VLAN**
Cat4000	Scheduling Actions	Properties	Not available
Cat5000	Actions	Not available	Not available
Cat6000_NO_PFC	Scheduling	Properties	Not available
Cat6000_PFC1	Scheduling DSCP Mappings Actions	Properties Actions	Actions **Note:** VLAN scheduling is inherited from its ports.
Cat6000_PFC2	Scheduling DSCP Mappings Actions	Properties Actions	Actions **Note:** VLAN scheduling is inherited from its ports.

Table 6-3 Types of QoS Configurations on Layer 2 Switches Running IOS

Devices / NEs	Device	Interface
Cat2900	Not available	Actions
Cat2950	Scheduling	Actions
Cat3500	Not available	Properties Actions

Table 6-4 Types of QoS Configurations on Layer 3 Devices

Devices / NEs	Device	Interface	POI
Cat2948_L3	Scheduling	Scheduling Actions	Not available
Cat4232_L3	Scheduling	Scheduling Actions	Not available
Cat4908_L3	Scheduling	Scheduling Actions	Not available
Cat8500	Not available	Not available	Scheduling

Configuring FRTS Policies

This section describes how to configure Frame Relay Traffic Shaping (FRTS) on a frame relay main interface, and how to configure FRTS for frame relay subinterfaces and DLCIs.

Configuring FRTS for Frame Relay Main Interfaces

To configure FRTS for frame relay main interfaces:

1. Use the Policy Definition wizard to create a new policy group with the following constraint definition:
   - Select the device's Model and OS version.
   - Network Element—Select **Interface**.

- Interface Type—Select **Frame Relay**.
- Interface Card—Select **NA**.

2. In the QoS Properties wizard, define the following:
   - In the Congestion Management page, select a scheduling method.
   - In the Shaping Settings page, enable FRTS, and configure FRTS parameters.
   - Define any other desired property.
3. Use the Policy wizard to configure policies if required.
4. Assign frame relay main interfaces to the policy group.

Configuring FRTS for Frame Relay Subinterfaces or DLCIs

To configure FRTS for frame relay subinterfaces or DLCIs, you must create two policy groups:

- A policy group to enable FRTS on the frame relay main interface to which the subinterfaces or DLCIs belong.
- A policy group to configure FRTS for the subinterfaces or DLCIs.

To configure FRTS for frame relay subinterfaces or DLCIs:

1. Create a policy group for the frame relay main interface:
   a. Use the Policy Definition wizard to create a new policy group as described in Step 1 in Configuring FRTS for Frame Relay Main Interfaces.
   b. In the QoS Properties wizard, select the Enable FRTS in the Shaping Settings page. Do not set FRTS parameters.
   c. Assign the main interface of the frame relay subinterfaces or DLCIs to this policy group.
2. Create a policy group for the frame relay subinterfaces or DLCIs:
   a. Use the Policy Definition wizard to create a new policy group as described in Step 1 in Configuring FRTS for Frame Relay Main Interfaces. For DLCIs, select FR DLCI as the network element in the Constraints Definition page.

b. Define FRTS properties and other policies as described in steps 2 and 3 in Configuring FRTS for Frame Relay Main Interfaces.

c. Assign frame relay subinterfaces or DLCIs to the policy group.

Note

- Frame relay main interfaces and subinterfaces can have different QoS capabilities, therefore do not assign main interfaces and subinterfaces to the same policy group. Create one policy group for the main interfaces and another policy group for the subinterfaces, as described above.
- If FRTS is configured for frame relay subinterfaces or DLCIs, but their parent interfaces are not defined with FRTS, the subinterface configuration will not be deployed. You can generate a FRTS Conflicts report to display these frame relay subinterfaces or DLCIs. See FRTS Conflicts - Subinterfaces Page, page D-30 and FRTS Conflicts - DLCIs Page, page D-31 for more information about FRTS Conflicts reports.

Related Topics

- Creating a Policy Group, page 6-5
- Defining QoS Properties and Mappings, page 6-8
- Setting Network Element Assignments, page 6-13

Configuring VLAN Policies

To configure policies on a VLAN, you must create two policy groups:

- A policy group for the VLAN:
  - Define the type of network element in the Device Constraints Definition page of the Policy Group Definition wizard as VLAN.
  - Assign the VLAN to the policy group.
  - Define policies for the VLAN.

- A policy group for the VLAN interfaces on which you want to configure the VLAN policies:
  - In the QoS Properties wizard, define the QoS style in the Traffic Control Settings page as VLAN-based.
  - Assign the required VLAN interfaces to the policy group.
  - Do not define any policies in this policy group.

Note When configuring VLAN-based policies for devices with Native IOS, the **switch port** CLI command must be configured on the device.

Related Topics

- Creating a Policy Group, page 6-5
- Defining QoS Properties and Mappings, page 6-8
- Setting Network Element Assignments, page 6-13

Deploying QoS Policies

After you have defined your QoS policies and assigned them to network elements, you can deploy the policies to the network devices.

The following topics describe policy deployment and the tasks associated with the deployment of QoS policies:

Understanding Policy Deployment

QPM deploys the QoS policies in a deployment group to your network devices. You can deploy an entire deployment group, or you can specify a subset of devices within a selected deployment group to which QPM will deploy the appropriate QoS policies. Each deployment event is called a "job."

Note You can only deploy QoS policies to devices in the network if the devices are real. If you are using virtual devices, you will not be able to deploy your policies to the network.

When you deploy your QoS policies to network devices, QPM translates the policies into device commands and enters the commands through the device's command line interface (CLI). You can choose to deploy your QoS configurations directly to network devices using Telnet. QPM automatically deploys your QoS configurations to configuration files. This deployment process does not configure the devices but generates configuration files that can be sent manually to the devices. QoS configurations can be deployed to the device using any application that downloads configuration files to the devices. QPM allows you to monitor the deployment process in real-time, viewing the active deployment jobs and their status.

Through QPM, you can verify the device configuration to ensure that your deployment group policy definitions match the actual device configurations, and preview the commands that will be used to configure the devices.

Upon deployment of a job, a read-only copy of the current deployment group is automatically made. This allows you to continue editing the deployment group, and also provides a historical version of it.

QPM allows you to restore, as the current editable deployment group, a previous version of a deployment group that was already deployed to the network. You can restore a deployment group for editing without deploying it, or you can restore and redeploy the deployment group. This feature is very useful when unexpected errors occur as a result of a deployment and you must go back to a previous version of the deployment group.

QPM maintains a history of deployments and their status results. This history allows you to view the deployment groups deployed and the deployment status results. QPM also provides static job reports that display the statuses of the devices in the deployment.

Note You can also trigger the deployment process from an application that is external to QPM, by issuing an HTTPS request.

Related Topics

- Deploying Policies and QoS Configurations, page 7-3
- Viewing the Deployment Status, page 7-10
- Managing Historical Versions, page 7-14
- Previewing the CLI Commands, page 7-24
- Verifying Device Configuration, page 7-30
- Deploying Jobs from an External Trigger, page 7-36

Deploying Policies and QoS Configurations

QPM provides options for deploying policies and QoS configurations to network devices. Using the Deployment wizard, you can deploy a current or historical version of a deployment group. If a deployment job fails, you can redeploy it to some or all of its failed devices.

The Deployment wizard guides you through the steps required for deploying a deployment group. You select your deployment group, enter the job details and select the deployment options. The wizard gathers and validates all the information that you enter, and allows you to view a summary of the job information. You can confirm or edit this information before deploying.

The following sections describe the step-by-step procedures for creating a deployment job, using the Deployment wizard.

The following topics describe the steps of the wizard:

- Step 1: Selecting a Deployment Group for Deployment, page 7-4
- Step 2: Validating the Historical Deployment Group, page 7-6
- Step 3: Selecting and Previewing the Devices for Deployment, page 7-7
- Step 4: Entering the Job Details for Deployment, page 7-9
- Step 5: Confirming the Wizard Information for Deployment, page 7-10

Related Topics

- Using QPM Wizards, page 3-10

Step 1: Selecting a Deployment Group for Deployment

The first step in the deployment process is to select the deployment group to be deployed. While the default is to select one of the currently managed deployment groups, you can select a historical version of a deployment group that was deployed.

Note If deployment was activated from the IP Telephony wizard, the first page of the wizard—Deployment Group Selection, does not display. In this case, the Device Selection and Preview page automatically appears.

If you select a historical version of a deployment group, it is restored as the current deployment group for editing. The existing current deployment group is saved as a historical version.

Procedure

Step 1 Select **Deploy > Deployment**. The first step of the Deployment wizard is displayed—Deployment Group Selection.

Step 2 Choose the type of deployment group (current or historical), by selecting the Current version of a deployment group or Restore a previous version of a deployment group radio button.

Step 3 Select the deployment group:

- If you are deploying a current deployment group, select the deployment group name from the list.

  To view the details (Owner, Creation Time) of all the deployment groups before making your selection:

  – Click the View list link. The Deployment Groups List page appears, displaying all the currently managed deployment groups. For more information about this page, see Deployment Groups List Page, page C-3.

  – Select the required deployment group and click **Select**.

The selected deployment group name will be displayed in the Deployment Group list in the first page of the wizard.

- If you are deploying a historical deployment group, select the deployment group name from the list.

  To view the details (Version, Job, Owner, Creation Time) of all the historical deployment groups before making your selection:

  - Click the View list link. The Job History List page appears, displaying all the historical deployment groups. For more information about this page, see Job History List Page, page C-4.
  - Select the required deployment group and click **Restore**.

  The selected deployment group name will be displayed in the Deployment Group list in the first page of the wizard.

Step 4 Click **Next** to move to the next step of the wizard:

- If you selected to deploy a current deployment group, the next step of the wizard is to select your devices.
- If you selected to deploy a historical version of a deployment group, the next step of the wizard is to validate the deployment group.

Related Topics

- Step 2: Validating the Historical Deployment Group, page 7-6
- Step 3: Selecting and Previewing the Devices for Deployment, page 7-7
- Managing Historical Versions, page 7-14

Step 2: Validating the Historical Deployment Group

Note This step of the wizard is only available if you selected to deploy a historical version of a deployment group.

Whenever a previous version of a deployment group is restored, validation checks must be done on the deployment group. The validation process is automatically activated after selecting a historical deployment group and clicking the Next button in Step 1: Selecting a Deployment Group for Deployment.

The system does the following checks and automatically provides a report of violations, where relevant:

- Missing Network Elements—This validation procedure checks for the coordination of policies and managed devices. If the validation procedure detects network elements that are missing from the current device group, they will be displayed in the report. The assignments of policies to these network elements in the restored deployment group will be automatically removed.
- Invalid Assignments—This validation procedure checks for assigned network elements that no longer match the constraints of their policy groups. Any invalid assignments will be displayed in the report. The network elements will be removed from the assignment.
- Reusable Components Violations—This validation procedure checks for the coordination of policies and library components (IP aliases, application aliases and policy group templates). If the validation process detects some library components in the restored version that are different than the ones in the current libraries, this will be displayed. The validation process overrides the current library components with the original ones and adds them locally to the deployment group. In this case, the dynamic link to the library components will no longer exist.
- Constraints Violations—This check validates the policy group device constraints against the predefined constraints limitations. These limitations might change from time to time causing some of the policy group constraints to be invalid. Policy groups that are invalid will be displayed and removed along with their assignments.

Procedure

Step 1 In the Deployment Group Validate Historical page, click the View Restore Validation Report button.

The Restore Validation Report window opens, displaying any validation violations that were discovered during the deployment group restore procedure.

For more information about this window, see Restore Validation Report Window, page C-5.

Step 2 After you have finished viewing the report, close the window.

Step 3 Click **Next** or **Finish** to accept any changes made as a result of the validation checks, and move to the next step of the wizard.

Step 4 To stop the deployment without saving any changes, click **Cancel**.

Related Topics

- Step 3: Selecting and Previewing the Devices for Deployment, page 7-7
- Managing Historical Versions, page 7-14

Step 3: Selecting and Previewing the Devices for Deployment

Note If you are deploying a deployment group from the IP Telephony wizard, the Deployment wizard will open automatically on this page.

In this step of the wizard, you select the devices to which you want to deploy your policies. You can also preview the CLI commands that will be configured on your devices prior to deployment. This page displays a list of all the devices that are available for deployment and their configurations. Devices whose configurations have changed since the last deployment will be displayed with the check boxes alongside them selected. You can accept the default selection, or you can make your own selection of devices.

Procedure

Step 1 In the Device Selection and Preview page, select the check boxes alongside the devices to which you want to deploy your policies. Deselect those you do not want to deploy to.

Step 2 To preview the CLI configuration commands for a device:

a. Click its Policy Configuration link in the table.

A preview window opens, displaying the following configuration details for the device:

- Backup ShowRun configuration commands.
- Incremental Telnet script commands to be written (if deploying directly to network devices).

b. Click the appropriate buttons to view the relevant configuration details.

c. After you have finished previewing the device's configuration, click **Close** to close the Preview window.

Step 3 Click **Next** to move to the next step of the wizard.

Related Topics

- Previewing the CLI Commands, page 7-24
- Deployment Wizard - Device Selection and Preview Page, page C-7
- Device Configuration Preview Window, page C-8
- Step 4: Entering the Job Details for Deployment, page 7-9

Step 4: Entering the Job Details for Deployment

In this step of the wizard, you enter a name (a default name is provided) and, optionally, a description for the job you want to deploy.

In this page, you must also select if you want to deploy the configuration to the devices using Telnet. This option triggers actual deployment of the deployment group to the devices.

QPM also deploys the QoS configurations to files. This process does not configure the devices, but generates configuration files that can be sent manually to the device. Individual files are created per device and the complete set of files can be saved to your hard disk. When required, you can download these files as a single zip file to your desktop, by clicking the Files icon in the Job History report.

Procedure

Step 1 In the Job Details page, enter a name for your job (or accept the default).

Step 2 If required, you can enter a description of the job in the Job Description field.

Step 3 Select/deselect the check box depending on whether you want to deploy configuration to the devices using Telnet. (The default is selected.)

Step 4 Click **Next** to move to the final step of the wizard.

Related Topics

- Restoring and Deploying a Historical Deployment Group, page 7-16
- Step 5: Confirming the Wizard Information for Deployment, page 7-10
- Downloading a Historical Job's Configuration Files, page 7-19

Step 5: Confirming the Wizard Information for Deployment

The last page of the Deployment wizard presents a summary of all the data collected through the Deployment wizard for you to verify. After you are satisfied with the job information, you can deploy the deployment group to the network.

Caution Jobs are not necessarily deployed to devices in the order in which they are triggered. Avoid deploying several jobs to the same device simultaneously. This could result in the incorrect configuration of the device.

Procedure

Step 1 Verify the job information displayed on the page. If you are not satisfied with any of the job details, you can go back through the wizard to make the required changes.

Step 2 After you are satisfied with the job information, click **Deploy** to deploy the deployment group to the network.

The Active Jobs page appears, allowing you to view the deployment process.

Related Topics

- Step 4: Entering the Job Details for Deployment, page 7-9
- Viewing the Deployment Status, page 7-10

Viewing the Deployment Status

You can view the status of your job during deployment using the Active Jobs page. The Active Jobs page provides a dynamic view of all the active deployments and their status. For each deployment job, the start time of its configuration, its status, and a summary of the number of devices deployed according to their status, are displayed. The status of a job deployment or a device deployment might be Pending, In Progress, Completed, or Failed. A job deployment may also have the status of Aborted or Paused.

During the deployment process, a status of "In Progress" will be displayed for a job. When the job is completed successfully, its status will change to "Completed". For a deployment job to be Completed, all the devices must be successfully configured. If the deployment of at least one device fails, and all the other devices passed without errors, the overall status of the deployment is Failed. Completed jobs are automatically removed from the display after ten minutes.

From the Active Jobs page, you can:

- View the deployment details of a job.
- Pause and resume the deployment process.
- Stop the deployment.
- Redeploy a failed deployment.
- Remove a deployment job from the display.

Procedure

Step 1 Select **Deploy > Jobs > Active Jobs**.

The Active Jobs page appears, displaying the currently active deployment jobs and their status, in a table.

Tip The display is automatically refreshed every ten seconds. To force a refresh manually, click **Refresh**.

For more information about the Active Jobs page, see Active Jobs Page, page C-12.

Note The Active Jobs page appears automatically when you click **Deploy** in the Summary page of the Deployment wizard (see Step 5: Confirming the Wizard Information for Deployment, page 7-10).

Step 2 View the status of the active job deployments and device deployments:

- To view the details of a deployment job, select its Job Name link in the table. The Job Details report appears.
- To remove a deployment job from the table, select it and click **Remove From Display**.

Related Topics

- Pausing and Resuming a Deployment Job, page 7-12
- Stopping a Deployment Job, page 7-13
- Redeploying a Job, page 7-14
- Viewing the Job Details Report, page 7-20
- Troubleshooting Deployment Problems, page 11-7

Pausing and Resuming a Deployment Job

You can pause a job during deployment. However, QPM will not stop the configuration of a device after it has begun. Any devices that are being configured when the Pause command is issued will be finished. Devices for which deployment had not yet begun will remain with the status Pending. You can also cause any paused deployment to resume configuration of devices. This does not create a new job—it continues the selected job.

Procedure

Step 1 Select **Deploy > Jobs > Active Jobs**. The Active Jobs page appears.

Step 2 In the Active Jobs list, select the check box next to your deployment job and click **Pause**.

A message appears asking you if you are sure you want to pause the deployment of your job.

Step 3 Click **Yes** to pause the job's deployment.

Step 4 To resume the deployment of your job, select the check box next to the job and click **Resume**.

The deployment of the selected job will resume.

Related Topics

- Viewing the Deployment Status, page 7-10

Stopping a Deployment Job

You can stop a deployment job that is currently in progress or has been paused. This feature is useful if you want to change a job's configuration details before deploying it, or if a job becomes stuck while in progress. Terminating a job stops the configuration of the devices. All the devices that were In Progress or Pending will receive a Failed status. You cannot resume a stopped deployment job.

Procedure

Step 1 Select **Deploy > Jobs > Active Jobs**. The Active Jobs page appears.

Step 2 In the Active Jobs list, select the check box next to the deployment job (In Progress or Pending) that you want to stop, and click **Abort**.

A message appears warning you that the job will be aborted with no option to resume it.

Step 3 Click **Yes** to confirm the stop procedure.

The job status for the selected deployment job will display "Aborted".

Related Topics

- Viewing the Deployment Status, page 7-10

Redeploying a Job

You can manually request that deployment be retried for either a specific device that failed or all failed devices in any displayed failed job. This does not create a new job—it creates another deployment for the job. The redeployment process resets the status of the selected devices and re-requests the deployment of the selected job.

Procedure

Step 1 Select **Deploy > Jobs > Active Jobs**. The Active Jobs page appears.

Step 2 In the Active Jobs table, select the check box next to the job you want to redeploy and click **Redeploy**. The Device Selection and Preview page of the Deployment wizard appears, displaying all the failed devices of the job. See Step 3: Selecting and Previewing the Devices for Deployment, page 7-7.

Step 3 Select the check boxes alongside the devices to which you want to deploy your policies. If required, preview the CLI commands that will be configured on your devices. Then click **Next**.

Step 4 Enter the job details and select the deployment options, and click **Next** (see Step 4: Entering the Job Details for Deployment, page 7-9).

Step 5 Verify the job information and click **Deploy** to redeploy your job to the network (see Step 5: Confirming the Wizard Information for Deployment, page 7-10).

Related Topics

- Viewing the Deployment Status, page 7-10

Managing Historical Versions

QPM allows you to restore previous versions of deployment groups that were deployed to the network, for editing and deploying. The Restore feature is very useful when unexpected errors occur as a result of the deployment of a deployment group and you must go back to a previous version of that deployment group. You can also view a historical version of a deployment group without restoring.

You can manage historical versions of deployment groups from the Job History report, which displays a table of historical deployment jobs and all their details.

From the Job History report, you can do the following:

- Restore a historical deployment group to edit and deploy it.
- View a historical deployment group's policy groups.
- Delete a historical job.
- Lock a job to prevent automatic deletion when the history cache is full, or release a job from being locked.
- Download the configuration files of a historical deployment job.
- View a Job Details report for each deployment job.
- View a Deployment History report for each deployment job.
- View the results of a DNS host name resolution check for a deployment job.

Procedure

Step 1 Select **Deploy > Jobs > Job History**. The Job History report appears.

For more information about the Job History report, see Job History Page, page C-14.

Step 2 Select the required historical report, and click the appropriate button or link depending on the procedure you want to do, as described in the following sections.

Related Topics

- Restoring and Deploying a Historical Deployment Group, page 7-16
- Viewing a Historical Deployment Group, page 7-17
- Deleting a Historical Job, page 7-18
- Locking and Unlocking a Historical Job, page 7-19
- Downloading a Historical Job's Configuration Files, page 7-19
- Viewing the Job Details Report, page 7-20

- Viewing the Deployment History Report, page 7-22
- Viewing the DNS Resolution, page 7-23

Restoring and Deploying a Historical Deployment Group

This topic describes how you can restore a previous version of a specific deployment group that was deployed to the network, for editing purposes. It also describes how to deploy the restored version, if required.

Note If required, you can view a history of all the deployment group restore operations, from the Restore Reports page. See Restore Reports Page, page D-39 for more information.

Procedure

Step 1 Select **Deploy > Jobs > Job History**. The Job History report appears.

Step 2 Select the historical job you want to restore, in the table.

Step 3 Click **Restore**.

Validation checks are automatically done on the deployment group. If the restore process detects any validation violations, the results will be written to a report. The Restore Deployment Group page appears, from which you can view the validation report.

For more information about this page, see Restore Deployment Group Page, page C-16.

Step 4 To view a validation report:

a. Click **Show Restore Report**. The Restore Validation Report window opens.

For more information about this window, see Restore Validation Report Window, page C-5.

b. When you have finished viewing the report, close the window.

Step 5 Click **OK** to confirm the Restore process, or **Cancel** to stop the process.

If you clicked OK, the restored version will be selected as the current editable deployment group. The Policy Groups page appears, displaying the policy groups for the current deployment group (see Modifying a Policy Group, page 6-19).

Step 6 If you want to deploy the restored version, follow the steps of the Deployment wizard (see Step 1: Selecting a Deployment Group for Deployment, page 7-4 through Step 5: Confirming the Wizard Information for Deployment, page 7-10).

Related Topics

- Step 2: Validating the Historical Deployment Group, page 7-6
- Managing Historical Versions, page 7-14
- Working with Policy Groups, page 6-2
- Deploying Policies and QoS Configurations, page 7-3

Viewing a Historical Deployment Group

If you want to verify the details of a historical version of a deployment job, QPM allows you to view its policy groups. You will not be able to make changes to the deployment group or deploy it to the network.

Note You can view only one historical deployment group at a time. The deployment group will not be saved. If you select another deployment group, you will lose the previous version you selected to view. To view it, you will have to select it again from the Job History report page.

Procedure

Step 1 Select **Deploy > Jobs > Job History**. The Job History report appears.

Step 2 Select the historical job in the table and click **View Deployment Group**.

The Policy Groups page appears in read-only mode, displaying the selected deployment group and its policy groups.

Related Topics

- Managing Historical Versions, page 7-14
- Working with Policy Groups, page 6-2

Deleting a Historical Job

You can delete historical jobs from the Job History report list.

Procedure

Step 1 Select **Deploy > Jobs > Job History**. The Job History report appears.

Step 2 Select the historical jobs you want to remove from the report, and click **Delete**.

A dialog box opens, warning you that the selected jobs will be deleted.

Step 3 Click **OK** to confirm the deletion. The jobs will be deleted from the list of historical jobs. You will no longer be able to restore them.

Related Topics

- Managing Historical Versions, page 7-14

Locking and Unlocking a Historical Job

The Job History report can display up to a predefined maximum number of jobs. When the history cache is full, the oldest historical jobs are automatically deleted. You can prevent this automatic deletion by "locking" a job. Similarly, you can "unlock" a historical version, making it available for deletion.

Procedure

Step 1 Select **Deploy > Jobs > Job History**. The Job History report appears.

Step 2 Select the historical job you want to prevent from automatic deletion, and click **Lock Job**. The Lock Job status of the job in the report will display **Lock**.

Step 3 To release a historical job from being locked from automatic deletion, select it and click **Unlock Job**. The Lock Job status of the job in the report will display **Unlock**.

Related Topics

- Managing Historical Versions, page 7-14

Downloading a Historical Job's Configuration Files

When QPM deploys QoS configurations to files, it generates configuration files that can be sent manually to the devices. Individual files are created for each device, and the complete set of files are saved as a single zip file to your hard disk.

From the Job History report, you can download to your desktop the zip file that contains the individual configuration files for each device in a historical deployment job that you select for editing.

Procedure

Step 1 Select **Deploy > Jobs > Job History**. The Job History report appears.

Step 2 Select the historical job whose configuration zip file you want to download, and click its Files icon. The File Download dialog box opens.

Step 3 Save the zip file to the required location on your desktop and extract the configuration files.

Related Topics

- Managing Historical Versions, page 7-14
- Step 4: Entering the Job Details for Deployment, page 7-9

Viewing the Job Details Report

The Job Details report shows the final status of all the deployments of a selected job. It can also show the current deployment status of a job that is still in progress.

Note The redeployment process can result in more than one deployment for a job (see Redeploying a Job, page 7-14).

The job's deployment details are displayed at the top of the page, and a table of all the devices related to the deployment is displayed below. From this report, you can view details about any errors or warnings that resulted from the deployment of a device. You can also view the CLI commands that were used to configure a device.

Note If the error message for a failed job displays "Internal error - unknown device state", some of the devices might be stuck in progress. In such a case, QPM will not be able to determine what was configured on these devices. You should contact technical support on the Cisco TAC web site to resolve this problem.

Procedure

Step 1 Select **Deploy > Jobs > Job History**. The Job History report appears.

Step 2 Click the Job Name link of the job whose details you want to view or click the Details icon for the job.

Note You can also open the Job Details page, by clicking the Job Name link for a job in the Active Jobs page, or by clicking the Job Name link for a device in the Managed Devices report.

The Job Details page appears, displaying the job's details and a table listing status information for each device in the job. For more information about the Job Details page, see Job Details Report Page, page C-17.

Step 3 To view details about an error or warning that resulted from the deployment of a device, click the Errors/Warnings link for the required device in the table. The Device Errors and Warnings page appears.

Step 4 To view the CLI commands that were used to configure a device:

a. Select the check box next to the required device in the table.

b. Click **View CLI Commands**.

A preview window opens, displaying the following configuration details for the device:

- Backup ShowRun configuration commands.
- Any incremental Telnet script commands that were written (if deployed directly to network devices).

c. Click the appropriate buttons to view the relevant configuration details.

d. Click **Close** to close the Preview window.

Related Topics

- Managing Historical Versions, page 7-14
- Viewing Device Deployment Errors and Warnings, page 7-22
- Viewing the Status of Devices, page 7-24

Viewing Device Deployment Errors and Warnings

In the Device Errors and Warnings page, you can view details about any errors or warnings that resulted from the deployment of a device. The page displays the reason for the error or warning message, and the time it occurred.

Procedure

Step 1 In the Job Details page, click the Errors/Warnings link for the device whose deployment error details you want to view. The Device Errors and Warnings page appears.

For more information about this page, see Device Errors and Warnings Page, page C-19.

Step 2 When you have finished viewing the error or warning messages, close the page.

Related Topics

- Viewing the Job Details Report, page 7-20

Viewing the Deployment History Report

The Deployment History report displays the deployment history details of a selected deployment.

Note The redeployment process can result in more than one deployment for a deployment job (see Redeploying a Job, page 7-14). A deployment history report shows only the devices that were configured in the selected deployment. These might not be all the devices in the deployment job.

Procedure

Step 1 Select **Deploy > Jobs > Job History**. The Job History report appears.

Step 2 Click the Deployments link of the job whose deployment details you want to view. The Deployment History report is displayed for the selected deployment.

For more information about the Deployment History report, see Deployment History Report Page, page C-19.

Step 3 To view the job details of the selected deployment, click the Deployment Type link. A Job Details report appears for the selected deployment.

Related Topics

- Managing Historical Versions, page 7-14
- Viewing the Job Details Report, page 7-20

Viewing the DNS Resolution

QPM resolves newly added host names to their IP addresses, to update any changes in the network. From the Job History report, you can view the results of a DNS resolution check done by QPM on the host names that QPM resolved to IP addresses, for a selected deployment job.

Procedure

Step 1 Select **Deploy > Jobs > Job History**. The Job History report appears.

Step 2 Select the historical job in the table and click **DNS Resolution**.

The DNS Resolution page appears, displaying a list of IP addresses to which the host names were resolved, for the selected deployment job.

For more information about the DNS Resolution page, see DNS Resolution Page, page C-17.

Related Topics

- Managing Historical Versions, page 7-14
- Creating a CLI Preview Job, page 7-25

Viewing the Status of Devices

The Managed Devices report allows you to view all the devices in the device group that were configured (deployed to) by QPM, and their statuses. You can also see which deployment jobs are responsible for them. From this report, you can view details about a device's deployment job and its status.

Procedure

Step 1 Select **Deploy > Jobs > Managed Devices**. The Managed Devices page appears.

For more information about the Managed Devices report, see Managed Devices Page, page C-20.

Step 2 To view details about the device's deployment job, click the Job Name link for the device. A Job Details report is displayed.

Related Topics

- Viewing the Job Details Report, page 7-20

Previewing the CLI Commands

QPM allows you to view in advance the CLI commands that will be sent to the devices upon deployment. You can create a CLI Preview job to view the commands for the current deployment group. You cannot create a CLI Preview job for a historical version. CLI previews are determined by querying the devices for their existing configuration and then calculating the incremental changes.

QPM provides several ways in which you can view the CLI commands that are already configured, or will be configured, on devices in your deployment group:

- Using the CLI Preview wizard, you can activate a CLI Preview job in which CLI commands are generated for all or some of the devices in a deployment group.
- During the deployment process, you can preview the CLI commands that will be configured on a single device, prior to deployment (see Step 3: Selecting and Previewing the Devices for Deployment, page 7-7).
- In the Job Details report, you can view the CLI commands that were configured on a selected device.
- In the Policy Translation page, you can view the CLI configuration of policies for a device (see Viewing Policy Translations, page 6-23).

Related Topics

- Viewing the Job Details Report, page 7-20
- Creating a CLI Preview Job, page 7-25
- Viewing the CLI Preview Jobs, page 7-28

Creating a CLI Preview Job

The CLI Preview wizard guides you through the steps required to create a new CLI Preview job, for all the devices in a deployment group.

The steps of the CLI Preview wizard are:

- Step 1: Selecting the Deployment Group for a CLI Preview Job, page 7-26
- Step 2: Previewing and Selecting the Devices for a CLI Preview Job, page 7-27
- Step 3: Confirming the Wizard Information for a CLI Preview Job, page 7-28

Related Topics

- Using QPM Wizards, page 3-10
- Previewing the CLI Commands, page 7-24

Step 1: Selecting the Deployment Group for a CLI Preview Job

In this step of the wizard, you select the deployment group that contains the devices whose CLI commands you want to preview. The deployment group must be one of those that are currently managed.

Procedure

Step 1 Select **Deploy > Previews**. The CLI Preview page appears.

Step 2 Click **New Preview**.

The CLI Preview wizard appears at the first page—Deployment Group Selection.

Step 3 Select the current deployment group from the list box.

To view the details (Owner, Creation Time) of all the current deployment groups, and then make your selection:

a. Click the View list link. The Deployment Groups List page appears.

b. Select the required deployment group and click **Select**.

The deployment group will appear selected in the Deployment Group Selection page of the wizard.

Step 4 Click **Next** to move to the next step of the wizard.

Related Topics

- Creating a CLI Preview Job, page 7-25
- Step 2: Previewing and Selecting the Devices for a CLI Preview Job, page 7-27

Step 2: Previewing and Selecting the Devices for a CLI Preview Job

In this step of the wizard, you select the devices and preview their configurations. This page displays a list of all the devices that are assigned to policy groups in the selected deployment group.

Procedure

Step 1 In the Device Selection and Preview page, select the check boxes alongside the devices whose configuration details you want to preview. By default, all the devices will be selected.

Step 2 To preview the CLI configuration commands for a device:

a. Click its Policy Configuration link.

A preview window opens, displaying the following configuration details for the device:

- Backup ShowRun configuration commands.
- Any incremental Telnet script commands that will be written (if deploying directly to network devices).

b. Click the appropriate buttons to view the relevant configuration details.

c. After you have finished previewing the device's configuration, click **Close** to close the Preview window.

Step 3 Click **Next** to move to the final step of the CLI Preview wizard.

Related Topics

- Creating a CLI Preview Job, page 7-25
- Step 3: Confirming the Wizard Information for a CLI Preview Job, page 7-28

Step 3: Confirming the Wizard Information for a CLI Preview Job

The last step of the CLI Preview wizard asks you to verify the deployment group name and the number of devices that were selected for previewing.

Procedure

Step 1 Verify the job information displayed on the page. If you are not satisfied with any of the job details, you can go back through the CLI Preview wizard to make the required changes.

Step 2 Click **Preview**. The CLI Preview page appears, allowing you to view the current CLI jobs that are being executed.

Related Topics

- Creating a CLI Preview Job, page 7-25
- Viewing the CLI Preview Jobs, page 7-28

Viewing the CLI Preview Jobs

The CLI Preview page displays a table of all the CLI Preview job requests that were created and those that are currently being executed. This page provides a dynamic view of all the CLI Preview jobs and their status. It also displays the time the last preview was initiated for a job, the job's status, and its owner. The status of a CLI Preview job may be Pending, In Progress, Completed, or Failed.

During the CLI Preview process, CLI commands are generated for all the devices in the deployment group. A status of "In Progress" will be displayed for a job during this process. When the job is completed successfully, its status will change to "Completed".

From the CLI Preview page, you can:

- Create a new CLI Preview job.
- View the details of a CLI Preview job. The CLI Preview Details report describes the details of a CLI Preview job. From this report, you can also view the CLI commands that were used to configure a device.

- View the results of a DNS host name resolution check for a selected CLI Preview job.
- Delete a CLI Preview job from the list.

Procedure

Step 1 Select **Deploy > Previews**. The CLI Preview page appears.

Note The CLI Preview page appears automatically when you click **Preview** in the last step of the CLI Preview wizard (see Step 3: Confirming the Wizard Information for a CLI Preview Job, page 7-28).

For more information about the CLI Preview page, see CLI Preview Page, page C-21.

Step 2 To create a new CLI Preview job, click **New Preview**. The CLI Preview wizard appears.

Step 3 To view the details of a CLI Preview job:

a. Select the CLI Preview job whose details you want to view, and click its Details icon or the View Preview Details button. The CLI Preview Details page appears.

For more information about the CLI Preview Details page, see CLI Preview Details Page, page C-25.

b. To view the CLI commands that were used to configure a device:

- Select the check box next to the required device in the table.
- Click **View CLI Commands**.

  A preview window opens, displaying the Backup ShowRun configuration commands and any incremental Telnet commands that were written to the device.
- Click the appropriate buttons to view the relevant configuration details.
- Click **Close** to close the Preview window.

Step 4 To view the results of a DNS host name resolution check, select the preview job and click **DNS Resolution**. The DNS Resolution page appears, displaying a list of IP addresses to which the host names were resolved, for the selected preview job.

For more information about the DNS Resolution page, see DNS Resolution Page, page C-17.

Step 5 To delete a CLI Preview jobs:

a. Select the jobs you want to remove from the list, and click **Delete**.

A dialog box opens, warning you that the selected jobs will be deleted.

b. Click **OK** to confirm the deletion. The jobs will be deleted from the list of CLI Preview jobs.

Related Topics

- Previewing the CLI Commands, page 7-24
- Creating a CLI Preview Job, page 7-25
- Viewing the DNS Resolution, page 7-23

Verifying Device Configuration

QPM allows you to verify whether any configuration changes were made on your devices since the last time you deployed. It compares the policies currently configured on the devices with the policies defined in your deployment group. You can create a Device Configuration Verification job to view the configuration for the current deployment group. You cannot create a device configuration verification job for a historical version.

If CLI changes were made on a device after deployment, there might be a mismatch between the deployment group and the device configuration. For each device, the assigned QoS configuration in the current deployment group is compared with the actual configuration on the device. A status of Match or Mismatch is displayed for each device.

The following topics describe:

- Creating a Device Configuration Verification Job, page 7-31
- Viewing the Device Configuration Verification Jobs, page 7-33

Creating a Device Configuration Verification Job

The Device Configuration Verification wizard guides you through the steps required to create a new device configuration verification job, for some or all of the devices in a deployment group.

The steps of the wizard are:

- Step 1: Selecting the Deployment Group for a Verification Job, page 7-31
- Step 2: Previewing and Selecting the Devices for a Verification Job, page 7-32
- Step 3: Confirming the Wizard Information for a Verification Job, page 7-33

Related Topics

- Using QPM Wizards, page 3-10
- Creating a Device Configuration Verification Job, page 7-31

Step 1: Selecting the Deployment Group for a Verification Job

In this step of the Device Configuration Verification wizard, you select the deployment group that contains the devices whose configurations you want to verify. The deployment group must be one of those that are currently managed.

Procedure

Step 1 Select **Reports > Conflicts > Verify Device Configuration**. The Verify Device Configuration page appears.

Step 2 Click **New Verification**.

The Device Configuration Verification wizard appears at the first page—Deployment Group Selection.

Step 3 Select the current deployment group from the list.

To view the details (Owner, Creation Time) of all the current deployment groups, and then make your selection:

a. Click the **View list** link. The Deployment Groups List page appears.

b. Select the required deployment group and click **Select**.

The deployment group will appear selected in the Deployment Group Selection page of the wizard.

Step 4 Click **Next** to move to the next step of the wizard.

Related Topics

- Creating a Device Configuration Verification Job, page 7-31
- Step 2: Previewing and Selecting the Devices for a Verification Job, page 7-32

Step 2: Previewing and Selecting the Devices for a Verification Job

In this step of the Device Configuration Verification wizard, you select the devices and preview their configurations. This page displays a list of all the devices that are part of the selected deployment group.

Procedure

Step 1 In the Device Selection and Preview page, select the check boxes alongside the devices whose configuration details you want to verify. By default, all the devices will be selected.

Step 2 To preview the CLI configuration commands for a device:

a. Click its Policy Configuration link.

A preview window opens, displaying the following configuration details for the device:

- Backup ShowRun configuration commands.
- Incremental Telnet script commands that will be written (if deploying to network devices).

b. Click the appropriate buttons to view the relevant configuration details.

c. After you have finished previewing the device's configuration, click **Close** to close the Preview window.

Step 3 Click **Next** to move to the final step of the Device Configuration Verification wizard.

Related Topics

- Creating a Device Configuration Verification Job, page 7-31
- Step 3: Confirming the Wizard Information for a Verification Job, page 7-33

Step 3: Confirming the Wizard Information for a Verification Job

The last step of the Device Configuration Verification wizard asks you to verify the deployment group name and the number of devices selected for verification.

Procedure

Step 1 Verify the job information displayed on the page. If you are not satisfied with any of the job details, you can go back through the wizard to make the required changes.

Step 2 Click **Verify**. The Verify Device Configuration page appears, displaying the current verification jobs that are being executed.

Related Topics

- Creating a Device Configuration Verification Job, page 7-31
- Viewing the Device Configuration Verification Jobs, page 7-33

Viewing the Device Configuration Verification Jobs

The Verify Device Configuration page displays a table of all the verification requests that were created and those that are currently being executed. This page provides a dynamic view of all the device verification jobs and their status. It also

displays the time the last device verification was initiated for a job, the job's status, and its owner. The status of a device verification job may be Pending, In Progress, Completed, or Failed.

During the device verification process, CLI commands are generated for all the devices in the deployment group. A status of "In Progress" will be displayed for a job during this process. When the job is completed successfully, its status will change to "Completed".

From this page, you can open a Job Verification Details report that describes the configuration details of a device configuration verification job. For each device in your deployment group, the device status is displayed and whether there was a Match or Mismatch in the device configuration. If the configuration assigned to the device in the current deployment group is the same as the configuration on the device, a status of "Match" is displayed. If CLI changes were made on a device after deployment, a status of "Mismatch" will be displayed for it, indicating a mismatch between the deployment group and the device configuration. If required, you can determine why a mismatch occurred by viewing the CLI commands that were used to configure the device.

From the Verify Device Configuration page, you can:

- Create a new device configuration verification job.
- View the configuration details of a device verification job.
- Delete a device configuration verification job from the list.

Procedure

Step 1 Select **Reports > Conflicts > Verify Device Configuration**. The Verify Device Configuration page appears.

Note The Verify Device Configuration page appears automatically when you click **Verify** in the last step of the Device Configuration Verification wizard (see Step 3: Confirming the Wizard Information for a Verification Job, page 7-33).

For more information about the Verify Device Configuration page, see Verify Device Configuration Page, page D-34.

Step 2 To create a new device configuration verification job, click **New Verification**. The Device Configuration Verification wizard appears.

Step 3 To view the details of a device configuration verification job:

a. Select the check box next to the verification job and click **View Verification Details** or click the job's Details icon. The Job Verification Details page appears for the device configuration verification job.

   For more information about the Job Verification Details page, see Job Verification Details Page, page D-35.

b. To view the CLI commands that were used to configure a device:

   – Select the check box next to the required device in the table.

   – Click **View CLI Commands**.

     A preview window opens, displaying the Backup ShowRun configuration commands and any incremental Telnet script commands that were written to the device.

   – Click the appropriate buttons to view the relevant configuration details.

   – Click **Close** to close the Preview window.

Step 4 To delete a device configuration verification job:

a. Select the jobs you want to remove from the list, and click **Delete**.

   A dialog box opens, warning you that the selected jobs will be deleted.

b. Click **OK** to confirm the deletion. The jobs will be deleted from the list of device configuration verification jobs.

Related Topics

- Verifying Device Configuration, page 7-30
- Creating a Device Configuration Verification Job, page 7-31

Deploying Jobs from an External Trigger

QPM allows external applications to trigger the deployment of a deployment group, by issuing an HTTPS request. This feature allows you to implement event or time-based triggering of deployment, as required.

Note You can only trigger the deployment of the current version of a deployment group.

Certain parameters *must* be included in the HTTPS request. They are:

- Username.
- User password.
- Device group name.
- Deployment group name.

Job Name and Job Description are optional parameters that may be included in the HTTPS request.

The format of the HTTPS request is as follows (there are no spaces in the URL):

https://<*host_name*>/MDC/servlet/com.cisco.core.mice.direct?
command=directOneTimeConnection
&username=<*user_ID*>&password=<*user_password*>
&url=/qpm/servlet/ExternalDeploymentServlet
&deployment_group=<*deployment_group_name*>
&device_group=<*device_group_name*>
&job_name=<*job_name*>&job_description=<*job_description*>

The following provides an example of an external HTTPS request:

https://localhost/MDC/servlet/com.cisco.core.mice.direct?
command=directOneTimeConnection &username=john&password=abc
&url=/qpm/servlet/ExternalDeploymentServlet
&deployment_group=Default%20Deployment%20Group
&device_group=Default%20Device%20Group
&job_name=external%20deployment
&job_description=auto%20deployment%20on%20weekend

If the input parameters are correct, the deployment process will be activated. The request will respond with either a success or failure message, including descriptions of any errors or warnings.

Related Topics

- Understanding Policy Deployment, page 7-2

Working with Deployment Groups

The QPM deployment groups contain the policies and policy groups, and other associated definitions you create. QPM uses the information in these deployment groups to apply your policies to the assigned network devices.

The following topics cover tasks associated with the management of QPM deployment groups.

Understanding Deployment Groups

A QPM deployment group contains policy group definitions, with all their associated policies and library components, such as IP aliases and application aliases.

QPM provides an empty default deployment group. You can rename this deployment group and begin working with it. You can create and manage multiple deployment groups.

Note You can view multiple deployment groups simultaneously in separate browser windows. However, we recommend that you edit only one deployment group at a time.

Whenever you save changes to a policy group or policy component, the changes are automatically saved in the deployment group. When you use library components in your policies, the dynamic link is automatically saved in the deployment group. Thus, there is no specific deployment group action required to save policy changes to the QPM deployment group.

When you create a deployment job from a deployment group, QPM creates a versioned backup copy of the deployment group. This historical version can be viewed, restored for editing, and redeployed. For more information about managing historical deployment groups, see Chapter 7, "Deploying QoS Policies."

Deployment groups are stored on the QPM server. QPM maintains audit trail records for each deployment group, including the time the deployment group was last modified.

Related Topics

- Opening a Deployment Group, page 8-3
- Creating a New Deployment Group, page 8-4
- Renaming a Deployment Group, page 8-6
- Using the QPM Audit, page 10-9

Opening a Deployment Group

In QPM, the default deployment group for policy configuration tasks, deployment tasks, and audit trail logs, is the last deployment group with which you worked. You can open a different deployment group, as required, when working with the following:

- Policy groups
- IP Telephony wizard
- Deployment wizard
- Audit Trail logs

You can also open a deployment group from the Deployment Groups page.

Procedure

Step 1 Select **Configure > Deployment Groups**. The Deployment Groups page appears displaying a list of existing deployment groups.

Step 2 Open a deployment group in one of the following ways:

- Click the deployment group name, or select the deployment group check box and click **Edit**, to open the Deployment Group page. In this page you can view and edit the deployment group's name and description.
- Click the deployment group's Policy Groups icon to open the deployment group's Policy Groups page.

Related Topics

- Creating a New Deployment Group, page 8-4
- Copying a Deployment Group, page 8-5
- Renaming a Deployment Group, page 8-6
- Working with Policy Groups, page 6-2

Creating a New Deployment Group

You can create a new QPM deployment group when you want to:

- Organize the policy groups for different sets of devices in separate deployment groups.
- Experiment with different policy definitions for the same devices.

Procedure

Step 1 Select **Configure > Deployment Groups**. The Deployment Groups page appears.

Step 2 Click **Create**. The Deployment Group page appears.

Step 3 Enter the new Deployment Group name in the Name field.

Step 4 Enter a description in the Description field (optional).

Step 5 Click **OK**. The Deployment Groups page appears and displays the new deployment group name in the list.

Tip You can also create a new deployment group by copying an existing deployment group. See Copying a Deployment Group, page 8-5.

Related Topics

- Opening a Deployment Group, page 8-3
- Working with Policy Groups, page 6-2

Copying a Deployment Group

You can create a new deployment group by copying an existing deployment group. If the source and target deployment groups are in the same device groups, you can copy the network element assignments for the policy groups in the source deployment group.

Procedure

Step 1 Select **Configure > Deployment Groups**. The Deployment Groups page appears.

Step 2 Select the check box next to the deployment group you want to copy.

Step 3 Click **Copy**. The Copy Deployment Group dialog box opens.

Step 4 Enter the device group to which you want to copy the deployment group.

Step 5 Select the **Copy with network element assignments** check box if you want to copy the network element assignments for the policy groups. You can only do this if you are copying within the same device group.

Step 6 Click **OK**. The new deployment group appears in the Deployment Groups list with the name "Copy of <*source*>".

You can change the new deployment group name to a more meaningful name.

Related Topics

- Creating a New Deployment Group, page 8-4
- Renaming a Deployment Group, page 8-6

Renaming a Deployment Group

When you begin working with QPM, a new deployment group is automatically loaded. You should rename this deployment group with a meaningful name before you start to create policy groups.

When you copy a deployment group, a default name is given to the new deployment group. You should change it to a more meaningful name.

Procedure

Step 1 Select **Configure > Deployment Groups**. The Deployment Groups page appears.

Step 2 Click the deployment group name you want to change, or select the deployment group check box and click **Edit**. The Deployment Group page appears.

Step 3 Change the deployment group name in the Name field. You can change or add a description in the Description field.

Step 4 Click **OK**. The Deployment Groups page appears and displays the changed deployment group name in the list.

Related Topics

- Opening a Deployment Group, page 8-3
- Creating a New Deployment Group, page 8-4
- Copying a Deployment Group, page 8-5

Deleting a Deployment Group

You can delete a deployment group. The deployment group's policy groups and policies are deleted. Attached global library components are not deleted. The deployment group's historical jobs are not deleted.

Procedure

Step 1 Select **Configure > Deployment Groups**. The Deployment Groups page appears.

Step 2 Select the check boxes next to the deployment groups you want to delete.

Step 3 Click **Delete**. The deployment group and its contents are deleted.

Managing Multiple Deployment Groups

QPM supports multiple deployment groups per device group; however policy groups cannot be split across deployment groups. Each deployment group is a complete entity with all components. Effectively, there are an unlimited number of deployment groups that can be opened at the same time.

Multiple users can work with the same deployment group, at any time. Any changes made to the deployment group are saved directly to the deployment group.

You can track changes made to deployment groups in the Audit Trail logs.

Related Topics

- Opening a Deployment Group, page 8-3
- Creating a New Deployment Group, page 8-4
- Using the QPM Audit, page 10-9

Using QoS Analysis

QPM allows you to obtain a baseline traffic profile of your network and analyze the effect of QoS on the network.

The following topics describe how to use QPM performance analysis:

Understanding QoS Analysis

QPM allows you to perform the following analysis of your network's traffic:

- You can perform a baseline analysis to determine how traffic is flowing on the network. For more information, see Performing Baseline QoS Analysis, page 9-4.
- You can analyze the effect of QoS on the network. You can use this information to assess the effectiveness of the QoS and plan policy changes. For more information, see Understanding the Types of QoS Analysis, page 9-2.

QPM monitors class-based QoS and CAR QoS types. QPM does not support monitoring of network elements that are assigned to a policy group configured with Modular Shaping.

Only policies that are deployed to the network by QPM can be monitored. For information about monitoring QoS that you configured without using QPM, see Using QoS Analysis with Existing QoS Configuration, page 9-5.

Tip If you add interfaces to a device that has network elements that are being monitored, either by a running historical monitoring task or by a running real-time monitoring report, you must rediscover the device. If you do not rediscover the device, the monitoring application will not be able to poll monitoring data for the device interfaces, resulting in an application error. For information about rediscovering devices, see Rediscovering Device Information, page 4-18.

The following topics provide more overview information about using QPM QoS analysis:

- Understanding the Types of QoS Analysis, page 9-2
- Understanding What QPM Monitors, page 9-3

Understanding the Types of QoS Analysis

There are two types of QoS analysis in QPM:

- Historical analysis monitors traffic for all QPM policies on one or more interfaces, polling on a regular basis and storing the gathered data.

  Historical monitoring jobs gather data between a start time and end time that you define. All of the gathered data can be displayed in historical monitoring reports.

  You would typically use historical monitoring as an operations tool. It is useful for monitoring the performance of your network's QoS configuration on an ongoing basis, over a period of time.

- Real-time analysis monitors traffic for all QPM policies on one interface continuously, in real time. No historical data is stored.

  You would typically use real-time monitoring for immediately viewing the effects of QoS change, troubleshooting QoS problems, or investigating new QoS configurations in a lab environment.

Related Topics

- Performing Historical QoS Analysis, page 9-6
- Performing Real-Time QoS Analysis, page 9-17

Understanding What QPM Monitors

Both historical and real-time QoS monitoring reports display the same types of QoS monitoring data. Each QoS monitoring report contains graphs of the following types of QoS monitoring data:

- The amount of traffic that matched the policy's filters (before QoS), the amount of matching traffic that was dropped by QoS, and the amount of matching traffic that was transmitted (after QoS).

  This information provides a general view of the efficiency of queued traffic through an interface. For example, you can see how much traffic has been dropped, and whether, on average, the classes of traffic are using the bandwidth allocated to them efficiently.

  See the following topics for more detailed information:

  - Policies Graphs: Matching and Dropped Traffic for Policies Page, page D-12
  - QoS Policy Manager - Real Time Report Window, page D-22

- A breakdown of the traffic that matched each of the policy's filters.

  This information allows you to see how traffic within each class is distributed among its match statements.This enables you to analyze your traffic by application. For example, you can see if traffic from one application is using too much of the bandwidth allocated to its traffic class.

  See the following topics for more detailed information:

  - Filters Graphs: Matching Traffic for Filter Conditions Page, page D-15
  - QoS Policy Manager - Real Time Report Window, page D-22

- The amount of traffic to which QoS actions were applied because of the policy's QoS configuration, broken out by the following types of QoS features:
  - Queuing
  - WRED

- Policing
- Traffic shaping

See the following topics for more detailed information:

- Actions Graphs: Policy Actions on Matching Traffic Page, page D-17
- QoS Policy Manager - Real Time Report Window, page D-22

Performing Baseline QoS Analysis

To determine how to deploy QoS on a network, it is helpful to perform a baseline analysis of the network's traffic flow. A baseline QoS analysis shows you how the important traffic classes on your network are flowing. You can use this information to design QoS that better meets the needs of your network.

Baseline QoS analysis is part of the larger QoS workflow that you should use to ensure the effectiveness of the QoS on your network on an ongoing basis. For more information, see Planning for QoS Deployment, page 2-1.

In summary, you use QPM QoS analysis to perform a baseline QoS analysis by deploying QoS that identifies the important traffic classes on your network but does not perform any QoS actions that affect traffic flow. The purpose of this QoS is just to identify the traffic so that QPM QoS analysis can collect data about how the important traffic flows through the network. Then you can view QoS analysis reports that show you this data.

You can perform a baseline QoS analysis using either historical or real-time QoS analysis. For information about determining which type of QoS analysis to use, see Understanding the Types of QoS Analysis, page 9-2.

Selecting Traffic Classes

Baseline QoS analysis works best when you identify ten or fewer traffic classes to monitor. Each traffic class can contain one or more traffic types (for example, voice classes, SAP, Oracle, or web traffic), so you should group the important applications running on your network into sensible classes. Keep in mind that the reports show network activity at the class level, so you cannot view a breakdown of the traffic types within a class.

Applying QoS To Enable QoS Analysis

After you have identified your traffic classes, you can create QPM policies that mark the classes without taking any QoS actions that affect traffic flow. The following QoS settings are ideal for this:

- QoS feature: Policing.
- Set rate, burst rate, and exceed burst rate to 8.
- Set conformed, exceeded, and violated actions to transmit.
- Do not configure an excess rate.

For information about creating policies, see Working with Policy Groups and Policies.

Related Topics

- Planning for QoS Deployment, page 2-1
- Working with Policy Groups and Policies

Using QoS Analysis with Existing QoS Configuration

Only policies that are deployed to the network by QPM can be monitored. If you have configured QoS on devices without using QPM, you can use this procedure to monitor the QoS that you have already created.

Procedure

Step 1 Upload the devices' configurations into QPM. For more information, see Uploading Device QoS Configurations to Policy Groups, page 6-16.

QPM automatically creates policies based on device QoS configuration.

Step 2 Edit the automatically created policies as desired. For more information, see Working with Policy Groups and Policies.

Step 3 Deploy the uploaded policies back to the network to monitor them.

For more information, see Deploying Policies and QoS Configurations, page 7-3.

This step is necessary because QPM only monitors QoS that it has deployed.

You can now monitor the policies that you deployed to the network.

Performing Historical QoS Analysis

To monitor policies, you create a QoS monitoring task. Each historical monitoring task has a corresponding report that you can view. Historical QoS analysis reports display results after the task has polled data three times (which depends on the start time you configure). But they are most useful if you let them run for a significant period of time because the results are more representative after the data has been polled a number of times.

You define the traffic to be monitored by specifying the interfaces and policies to be monitored. Each historical QoS analysis task can monitor a maximum of 12 interfaces, and a maximum of 12 policies on each interface.

You specify when each task starts and ends, and the polling interval. The duration limits for historical monitoring tasks depend on the polling interval, as shown in Table 9-1.

Table 9-1 Historical Monitoring Task Duration Limits

Polling Interval	Maximum Task Duration (Days)
1	1
5	5
10	10
15	30
20	40
25	50
30	90
60	180

Note When viewing a historical analysis report, you can select the time period of data that is displayed.

The amount of time required to load a report into the Analysis Report page depends on the amount of data collected, and can take from half a minute to several minutes.

Historical QoS analysis data is stored with all the QPM data, on the QPM server. If you run out of available disk space for collecting historical QoS analysis data, all current tasks are automatically stopped. For information about freeing disk space and resuming monitoring tasks, see Freeing Disk Space for QoS Analysis, page 9-16.

Historical monitoring tasks add collected data to the analysis database one time per hour. Historical monitoring reports only display data that has been added to the database, so the data displayed in reports lags behind the current time by as much as one hour.

Tip If you make changes using QPM to a QoS feature that QPM is monitoring, running historical monitoring tasks that are monitoring the QoS feature stop when you deploy the changes. All data collected up to the time of the change is preserved. To continue monitoring the QoS feature that you changed, you must create new monitoring tasks.

Tip If you remove a device that contains network elements that are being monitored by a historical monitoring task, QPM continues to monitor these network elements. To stop QPM from monitoring these network elements, you must stop or delete the historical monitoring task. If the historical monitoring task was monitoring other network elements that you want to continue to monitor, you must create a new historical monitoring task to monitor those network elements, because you cannot edit a historical monitoring task.

The following topics describe historical QoS analysis:

- Customizing Historical QoS Analysis Reports, page 9-15
- Freeing Disk Space for QoS Analysis, page 9-16

Related Topics

- Understanding QoS Analysis, page 9-1

Defining a Historical QoS Analysis Task

Define a historical monitoring task to begin monitoring traffic for policies on one or more interfaces. The collected data is stored and used in historical monitoring reports.

Procedure

Step 1 Select **Reports**. The Historical Monitoring Tasks page appears.

Click **Create**. The Monitoring Task Wizard - Task Definition page appears. For more information about this page, see Monitoring Task Wizard - Task Definition Page, page D-8.

Step 2 Do the following in the Monitoring Task Wizard - Task Definition page:

a. Enter a task name in the Name field.

b. Select a polling interval from the Polling Interval(min) list box.

The polling interval is the period of time (in minutes) between each collection of the monitored data.

c. Enter a start date and an end date using the Start Time and End Time fields.

You can enter each date directly into the field (in the format mm/dd/yyyy), or click the calendar button and use the popup calendar that appears.

If the duration of the task is longer than the limit for the specified polling interval (see Table 9-1), an error message appears, displaying the duration limit in days.

d. Check the Enabled check box to enable the task. If you do not, the task will not run.

e. Optionally, you can enter a comment or description for the task in the Enter a comment or description field.

f. Click **Next**. The Monitoring Task Wizard - Select Devices page appears. For more information about this page, see Monitoring Task Wizard - Select Devices Page, page D-9.

Step 3 Do the following in the Monitoring Task Wizard - Select Devices page:

a. Select the check box next to the devices containing the interfaces you want to monitor.

Only devices that contain interfaces on which QoS is configured that QPM can monitor appear in the list.

b. Click **Next**. The Monitoring Task Wizard - Select Interfaces page appears. For more information about this page, see Monitoring Task Wizard - Select Interfaces Page, page D-10.

Step 4 Do the following in the Monitoring Task Wizard - Select Interfaces page:

a. Select the check box next to the interfaces containing the policies you want to monitor.

Only interfaces on which QoS is configured that QPM can monitor appear in the list.

b. Click **Next**. The Monitoring Task Wizard - Select Policies page appears. For more information about this page, see Monitoring Task Wizard - Select Policies Page, page D-11.

Step 5 Do the following in the Monitoring Task Wizard - Selection Policy Group and Policies page:

a. Select the QoS policies that you want to monitor on each interface.

b. Click **Next**.

The Monitoring Task Wizard - Summary page appears. For more information about this page, see Monitoring Task Wizard - Summary Page, page D-11.

Step 6 In the Monitoring Task Wizard - Summary page, review the summary page to make sure the task is configured as you want it.

Click the arrow icons next to device and interface names to view the Interfaces and policies that are selected for analysis.

Step 7 Click **Finish** to finish the task.

The Analysis page appears with the new task displaying in the task list.

Tip QoS analysis operates within the context of the active device group. For more information, see Setting the Active Device Group, page 4-35. This has the following effects:

- When creating a QoS analysis task, only devices that belong to the active device group are available to select.
- The QoS analysis task lists (historical and real-time) only display tasks that monitor network elements that belong to the active device group.

Related Topics

- Performing Historical QoS Analysis, page 9-6
- Viewing Historical QoS Analysis Reports, page 9-12
- Troubleshooting QoS Analysis Problems, page 11-10

Editing Historical QoS Analysis Tasks

You can edit tasks that not yet finished running and have the following status (shown in the Status column of the Analysis page):

- In Edit
- Collector Error
- Processing

After a task has started running normally or has finished running you cannot edit it.

Procedure

Step 1 Select **Reports**. The Historical Monitoring Tasks page appears.

Step 2 Select a report from the list, then click **Edit**. The Monitoring Task Wizard starts.

Step 3 Edit any of the task parameters using the Monitoring Task wizard, as described in Defining a Historical QoS Analysis Task, page 9-8.

Related Topics

- Performing Historical QoS Analysis, page 9-6
- Viewing Historical QoS Analysis Reports, page 9-12

Deleting Historical QoS Analysis Tasks

You can delete historical monitoring tasks that you no longer want to use. When you delete a task, all historical data collected by that task is deleted.

Procedure

Step 1 Select **Reports**. The Historical Monitoring Tasks page appears.

Step 2 Select a task from the list, then click **Delete**. A confirmation dialog box appears.

Step 3 In the confirmation dialog box, select **Yes**.

The Historical Monitoring Tasks page appears with the deleted task no longer displayed.

Related Topics

- Performing Historical QoS Analysis, page 9-6

Stopping Historical QoS Analysis Tasks

You can stop a running task. You cannot restart or edit a stopped task, so the primary use of this feature is to stop tasks that have collected sufficient data, but are still running.

Procedure

Step 1 Select **Reports**. The Historical Monitoring Tasks page appears.

Step 2 Select a report from the list, then click **Stop**. A confirmation dialog box appears.

Step 3 In the confirmation dialog box, click **Yes**.

The dialog box closes and the Historical Monitoring Tasks page appears with the job status listed as stopped.

Related Topics

- Performing Historical QoS Analysis, page 9-6

Viewing Historical QoS Analysis Reports

Historical QoS monitoring reports are available after the QoS analysis task has polled data three times (which depends on the start time and polling interval you configure). But they are most useful if you let them run for a significant period of time because the results are more reliable after the data has been polled a number of times.

Procedure

Step 1 Select **Reports**. The Historical Monitoring Tasks page appears.

Step 2 Select a report from the list, then click **View Report**.

The Analysis Report page appears. For information about this report, see Policies Graphs: Matching and Dropped Traffic for Policies Page, page D-12.

Related Topics

- Performing Historical QoS Analysis, page 9-6
- Customizing Historical QoS Analysis Reports, page 9-15
- Troubleshooting QoS Analysis Problems, page 11-10

Exporting Historical QoS Analysis Data

You can export the data gathered by a historical monitoring task to a CSV file on your client system. You can use this CSV file to import the data to another application for analysis.

If you export the data from a task that has not run or did not run successfully, the resulting file will contain only variable names, without the variable definitions that result from running the task.

Export File Format

The export file is in comma separated value (CSV) format. It contains the data collected by a historical monitoring task, which is separated into the following sections:

- Class map data.

  This section contains traffic flow data about all of the traffic monitored by the task. This section contains the following columns:

  - TimeStamp—The time at which each sample was taken. The first column of the entire file contains timestamps, which are used to correlate the data in the sections of the file.
  - Total Dropped Bit Rate—The number of bits dropped due to QoS actions since the previous sample.
  - Total Dropped Packet Rate—The number of bits dropped due to QoS actions since the previous sample.
  - Total Post Bit Rate—The number of bits transmitted after QoS was applied, since the previous sample.
  - Total Post Packet Rate—The number of packets transmitted after QoS was applied, since the previous sample.

  - Total Traffic Bit Rate—The number of bits that matched the filters of the policies monitored by the task, since the last sample.
  - Total Traffic Packet Rate—The number of bits that matched the filters of the policies monitored by the task, since the last sample.

- Filters data.

  This section contains a set of data for each filter monitored by the task. Each set of data contains the following columns:

  - TimeStamp—The time at which each sample was taken. The first column of the entire file contains timestamps, which are used to correlate the data in the sections of the file.
  - Matching Traffic Bit Rate—The number of bits that matched the filter since the previous sample.
  - Matching Traffic Packet Rate—The number of packets that matched the filter since the previous sample.

- Actions data.

  This section contains a set of data for each QoS action monitored by the task. Each set of data contains the following columns:

  - TimeStamp—The time at which each sample was taken. The first column of the entire file contains timestamps, which are used to correlate the data in the sections of the file.
  - Discard Bit Rate—The number of bits dropped by the action since the previous sample.
  - Discard Packet Rate—The number of packets dropped by the action since the previous sample.

Procedure

Step 1 Select **Reports**. The Historical Monitoring Tasks page appears.

Step 2 Select a report from the list, then click **Export Data**. A dialog box appears stating that the operation might take a few minutes.

Step 3 Click **OK**. The browser file download process begins.

Step 4 Use the browser file download process to save the file to your client system.

Customizing Historical QoS Analysis Reports

Each historical QoS analysis report has the same customization controls that you can use to customize how the analysis data is presented in the report.

The types of customization you can perform include:

- Displaying the graphs in line or bar format.
- Selecting the graph units of measure.
- Selecting the scale of the graph vertical axis.
- Selecting to organize the graphs by policy or by interface.
- Selecting the time period of data to display.
- Selecting which policies or interfaces to display.

Procedure

Step 1 View a historical QoS analysis report as described in Viewing Historical QoS Analysis Reports, page 9-12.

Step 2 Use the customization controls available in each historical reports page. See the following for more information:

- Policies Graphs: Matching and Dropped Traffic for Policies Page, page D-12
- Filters Graphs: Matching Traffic for Filter Conditions Page, page D-15
- Actions Graphs: Policy Actions on Matching Traffic Page, page D-17

Related Topics

- Performing Historical QoS Analysis, page 9-6
- Viewing Historical QoS Analysis Reports, page 9-12

Freeing Disk Space for QoS Analysis

Historical QoS analysis data is stored with all other QPM data, on the QPM server. If you run out of available disk space for collecting historical QoS analysis data, the following happens:

- All running monitoring tasks are stopped automatically, and are set to the status `Stopped due to out of disk space`.
- The next time you open the Historical Monitoring Tasks page, a message notifies you that there is a disk space shortage, and provides instructions to free disk space by rebuilding the database.

Note This message only appears on the Historical Monitoring Tasks page. You will not receive notification that the disk space limit was reached until you open this page.

All data collected before the tasks were stopped is available for display in reports. To free the necessary disk space and continue monitoring, you must delete the stopped tasks, and run the Rebuild Database utility from the QPM server. Then you can recreate the deleted tasks to resume running them.

Note You might not have enough space in the QPM database for monitoring because the percentage reserved free disk space defined during installation is too high. If you have free disk space on the QPM server, you can change the percentage of reserved free disk space. See Disk Space Shortage Problems, page 11-10 for details.

Procedure

Step 1 Delete all tasks that have the status `Stopped due to out of disk space`. See Deleting Historical QoS Analysis Tasks, page 9-11.

Step 2 Make a full backup of the QPM database. Go to **Admin > Backup / Retrieve Backup** in the CiscoWorks2000 desktop.

Step 3 Close QPM and log out of the CiscoWorks2000 desktop.

Step 4 On the QPM server, run the Rebuild Database utility. This utility is accessed from **Start > Programs > Cisco Systems > QoS Policy Manager > Rebuild Database** on the QPM server's Windows desktop. For more information about the database rebuild utility, see *Release Notes for QoS Policy Manager*.

Step 5 Reboot the QPM server.

Step 6 Log into the CiscoWorks2000 desktop and open QPM.

Step 7 Optionally, recreate any QoS analysis tasks that you deleted but want to continue running.

Related Topics

- Defining a Historical QoS Analysis Task, page 9-8

Performing Real-Time QoS Analysis

To analyze the effect of QoS in real time, first create a real-time QoS monitoring task. Then you can immediately run the analysis task to display the data it collects in real time. Data collection occurs only while the task is running, and no historical data is saved.

Each real-time QoS analysis task monitors only one interface. You can run multiple real-time QoS analysis tasks simultaneously because each real-time report appears in a separate browser window.

There is no preconfigured limit to the number of real-time report windows you can open simultaneously. However, each new report window uses system resources on the client and server, degrading system performance.

Tip If you make changes using QPM to a QoS feature that QPM is monitoring, running real-time monitoring reports that are monitoring the QoS feature stop collecting data when you deploy the changes. Close and rerun the report to continue monitoring.

Tip If you remove a device that contains a network element that is being monitored by a running real-time QoS analysis task, QPM continues to monitor this network element. To stop QPM from monitoring this network element, you must stop running the real-time QoS analysis task.

The following topics describe real-time QoS analysis:

Defining a Real-Time QoS Analysis Task

Define a real-time monitoring task to begin monitoring QoS data on a single interface in real time. You define the traffic to be monitored by specifying the device interface. All policies configured on the interface are monitored.

Procedure

Step 1 Select **Reports**. The Historical Monitoring Tasks page appears.

Step 2 Select **Real Time** in the TOC. The Real-Time Monitoring Tasks page appears.

Click **Create**. The Real Time Monitoring Wizard - Device Selection page appears. For more information about this page, see Real-Time Monitoring Wizard - Device Selection Page, page D-21.

Step 3 Do the following in the Real Time Monitoring Wizard - Device Selection page:

a. Enter a task name in the Name field.

b. Select a polling interval from the Polling Interval(sec) list box.

The polling interval is the period of time (in seconds) between each collection of the monitored data.

c. Optionally, you can enter a comment or description for the task in the Enter a comment or description field.

d. Select the device that contains the interface to monitor using the device table at the bottom of the page.

Click **Next**. The Real Time Monitoring Wizard - Interface Selection page appears. For more information about this page, see Real-Time Monitoring Wizard - Interface Selection Page, page D-21.

Step 4 Do the following in the Real Time Monitoring Wizard - Interface Selection page:

a. Select the interface to monitor from the interfaces list.

Only interfaces that have QoS policies assigned to them appear in the list.

b. Click **Finish**.

Tip QoS analysis operates within the context of the active device group. For more information, see Setting the Active Device Group, page 4-35. This has the following effects:

- When creating a QoS analysis task, only devices that belong to the active device group are available to select.
- The QoS analysis task lists (historical and real-time) only display tasks that monitor network elements that belong to the active device group.

Related Topics

- Performing Real-Time QoS Analysis, page 9-17
- Running Real-Time QoS Analysis Reports, page 9-21
- Troubleshooting QoS Analysis Problems, page 11-10

Editing Real-Time QoS Analysis Tasks

You can edit real-time QoS analysis tasks. If you edit a task while running its report, the changes you make will not take effect until the next time you run the report.

Procedure

Step 1 Select **Reports**. The Historical Monitoring Tasks page appears.

Step 2 Select **Real Time** in the TOC. The Real-Time Monitoring Tasks page appears.

Step 3 Select a task from the list, then click **Edit**. The Real-Time Monitoring wizard starts.

Step 4 Edit any of the task parameters using the Monitoring Task wizard, as described in Defining a Real-Time QoS Analysis Task, page 9-18.

Related Topics

- Performing Real-Time QoS Analysis, page 9-17
- Running Real-Time QoS Analysis Reports, page 9-21

Deleting Real-Time QoS Analysis Tasks

You can delete real-time QoS tasks. If you delete a real-time QoS task while viewing its report, the report will continue to work correctly. When you close the report, you will not be able to run it again.

Procedure

Step 1 Select **Reports**. The Historical Monitoring Tasks page appears.

Step 2 Select **Real Time** in the TOC. The Real-Time Monitoring Tasks page appears.

Step 3 Select a task from the list, then click **Delete**. A confirmation dialog box appears.

Step 4 In the confirmation dialog box, select **Yes**.

The Real-Time Monitoring Tasks page appears with the deleted task no longer displayed.

Running Real-Time QoS Analysis Reports

Real-time QoS monitoring reports are available immediately after you finish defining the QoS analysis task.

Procedure

Step 1 Select **Reports**. The Historical Monitoring Tasks page appears.

Step 2 Select **Real Time** in the TOC. The Real-Time Monitoring Tasks page appears.

Step 3 Select a task from the list, then click **Run**.

The QoS Policy Manager - Real Time Report window appears. Use this window to view and customize the real-time monitoring report. For information about this window, see QoS Policy Manager - Real Time Report Window, page D-22.

You can open multiple real-time monitoring reports by repeating this procedure.

Step 4 Click **Close Window** to close the report window.

Related Topics

- Performing Real-Time QoS Analysis, page 9-17
- Customizing Real-Time QoS Analysis Reports, page 9-22
- Troubleshooting QoS Analysis Problems, page 11-10

Customizing Real-Time QoS Analysis Reports

Real-time QoS analysis reports have the following customization controls that you can use to customize how the analysis data is presented in the report.

- Displaying the graphs in line or bar format.
- Selecting the graph units of measure.
- Selecting the scale of the graph vertical axis.
- Selecting which policies to display.

Procedure

Step 1 View a real-time QoS analysis report as described in Running Real-Time QoS Analysis Reports, page 9-21. The Report window appears.

Step 2 Use the customization controls. See QoS Policy Manager - Real Time Report Window, page D-22 for more information.

Related Topics

- Performing Real-Time QoS Analysis, page 9-17

CHAPTER 10

Additional Administration Features

The following topics describe additional QPM administration features:

Backing Up and Retrieving Data

You can back up all the QPM data on the QPM server. In the event of data loss, you can retrieve the data that has been backed up.

The following topics describe backing up and retrieving data:

Note Backing up is not the same as saving a version of an individual deployment group. To save a version of an individual deployment group, see Chapter 7, "Deploying QoS Policies."

Understanding QPM Backups

You can create the following types of backups to save QPM information on the QPM server:

- Full backup—Backs up all the QPM information on the QPM server. The file name of each full backup contains the date and time of the backup. You can make a full backup at any time to a location of your choice on the QPM server or to another computer through a mapped network drive. You can retrieve a full backup, and you can delete full backups.
- Incremental backups—An incremental backup saves all the changes since the previous incremental backup. Incremental backups are stored in a system-defined location on the QPM server. You can make an incremental backup at any time, and you can also create schedules for incremental backups.

  When you retrieve data from incremental backups, all the previous incremental backup files are also used to recreate the QPM database. You can delete all the incremental backups on the QPM server, but you cannot delete individual incremental backups.

Related Topics

- Making and Scheduling Backups, page 10-3
- Viewing Backup History, page 10-4
- Retrieving Backup Information, page 10-5
- Deleting Backups, page 10-7
- Viewing and Deleting Backup Schedules, page 10-9

Making and Scheduling Backups

You can make a full or incremental backup at any time. You can also create schedules for incremental backups.

Procedure

Step 1 Select **Admin > Backup/Retrieve Backup**.

If the Backup/Retrieve Backup application is already open, select **Create Backups** in the Backup/Retrieve Backup navigation TOC.

The Create Backup page appears.

Step 2 To make an immediate backup, select the Backup Now check box.

- To make a full backup, select the Full radio button. In the Backup directory path field, enter the full path of directory in which you want to save the backup files.
- To make an incremental backup, select the Incremental radio button. The incremental backup files are saved to a default location on the QPM server.

Step 3 To create a schedule of incremental backups:

a. Select the Schedule Incremental Backup check box.

b. Enter the date and time of the first scheduled backup.

c. Choose the frequency of the backups—once, daily, or weekly.

See Create Backup Page, page E-2 for more information about the fields in this page.

Step 4 Click **Submit**.

If you selected to make an immediate backup, the backup process starts, and the corresponding Retrieve Backup page appears.

If you created a backup schedule, you can view the next scheduled backup in the Scheduled Backups page. See Viewing and Deleting Backup Schedules, page 10-9.

Note You can create multiple backup schedules. You must click **Submit** to save each schedule.

Related Topics

- Viewing Backup History, page 10-4
- Retrieving Backup Information, page 10-5
- Deleting Backups, page 10-7
- Troubleshooting Database Backup Problems, page 11-17

Viewing Backup History

You can view the status and other details of full and incremental backups.

Procedure

Step 1 Select **Admin > Backup/Retrieve Backup**. The Create Backup page appears.

Step 2 To view the full backup history, select **Retrieve Full Backup** in the TOC in the left pane. The Retrieve Backup page appears displaying a list of full backups. From this page you can also retrieve and delete full backups. See Retrieve Full Backup Page, page E-3 for information about this page.

Step 3 To view the incremental backup history, select **Retrieve Incremental Backup** in the TOC in the left pane. The Retrieve Incremental Backup page appears displaying a list of incremental backups. From this page you can also retrieve and delete all incremental backups. See Retrieve Incremental Backup Page, page E-4 for information about this page.

Related Topics

- Retrieving Backup Information, page 10-5
- Deleting Backups, page 10-7

Retrieving Backup Information

You can retrieve the data from a full backup, or from the incremental backups. The retrieved data overwrites current QPM data on the QPM server.

Warning **You should use the QPM Retrieve feature with care.**

The following topics describe retrieving full and incremental backups:

- Retrieving a Full Backup, page 10-5
- Retrieving Incremental Backups, page 10-6
- Viewing Retrieved Backup History, page 10-7

Retrieving a Full Backup

You can retrieve a full backup at any time. Each full backup file is identified by the backup date and time.

Procedure

Step 1 Select **Admin > Backup/Retrieve Backup**. The Create Backup page appears.

Step 2 In the TOC in the left pane, select **Retrieve Full Backup**. The Retrieve Full Backup page appears displaying a list of full backups.

Step 3 Select the backup you want to retrieve.

Step 4 Click **Retrieve Backup**. The Retrieved Backup History page appears displaying the status and other details of the retrieved backup.

Step 5 Log out of QPM and the CiscoWorks2000 desktop, and restart the QPM server.

Note After you retrieve a full backup, you must delete all previous incremental backups before you can make incremental backups for the retrieved database. See Deleting Incremental Backups, page 10-8 for more information.

Related Topics

- Retrieving Incremental Backups, page 10-6
- Viewing Retrieved Backup History, page 10-7

Retrieving Incremental Backups

When you retrieve data from incremental backups, all the incremental backup files up to and including the selected backup are used to recreate the QPM database.

Procedure

Step 1 Select **Admin > Backup/Retrieve Backup**. The Create Backup page appears.

Step 2 In the TOC in the left pane, select **Retrieve Incremental Backup**. The Retrieve Incremental Backup page appears displaying a list of incremental backups.

Step 3 Select the backup you want to retrieve.

Step 4 Click **Retrieve Backup**. The Retrieved Backup History page appears displaying the status and other details of the retrieved backup.

Step 5 Log out of QPM and the CiscoWorks2000 desktop, and restart the QPM server.

Note After you retrieve from an incremental backup that is not the latest, you must delete all previous incremental backups before you can create incremental backups for the retrieved database. See Deleting Incremental Backups, page 10-8 for more information.

Related Topics

- Retrieving a Full Backup, page 10-5
- Viewing Retrieved Backup History, page 10-7

Viewing Retrieved Backup History

You can view the status and other details of retrieved backups.

Procedure

Step 1 Select **Admin > Backup/Retrieve Backup**. The Create Backup page appears.

Step 2 In the TOC in the left pane, select **Retrieved Backup History**. The Retrieved Backup History page appears displaying a list of retrieved backups. See Retrieved Backup History Page, page E-5 for more information about this page.

Step 3 To delete a row from the table, select the row, and click **Delete**.

Related Topics

- Retrieving a Full Backup, page 10-5
- Retrieving Incremental Backups, page 10-6

Deleting Backups

The following topics describe deleting full and incremental backups:

- Deleting a Full Backup, page 10-7
- Deleting Incremental Backups, page 10-8

Deleting a Full Backup

You can delete a full backup at any time. Each full backup file is identified by the backup date and time.

Procedure

Step 1 Select **Admin > Backup/Retrieve Backup**. The Create Backup page appears.

Step 2 In the TOC in the left pane, select **Retrieve Full Backup**. The Retrieve Full Backup page appears displaying a list of full backups.

Step 3 Select the backup you want to delete.

Step 4 Click **Delete**. A warning appears. Click **OK** to continue.

Related Topics

- Deleting Incremental Backups, page 10-8

Deleting Incremental Backups

You can delete all the incremental backups on the QPM server, but you cannot delete individual incremental backups. This is because when you retrieve incremental backups, all the previous incremental backup files are used to recreate the QPM database.

Note You must delete all incremental backups after you retrieve a full backup, or an incremental backup that is not the latest backup, before you can make incremental backups for the retrieved database.

Procedure

Step 1 Select **Admin > Backup/Retrieve Backup**. The Create Backup page appears.

Step 2 In the TOC in the left pane, select **Retrieve Incremental Backup**. The Retrieve Incremental Backup page appears displaying a list of incremental backups.

Step 3 To delete all incremental backups, click **Delete All**. A warning appears. Click **OK** to continue.

Related Topics

- Deleting a Full Backup, page 10-7

Viewing and Deleting Backup Schedules

You can view details of the next incremental backup for each schedule you have defined, and you can delete an entire backup schedule.

Procedure

Step 1 Select **Admin > Backup/Retrieve Backup**. The Create Backup page appears.

Step 2 In the TOC in the left pane, select **Scheduled Backups**. The Scheduled Backups page appears displaying a list of the next scheduled backup for each backup schedule. See Scheduled Backups Page, page E-6 for more information about this page.

Step 3 To delete an entire schedule (not just the next backup), select the backup that belongs to the schedule you want to delete, and click **Delete Schedule**.

Tip To modify the time or frequency of a schedule, delete the schedule and create a new schedule.

Related Topics

- Making and Scheduling Backups, page 10-3

Using the QPM Audit

The QPM audit feature provides audit logs about changes made to QPM deployment groups, global libraries, and device information:

- Viewing Audit Logs, page 10-10
- Deleting Audit Logs, page 10-11

Viewing Audit Logs

You can view the following audit logs:

- Policy groups—These logs track changes made to policy group properties and policies, including policy group device assignments in a specified deployment group.
- Deployment groups—These logs track Deploy, Save, Restore, Upload, and Import actions on a deployment group. The audit provides a message for each operation. Three message levels are available—information, warning, and error.
- Libraries—These logs track changes made to IP aliases, application aliases, and policy group templates. (System-created policy group templates are not recorded in the Audit logs.)
- General—These logs track changes made to the QPM device inventory following device rediscovery.

The logs provide links to view the items that have been modified.

Procedure

Step 1 Select **Admin > Audit**. The Audit Trail Policy Groups/Policies page appears.

Step 2 Select the type of logs you want to view in the TOC.

Step 3 For policy groups and deployment groups logs, select the deployment group for which you want to view information.

See the following topics for more information about the fields in these pages:

- Audit Trail Policy Groups/Policies Page, page E-7
- Audit Trail Deployment Group Actions Page, page E-8
- Audit Trail Library Components Page, page E-9
- Audit Trail General Logs Page, page E-10

Related Topics

- Deleting Audit Logs, page 10-11

Deleting Audit Logs

You can delete old audit logs that you no longer need.

Procedure

Step 1 Select **Admin > Audit**. The Audit Trail Policy Groups/Policies page appears.

Step 2 Select the type of logs you want to delete in the TOC.

Step 3 For policy groups and deployment groups logs, select the deployment group for which you want to delete logs. The logs for the selected deployment group are displayed.

Step 4 Click **Clear**. A Calendar dialog box opens.

Step 5 Use the navigation arrows above the calendar table to navigate through the calendar. In the calendar table, choose the date to which you want to delete logs.

Step 6 Click **OK**. The audit logs before and including the selected date are deleted, and no longer appear in the Audit display.

Related Topics

- Viewing Audit Logs, page 10-10

Importing Policies from QPM 2.1.x

You can import policies from a QPM 2.1.x export file. The QPM 2.1.x export file contains policy database information in XML format.

QPM creates new policy groups containing the imported policies and QoS properties. The policies are imported into policy groups, according to the network elements on which they were configured. If the network elements on which the policies were originally defined, exist in the QPM device inventory, you can assign them to the policy groups.

QPM does not assign network elements to existing devices in the following cases:

- The current device constraints are different from the imported devices, for example, the IOS version has been changed.

- The network element belongs to an ASIC.

Note If an interface is a member of an imported QPM 2.1.x device group, and also has its own policies, network element assignments are made only for the QPM 2.1.x device group policies.

The following changes are made to imported policies:

- Imported policies of policy types that have been upgraded in QPM 3 are upgraded. For example, QPM 2.1.x limiting policies are converted to QPM 3 policing policies, QPM 2.1.x coloring policies with PBR are converted to QPM 3 marking policies, and so on.
- Imported application services are translated into appropriate conditions in the filters.
- Imported policies for devices with IOS 12.2T branch versions are mapped to the relevant 12.2T branch version.
- Imported policies for devices with IOS 12.1E branch versions are mapped to the relevant 12.1E branch version.
- Policies for GGSN that are supported by 7200 devices, are imported into policy groups with device constraints for 7200 devices.

The following policies are not imported:

- Policies for devices with IOS 11.1, 11.2, and 11.3.
- Policies for LocalDirector devices.
- GGSN policies that are not supported by 7200 devices.

Before You Begin

- Export your QPM 2.1.x databases using the Export to XML utility that is provided on the QPM installation CD. See the *Installation Guide for QoS Policy Manager 3.0* for information on installing and using the Export to XML utility.
- Ensure that the devices to which you want to assign the imported policies, exist in the QPM device inventory. You can import devices from a QPM 2.1.x exported database into the QPM device inventory. See Chapter 4, "Managing Devices" for more details.

Procedure

Step 1 Select **Admin > Import Policy Groups**. The Import Policy Groups From 2.1 page appears.

Step 2 Select the deployment group to which you want to import the policies.

Step 3 In the Import file path field, enter the name and location of the QPM2.1.x XML file you want to import, or click the Browse button to select the file.

Step 4 Click **OK**.

The Import Policy Groups - Device Selection page appears displaying a list of the devices in the QPM device inventory. By default, all devices are selected.

For more information about this page, see Import Policy Groups - Device Selection Page, page E-13.

Step 5 Clear the check boxes by those devices you do not want to assign to imported policy groups. Click **Import Policies**.

A dialog box appears informing you that the import process has started.

Step 6 In the dialog box, do one of the following:

- View a report showing the status of the import process, and information about the policies that were not imported:
  - Click **View**. The Import Policy Groups Reports page appears.
  - Select the report you want to view, and click **View**. The selected report is displayed in a separate window. See Import Report, page D-28 for information about the Import report.

  Note To view a report later, select **Reports > Import Policy Groups** to display the Import Policy Groups Reports page.

- Click **Continue** to continue editing policies. The Policy Groups page appears.

Note If you are working with multiple ACS device groups, you should repeat this procedure for each device group in your QPM 3 system.

Changing SNMP Settings

QPM uses Simple Network Management Protocol (SNMP) to query network devices, and discover device information.

You can change the following SNMP properties, if you have the appropriate privileges:

- Timeout—Amount of time the system should wait for a device to respond before trying to access it again.
- Retries—Number of times the system tries to access devices.
- Minimum thread number—The minimum number of SNMP requests that can processed concurrently.
- Maximum thread number—The maximum number of SNMP requests that can processed concurrently.

Procedure

Step 1 Select **Admin > SNMP**. The SNMP Properties page appears.

Step 2 Change SNMP parameters as required. See SNMP Parameter/Properties Page, page E-14 for more information about the fields in this page.

Step 3 Click **Save**.

Troubleshooting QPM

The following topics can help you troubleshoot problems you might encounter when using QPM:

Obtaining System Status Information for Troubleshooting

If unusual exceptions occur or error windows are displayed while running QPM, you can obtain system status information by running the QPM Diagnostic Tool on the QPM server. This tool generates a report in a browser window of the system status with its diagnostics, and suggests possible solutions where applicable.

You can access the Diagnostic Tool only from the QPM server.

Note In general, if you come across troubleshooting problems that do not have an obvious solution, you should try logging out of QPM and CiscoWorks, and restarting the QPM server. If the problem persists, run the QPM Diagnostic Tool on the QPM server to create the troubleshooting log file, and consult your system administrator.

If you want to send the diagnostics results to a TAC representative, you can run the MDCSupport.exe command-line utility, which collects configuration and system information in a zip file, called MDCSupportInformation.zip. This zip file includes any problems that occurred during the installation or the running of QPM. You can send this file to the Cisco Technical Assistance Center (TAC) support staff to assist in diagnosing the problems.

Procedure

Step 1 On the QPM server, select **Start > Programs > Cisco Systems > QoS Policy Manager > Diagnostic Tool**.

A report is generated and displayed in a browser window for you to view.

Step 2 To send the diagnostics results to a TAC representative:

a. At the command line, enter **MDCSupport.exe** and press **Enter**.

A zip file named MDCSupportInformation.zip is created under c:\Program Files\CSCOpx\MDC\etc.

b. Send this file to the TAC representative by email.

Problems Starting QoS Policy Manager

The following topics describe causes and solutions for problems you might encounter when trying to start QoS Policy Manager:

Troubleshooting Problems Starting Common Services

Common Services might not start for any of the following reasons:

Changing Windows Account

Problem—If you install Common Services and QPM using a specific admin account/password everything works as planned. However, if you change the password to this Windows account then installed Services fail to start.

Recommended Action—Change the password for all services to match the current password of the account which they were installed. Common Services services include Tomcat, fms, lm, and da-framework.

Port Conflict

Problem—You cannot start Common Services because port 1741, which is used by Common Services is in use by another application.

Recommended Action—Try the following:

- Restart the QPM server.
- To run CiscoWorks, enter http://<*QPMinstall*>:1741/login.html, where <*QPMinstall*> is the name or IP address of the QPM server.

Troubleshooting Problems Starting QPM

QPM might not start for any of the following reasons:

- Old Version of Java Plug-In, page 11-4
- Unknown Cause, page 11-4

Changed Database Password

Problem—If you changed the QPM database password, and then try to start QPM without restarting the QPM server, the connection to the database is lost.

Recommended Action—Restart the QPM server after changing the QPM database password.

Old Version of Java Plug-In

Problem—QPM might not start if there is a older version of the Java plug-in, than required by QPM.

Recommended Action—Uninstall the old java plug-in.When you start CiscoWorks it automatically installs the java plug-in.

Unknown Cause

Recommended Action—Restart the QPM server.

Troubleshooting User Interface Problems

This topic describes causes and solutions for your user interface problems:

- Many buttons in the user interface are grayed out, page 11-4
- Options for QoS features do not appear in the user interface, page 11-5

Many buttons in the user interface are grayed out

Problem—You might not have the correct user permissions to perform the tasks associated with the grayed out buttons.

Recommended Action—Verify your user permissions in the CiscoWorks2000 desktop (**Server Configuration > Setup > Security**), or in ACS (depending on the method you are using for user authentication). For more information about user permissions, and working with ACS user permissions, see the *Installation Guide for QoS Policy Manager 3.0*.

Options for QoS features do not appear in the user interface

Problem—You cannot see options for QoS features that are not valid for the defined device constraints.

Explanation—When you define policy groups and policies, QPM presents you with only those QoS properties, and policy options that are valid for the defined device constraints.

Recommended Action—Verify the defined device constraints. For information about the devices and software releases that QPM supports, and the QoS features you can configure on the supported platforms, see the device support tables at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/qos/qpm3_0/qpm30dev/index.htm

Troubleshooting Device Management Problems

The following sections help you troubleshoot problems with QPM device management:

QPM cannot log into a device

Problem—QPM can connect to a device, but cannot log into it.

Recommended Action—Verify that the device access parameters in the QPM inventory match those configured on the device. If the device access parameters are correct but QPM still cannot log into the device, enable the blind login option, which causes QPM to send login information to the device (including access parameters) without waiting for or evaluating return prompts from the device. For instructions for enabling blind login, see Viewing and Editing Device Properties, page 4-14. You can also configure blind login as the default for all devices in a device group; see Editing Device Group Properties, page 4-37.

A device is not added to the expected device group when imported into QPM

Problem—The device might be defined in ACS as an AAA server and an AAA client, which is supported in ACS but not in QPM. In this case, the device is added to only the QPM AAA client device group in QPM.

Recommended Action—Remove the device from the ACS AAA server device group.

A device has a status that indicates an error

Problem—The device statuses described in Table 11-1 indicate that the device is in an error state. You cannot deploy to devices with these statuses.

Table 11-1 Device Status Errors

Device Status	Description	Explanation
Unreachable	The QPM server cannot establish basic network connectivity to the device.	Establish basic network connectivity to the device.

Table 11-1 Device Status Errors (continued)

Device Status	Description	Explanation
SNMP Error	The device has an SNMP error that is preventing QPM from gathering the data it needs to work with the device.	These are the common causes: • The device public community string entered in QPM is incorrect. Correct the community string in QPM. • QPM can't read all of the necessary SNMP information from the device, possibly because there are corrupted or missing MIBs. • The device does not have a functioning SNMP engine. • The SNMP request timed out, typically because the device or network was too congested to respond before the timeout limit. The possible resolutions are to retry the SNMP connection, or increase the SNMP timeout value.
Telnet Error	QPM cannot connect to the device using Telnet.	These are the common causes: • The device Telnet password entered in QPM is incorrect. Correct the Telnet password in QPM. • SSH is enabled but SSH login failed because SSH is not configured correctly on the device. Fix the SSH configuration on the device. • The login to the device failed. • There is no Telnet connection to the device.

Troubleshooting Deployment Problems

Policies can only be deployed to devices if QPM can correctly contact and connect to the device. QPM can usually provide a specific error message that clearly indicates the problem. However, sometimes providing a clear error message is not possible.

If QPM cannot configure a device, and the error is not clear in the device log for the device, this might be due to any of the following reasons:

Incorrect device read community string

Problem—An SNMP error is returned due to an incorrect read community string. This device access parameter is required by QPM to log into and configure the device.

Recommended Action—Check in the Access Parameters area of the Device Properties page that the device's read community string is correct.

Incorrect software version or device type

Problem—QPM does not support an imported device's Cisco IOS version. The device is assigned the status "Unsupported", and no mapped OS version is assigned to it. You cannot perform any tasks on a device that has been assigned this status.

Recommended Action—If the device model is supported by QPM but the Cisco IOS version is not, you can upgrade the device to a supported Cisco IOS version, and then rediscover the device to make it available in QPM. Click **Rediscover** in the Device Table to have QPM query the device for the correct information.

Deployment fails because QPM could not connect to a device

There are several possible explanations for this problem:

- **Problem**—Unable to log into the device due to an incorrect access passwords.

  Recommended Action—Check in the Device Properties page that the correct Telnet, TACACS, and Enable passwords are defined. QPM does not display the passwords (to maintain security), so carefully retype the passwords.

- **Problem**—There is no connectivity between QPM and the device—the device status is “Unreachable”.

  Recommended Action—Check the device to ensure that it is powered on and that it is connected to the network. Login to the server and telnet to the device to see if you can connect to it (from the Device Properties page).

- **Problem**—There might be a problem with the login prompts returned by the device.

  Recommended Action—Enable the Blind Login check box in the Access Parameters area of the Device Properties page. This feature lets you bypass the login prompts (such as, username and password) that wait for a response when the device returns a string. Then try to log in again.

  In the system configuration file of the QPM installation directory (CSCOpx\MDC\share\config\system.cfg), you can configure blind login for all devices, by setting **devcomm.blind_login=on**. To use blind login for a specific device, set **<***hostname***>.blind_login=On**, where *hostname* is the IP address or host name of the device. This will override the global blind login setting. If required, you can also increase the login timeout delay parameter for the devices (*devcomm/hostname***.blind_login_timeout**).

Configuration messages from the device indicate that distributed Cisco Express Forwarding (dCEF) is not configured on VIP cards

Problem—Some types of QoS configurations require that dCEF is configured on VIP cards and QPM cannot detect this.

Recommended Action—Before distributing policies to VIP interfaces, configure dCEF on the device’s VIP card interfaces through the device’s commands.

Configuration messages from the device indicate that Cisco Express Forwarding (CEF) is not configured on the device

Problem—Some QoS features, such as DWFQ and NBAR, require CEF to be configured on the devices (not on the VIP cards) and QPM cannot detect this.

Recommended Action—Before distributing policies to devices, configure CEF on the device through the device’s commands.

Related Topics

- Viewing and Editing Device Properties, page 4-14
- Connecting to a Device Using Telnet, page 4-16

- Rediscovering Device Information, page 4-18
- Device Properties Page, page A-7

Troubleshooting QoS Analysis Problems

The following sections help you troubleshoot problems with QoS analysis:

- Monitoring Error Messages, page 11-11
- Troubleshooting Display Problems, page 11-14
- Disk Space Shortage Problems, page 11-10

Disk Space Shortage Problems

Cannot perform monitoring; a Disk Space Shortage message appears

Problem—You do not have enough disk space on the QPM server because you have already performed monitoring tasks, and the database is full.

Recommended Action—Follow the instructions in the Disk Space Shortage message to free disk space by rebuilding the QPM database. See Freeing Disk Space for QoS Analysis, page 9-16 for details.

Note

- Occasionally, you might not have enough space in the QPM database for monitoring because the percentage of free disk space defined during installation is too high.

  Your system administrator can change the percentage of free disk space defined in the installation procedure:

  a. On the QPM server, locate the qpm.cfg file under mdc\qpm\config in the Common Services installation folder.
  b. Open qpm.cfg in WordPad or other text editor.
  c. In the command line, **database.trigger.percentage=0**, change the 0 to the percentage of free disk space required.
  d. Save and close the file.
  e. Reboot the QPM server. A new file, qpm.local.cfg, has been created.

f. Open qpm.local.cfg.

The original command line, **database.trigger.percentage=0**, reappears, and a new command line appears, **database.trigger.percentage.actual=<%>**, where % is the percentage you defined.

Monitoring Error Messages

The following sections describe monitoring error messages and their fixes or workarounds:

Error Message: Monitoring system error

Problem—This error message indicates that an unspecified error occurred when attempting to run a report.

Recommended Action—Restarting the QPM server might resolve the problem.

Error Message: Collection service error

Problem—This error message indicates that there was a collection service error when trying to run a real-time report or complete the definition of a historical analysis task. The error message contains additional explanation of the error. Each variation of the error is described in Table 11-2.

Table 11-2 Collection Service Error Troubleshooting

Error Variation	Description	Fix or Workaround
Connection to collector refused	The QPM collector service is not working properly.	Restarting the QPM Collector service might resolve the problem.
Failed to load task to the collector	The QPM collector service is not working properly.	Restarting the QPM Collector service might resolve the problem.
Failed to get settings from the collector	The QPM collector service is not working properly.	Restarting the QPM Collector service might resolve the problem.
Failed to get data from the collector	The QPM collector service is not working properly.	Restarting the QPM Collector service might resolve the problem.

Table 11-2 Collection Service Error Troubleshooting (continued)

Error Variation	Description	Fix or Workaround
SNMP request timeout	SNMP requests sent to the device timed out.	Try the following fixes in this order: 1. Verify basic device connectivity using ping or Telnet. 2. Verify that the device access parameters stored in QPM inventory agree with those configured on the device. 3. Check device CPU load. If it's abnormally high, SNMP requests might not get processed. Lower the CPU load to restore monitoring.
The device: <*IP address*> is not configured with the policy: "<*Policy*>" on interface with MIB index *y*	The device does not contain the policy or MIB index that QPM needs to monitor a policy. This happens when the device is changed in certain ways after the monitoring task was created.	These are possible causes of this error. To resolve the error, fix the applicable problem, then either rerun the real-time analysis report, or redefine the historical analysis task. • The interface is shut down. Enable the interface. • There was an undetected deployment error. Redeploying the policies to the device might resolve the problem. • You deployed policies to a file rather than to the network. QPM cannot detect that policies are deployed to a file, so it updates monitoring tasks that are affected by a policy deployment, even if the changes were not deployed to the actual device. There is no workaround. • You changed the device hardware configuration or created subinterfaces on the device, but did not rediscover the device. Rediscover the device. • You selected a CAR policy with the Mark and Transmit option configured. QPM cannot monitor this QoS configuration. Remove the CAR policy with the Mark and Transmit option from the monitoring task definition.

Error Message: Cannot run task

Problem—The device is not responding because the QPM SNMP timeout was changed to larger than 2 minutes.

Note It is recommended that you use the default QPM SNMP timeout value.

Recommended Action—Try the following fixes in this order:

1. Verify basic device connectivity using ping or Telnet.
2. Verify that the device access parameters stored in QPM inventory agree with those configured on the device.
3. Check device CPU load. If it's abnormally high, SNMP requests might not get processed. Lower the CPU load to restore monitoring.

Error Message: The task does not contain a device from the current device group

Problem—The analysis report cannot run because none of the devices that it is assigned to monitor are still in the current device group. The likely cause is that the devices were removed from the current device group. This error will also occur if you move a device that is being monitored from the Default device group to another device group.

If any of the devices assigned to the monitoring task are still in the current device group, you can run the report, which will contain data only for the devices that are still in the current device group.

Recommended Action—To fix this, add at least one of the devices that are assigned to the monitoring task back into the current device group.

Troubleshooting Display Problems

The following sections describe display problems and their fixes or workarounds:

- Graphs Do Not Appear in Analysis Reports, page 11-15
- Subinterface Graphs Display Incorrect Bandwidth Percentages, page 11-15

Graphs Do Not Appear in Analysis Reports

Problem—The browser's missing graphic icon appears where graphs should appear in analysis reports. The likely cause is that the Common Services session has expired.

Recommended Action—Log out of QPM and log back into Common Services using the Login dialog box in the desktop.

Subinterface Graphs Display Incorrect Bandwidth Percentages

Problem—When a subinterface is displayed in monitoring graphs with the units of display set to percentage, the graph will display incorrect values for the subinterface in the following cases:

- The subinterface has CIR or Minimum CIR configured on it and the value assigned to these Qos features is different than the actual rate configured on the parent interface of the subinterface.
- The bandwidth of the parent interface was changed on the device but the device was not rediscovered by QPM.

Recommended Action—To fix this, rediscover the device. See Rediscovering Device Information, page 4-18.

Troubleshooting the IP Telephony Network

The following topics help you troubleshoot problems with the IP telephony network:

Deployment fails because interface does not support "mls qos vlan-based" command

Problem—This occurs while trying to configure VLAN-based QoS on a Catalyst 6000 device running IOS. The reason it occurs is because you must first configure the switchport command on the interface to configure the VLAN-based QoS command.

Recommended Action—Configure the switchport command (switchport<cr>) manually on the interface before configuring VLAN-based QoS (mls qos vlan-based).

Shaping interval is 0 milliseconds. Intervals below 4 milliseconds rejected

Problem—This message displays while trying to deploy policies to a Frame Relay interface on a VIP card. The reason it occurs is because Modular shaping on VIP cards requires the BC/CIR interval to be in units of 4 milliseconds.

Recommended Action—Adjust the shaping parameters according to the link speed. If you have several rates, you can create a group for each rate. Note that the IP Telephony wizard will assign the interfaces to only one of the groups, and you will have to move the others manually.

Deployment fails for a serial PPP interface

Problem—After assigning a serial Point-to-Point interface with a rate equal to or less than 768kbs, this error occurs on deployment. The reason it occurs is that serial Point-to-Point cannot support LFI, which is applied on interfaces with link speeds below 768kbs.

Recommended Action—Select a multilink interface instead of a serial one. The following provides an example of a Multilink configuration:

- interface Multilink20
  - bandwidth 256
  - ppp multilink
  - multilink-group 20
- interface Serial5/2
  - bandwidth 256
  - encapsulation ppp
  - multilink-group 20

Selected interfaces were not assigned

Problem—After selecting an interface in a configuration step of the IP Telephony wizard, it was not assigned to any voice policy group. It appears in the "Selected but not assigned" counter. The reason could be that the interface has no policies for the current voice role.

Recommended Action—There is no recommended action since this is expected behavior for an interface with no policies for the current voice role. See Assignment Summary, page 5-8 for more details about interface assignments.

Troubleshooting Database Backup Problems

This topic describes causes and solutions for problems you might encounter when trying to backup the QPM database:

Scheduled Incremental Backup Fails

Problem—If the time or date was changed on the QPM server, and the server was not restarted, the scheduled incremental backups following the time/date change fail.

Recommended Action—Restart the QPM server.

Devices Tab Reference

The following topics describe the pages in the Devices tab. Topics are organized according to the following Devices tab options:

Manage

The following topics describe the fields in the pages that are accessed from the Manage option:

Device Table Page

Use this page to:

- View the devices in the device inventory and their device properties.
- Edit device properties.
- Rediscover device information.
- Assign network elements to and remove them from policy groups.
- Assign devices to and remove devices from device folders.
- Delete devices from the inventory.

To open this page, select **Devices > Manage**.

Table A-1 Device Table Page

Field	Description
Deployment Group list box	Contains the deployment groups defined on the system. Choose the deployment group that contains the devices you want to display. When you select a deployment group, only devices that have network elements that are assigned to policy groups in the deployment group will be displayed.
Sys Name column	Displays the system name, which is obtained from the SysName MIB variable. Click a name to display that device's properties.

Table A-1 Device Table Page (continued)

Field	Description
Primary Device Name column	Displays the device IP address or DNS name entered to identify the device when it was added to the inventory.
Model column	Displays the device model. See the section Adding Devices to the Device Inventory, page 4-3 for information about unsupported models.
OS Version column	Displays the device operating system (OS) version.
Mapped OS Version column	Displays the OS version that QPM has mapped to the device. See the section Adding Devices to the Device Inventory, page 4-3 for information about mapped OS versions.

Table A-1 Device Table Page (continued)

Field	Description
Status column	Displays the device status. The following statuses indicate that the device is working properly: • OK • Virtual—The device is a virtual device. The following statuses indicate a problem with the device. You cannot deploy to devices with these statuses: • Unreachable—The QPM server cannot establish basic network connectivity to the device. • SNMP Error—The device has an SNMP error that is preventing QPM from gathering the data it needs to work with the device. These are the common causes: – The device public community string entered in QPM is incorrect. – QPM can't read all of the necessary SNMP information from the device, possibly because there are corrupted or missing MIBs. – The device does not have a functioning SNMP engine. – The SNMP request timed out, typically because the device or network was too congested to respond before the timeout limit. The possible resolutions are to increase the SNMP timeout value and to increase the number of SNMP retries. • Telnet Error—QPM cannot connect to the device using Telnet. These are the common causes: – The device Telnet password entered in QPM is incorrect. Correct the Telnet password in QPM. – SSH is enabled but SSH login failed because SSH is not configured correctly on the device. Fix the SSH configuration on the device. – The login to the device failed. – There is no Telnet connection to the device.

Table A-1 Device Table Page (continued)

Field	Description
Policy Group column	Displays the policy group in the current deployment group to which the device is assigned. The current deployment group is the deployment group selected in the Deployment Group list box above the table. If All is selected in the list box, the current deployment group is displayed in the Deployment Group field in the context area at the top of the page.
Device Folder column	Displays the device folder that contains the device.
Interfaces column	Click the icon for a device to display the Interfaces page for that device.
Edit button	Click to edit the device properties of the selected devices. The Device Properties Page appears.
Rediscover button	Click to rediscover the selected devices. The Discovery Status Page appears.
Set Policy Group button	Click to assign the selected devices to a policy group or remove them from policy groups. The Policy Group Assignment Dialog Box opens.
Set Device Folder button	Click to assign the selected devices to a device folder or remove them from device folders. The Device Folder Setting Dialog Box opens.
Delete button	Click to delete the selected devices from the inventory. A confirmation prompt appears. When deletion is done, the device table refreshes.

Related Topics

- Viewing and Editing Device Properties, page 4-14
- Setting Device Policy Groups Assignments, page 4-17
- Rediscovering Device Information, page 4-18
- Working with Device Folders, page 4-19
- Removing Devices, page 4-24

Policy Group Assignment Dialog Box

Policy groups contain QoS policies and the assigned network elements to which they will be applied.

Use this dialog box to assign devices to policy groups.

To open this dialog box, select one or more devices in the Device Table page by selecting their check boxes, then click **Set Policy Group**.

Table A-2 Policy Group Assignment Dialog Box

Field	Description
Deployment Group list box	Lists deployment groups defined on the system. Select the deployment group that contains the policy group you want to select.
Remove Policy Group Assignments radio button	Click to remove the selected devices from a policy group.
Set Policy Group radio button	Click to assign the selected devices to a policy group.
Policy Group Name column	Lists policy groups that match the constraints of all of the selected devices. Select the policy group to assign by selecting its check box. The message `No suitable Policy Groups Found` appears if there are no policy groups to which all of the selected devices can be assigned.
Description column	Displays a description of the policy group.
OK button	Click to save changes and close the dialog box.
Close button	Click to close the dialog box without saving changes.

Related Topics

- Setting Device Policy Groups Assignments, page 4-17

Device Folder Setting Dialog Box

Device folders are groups of devices, used for organizational purposes.

Use this dialog box to assign devices to device folders.

To open this dialog box, select one or more devices in the Device Table page by selecting their check boxes, then click **Set Device Folder**.

Table A-3 Device Folder Setting Dialog Box

Field	Description
Remove from Device Folder radio button	Click to remove all of the selected devices from any device folder.
Set Device Folder radio button	Click to assign the selected devices to the selected device folder.
Device Folder Name column	Displays the names of the device folders on the system. Select the radio button next to a device folder name to select it.
Device Folder Description column	Displays a description of the device folder.
OK button	Click to save changes and close the dialog box.
Close button	Click to close the dialog box without saving changes.

Related Topics

- Working with Device Folders, page 4-19

Device Properties Page

Use this page to:

- View and edit a device's properties.
- Rediscover a device.
- View a device's running configuration.
- Telnet to a device.
- Export a device's information to a virtual device file.

To open this page, do any of the following in the Device Table page:

- Click a device name.
- Select the check box next to a device name, then click **Edit**.

General Information Area

Table A-4 Device Properties Page - General Information Area

Field	Description
Sys Name field	Displays the system name, which is obtained from the SysName MIB variable. Click a name to display that device's properties.
Primary Device Name field	Displays the device IP address or DNS name entered to identify the device when it was added to the inventory.
IP/DNS field	Displays the device IP address or DNS name. Although this field is a field, you cannot change its data. Changes will not be saved when you click the Save button. You cannot use device DNS names that contain the backslash (\) character.

Table A-4 Device Properties Page - General Information Area (continued)

Field	Description
Status field	Displays the device status. The following statuses indicate that the device is working properly: • OK • Virtual—The device is a virtual device. The following statuses indicate a problem with the device. Devices with these statuses are not usable in QPM: • Unreachable—The QPM server cannot establish basic network connectivity to the device. • SNMP Error—The device has an SNMP error that is preventing QPM from gathering the data it needs to work with the device. These are the common causes: – The device public community string entered in QPM is incorrect. – QPM can't read all of the necessary SNMP information from the device, possibly because there are corrupted or missing MIBs. – The device does not have a functioning SNMP engine. – The SNMP request timed out, typically because the device or network was too congested to respond before the timeout limit. The possible resolutions are to increase the SNMP timeout value and to increase the number of SNMP retries. • Telnet Error—QPM cannot connect to the device using Telnet. The most common cause is that the device Telnet password entered in QPM is incorrect.
Description field	Displays the device description. Edit it to change to description.
Role list box	Displays the device role, if one is assigned. Select a role from the list to assign it to the device.
OS field	Displays the device operating system (OS) version.

Table A-4 Device Properties Page - General Information Area (continued)

Field	Description
Mapped OS list box	Displays the OS version that QPM has mapped to the device. See the section Adding Devices to the Device Inventory, page 4-3 for information about mapped OS versions. **Note** If you change the mapped OS version, QoS that is currently configured on the device might not be supported in the new OS version. See Assignment Conflicts Reports Page, page D-32, for more information.
Model field	Displays the device model.
Last Discovery field	Displays the date the device was last discovered.
Device Group field	Displays the device group to which the device belongs.
Device Folder list box	Displays the device group to which the device is assigned. Select a device folder from the list to assign it to the device.
All Interfaces field	Displays the number of interfaces on the device that are in the QPM inventory.
Ignored Interfaces field	Displays the number of ignored interfaces on the device. Click the number to remove the ignore setting from one or more interfaces. the Ignored Interfaces List Dialog Box opens.

Device Settings Area

Table A-5 Device Properties Page - Device Settings Area

Field	Description
Enable Access Control Policies check box	Select to enable creation and modification of access control policies.
Enable Write Memory check box	Select to enable writing device configuration changes to the device's memory.
Enable NBAR Port Mapping check box	Select to enable NBAR port mapping.
Reset to default button	Click to reset the device settings to the device group defaults.

Access Parameters Area

For security, fields that contain passwords do not display the text that you type.

Table A-6 Device Properties Page - Access Parameters Area

Field	Description
Read Community String field	Contains the device read community string that QPM uses to access the device. You can change it by entering a new value in the field.
Blind login check box	Select to enable blind login to the device, in which QPM sends login information to the device (including access parameters) without waiting for or evaluating return prompts from the device. You can use any characters for the blind login, except $, ^, and \.
Use SSH connection check box	Select to enable support for SSH when connecting to the device.
TACACS User field	Contains the TACACS username that QPM uses to access the device. You can change it by entering a new value in the field.
TACACS Password field	Contains the TACACS password that QPM uses to access the device. You can change it by entering a new value in the field.
TACACS Enable Password field	Contains the TACACS enable password that QPM uses to access the device. You can change it by entering a new value in the field.
User Name field	Contains the username that QPM uses to access the device. You can change it by entering a new value in the field.
Enable Password field	Contains the enable or enable secret password that QPM uses to access the device. You can change it by entering a new value in the field.
Telnet Password field	Contains the Telnet password that QPM uses to access the device. You can change it by entering a new value in the field.
Local Password field	Contains the local password that QPM uses to access the device. You can change it by entering a new value in the field.
Reset to Default button field	Click to reset the values in the Access Parameters area to the device group default values.

ACL Ranges Area

Select ACL ranges for translation of QPM policies to CLI commands.

Note QPM supports only extended ACLs. QPM can upload standard ACLs, and on deployment, they are converted to extended ACLs.

Table A-7 Device Properties Page - ACL Ranges Area

Field	Description
Range 1 From list box	Enter the starting ACL number for range 1.
Range 1 To list box	Enter the end ACL number for range 1.
Range 2 From list box	Enter the starting ACL number for range 2.
Range 2 To list box	Enter the end ACL number for range 2.
Range 3 From list box	Enter the starting ACL number for range 2.
Range 3 To list box	Enter the end ACL number for range 2.

Topology Area

This area displays the topology of the device by listing the device to which each interface connects. Only devices in the QPM inventory that support Cisco Discovery Protocol (CDP) are listed.

Table A-8 Device Properties Page - Topology Area

Field	Description
Interface Name column	Displays the interface name.
Sys Name column	Displays the system name of the device to which to the interface connects. The system name is obtained from the SysName MIB variable.
Primary Device Name column	Displays the primary device name of the device to which to the interface connects.
Model column	Displays the Model of the device to which to the interface connects.
OS Version column	Displays the OS version of the device to which to the interface connects.

Buttons

Table A-9 Device Properties Page - Buttons

Field	Description
Save	Click to save any changes you have made in the page.
Rediscover	Click to rediscover the device. The Discovery Status Page appears.
Show Run	Click to display the device's running configuration. The Display show run Page appears.
Telnet	Click to Telnet to the device using your client system's default Telnet application. Does not work if your client system does not have a Telnet application installed.
Export	Click to export the device's information to a virtual device file, which you can use to import the device into the inventory as a virtual device. The browser's file saving process starts.

Related Topics

- Viewing and Editing Device Properties, page 4-14
- Rediscovering Device Information, page 4-18
- Connecting to a Device Using Telnet, page 4-16
- Viewing Device Configuration, page 4-17
- Importing Device Roles, page 4-23
- Configuring Default Device Access Parameters, page 4-12
- Exporting Device Information, page 4-15

Display show run Page

Use this page to display a device's running configuration.

Click **Show Run** to open.

This page displays the device's running configuration.

Related Topics

- Viewing Device Configuration, page 4-17

Ignored Interfaces List Dialog Box

Use this dialog box to display interfaces that were previously marked as ignored, and therefore hidden in QPM.

Click the number in the Ignored Interfaces field of the Interface Properties page to open.

Table A-10 Ignored Interfaces List Dialog Box

Field	Description
Check box column	Click a check box to select its row.
Name column	Displays the interface name.
Type column	Displays the interface type.
Description column	Displays the interface description.
Rate column	Displays the interface rate.
Card Type column	Displays the interface card type.
Cancel Ignore button	Click to cancel the ignore on the interface, which causes it to appear in the QPM UI again.
Close button	Click to close dialog box.

Related Topics

- Hiding and Displaying Interfaces, page 4-30

Interfaces Page

Use this page to:

- View the interface on a device and their properties.
- Mark interfaces as Ignored, hiding them and their DLCIs and VCs from being displayed in QPM.
- Assign interfaces to policy groups.

To open this dialog box, do any of the following:

- In the Device Table page, click the Interfaces icon in the Interfaces column of a device.
- In the Devices tab TOC, select **Device Information > Interfaces**.

Use this page to view the interfaces on a device.

Table A-11 Interfaces Page

Field	Description
Name column	Displays the interface name.
Type column	Displays the interface type.
Description column	Displays the interface description.
Rate column	Displays the interface rate in kilobits per second.
Card Type column	Displays the interface card type.
Policy Group column	Displays the policy group in the current deployment group to which the interface is assigned. The current deployment group is displayed in the Deployment Group field in the context area at the top of the page.
Connected to Device column	Displays the IP address of the device to which the interface is connected.
Mark as Ignore button	Click to mark the selected interfaces as ignored, which causes them not to appear in the QPM UI. Any DLCIs and VCs configured on ignored interfaces are also ignored. A confirmation dialog box opens. Click **Yes** to confirm the action.
Set Policy Group button	Click to set the policy group to which the interface is assigned. The Policy Group Assignment Dialog Box opens.

Related Topics

- Hiding and Displaying Interfaces, page 4-30
- Policy Group Assignment Dialog Box, page A-6

Interface Properties Page

Use this page to:

- View and edit interface properties.
- Ignore or cancel the ignore setting of interfaces.
- Assign interface subelements to policy groups.

Click the interface name in the Interfaces page to open.

General Area

Table A-12 Interface Properties Page - General Area

Field	Description
Name field	Displays the interface name.
Index field	Displays the interface index.
Type field	Displays the interface type.
Card Type field	Displays the interface card type.
Rate field	Displays the interface rate.
Description field	Displays the interface description.
IP field	Displays the interface IP address.
Subnet Mask field	Displays the interface IP address subnet mask.
Is Ignored check box	Indicated whether the interface is marked as ignored, which prevents it from appearing in the QPM UI. Select the check box to ignore the interface, or clear it to remove the ignore setting.

Topology Area

Note Not all device information is displayed for devices that are not in the QPM inventory. Only devices that support CDP are displayed.

Table A-13 Interface Properties Page - Topology Area

Field	Description
Connected to Device field	Displays the name of the device to which the interface is connected.
IP field	Displays the IP address of the device to which the interface is connected
Model field	Displays the model of the device to which the interface is connected.

VC ATM Area

Table A-14 Interface Properties Page - VC ATM Area

Field	Description
Check box column	Click a check box to select its row.
VC Name column	Displays the VC name.
Policy Group column	Displays the policy group in the current deployment group to which the VC is assigned. The current deployment group is displayed in the Deployment Group field in the context area at the top of the page.
Set Policy Group button	Click to assign the selected VCs to policy groups. The Policy Group Assignment Dialog Box opens.

DLCI Frame Relay Area

Table A-15 Interface Properties Page - DLCI Frame Relay Area

Field	Description
Check box column	Click a check box to select its row.
DLCI Name column	Displays the DLCI name.

Table A-15 Interface Properties Page - DLCI Frame Relay Area (continued)

Field	Description
Policy Group column	Displays the policy group in the current deployment group to which the DLCI is assigned. The current deployment group is displayed in the Deployment Group field in the context area at the top of the page.
Set Policy Group button	Click to assign the selected DLCIs to policy groups. The Policy Group Assignment Dialog Box opens.

Related Topics

- Viewing and Editing Network Element Properties, page 4-25
- Setting Network Element Policy Group Assignments, page 4-26
- Hiding and Displaying Interfaces, page 4-30

Source-Dest Pair Page

Source-destination pairs are logical (not physical) user-supplied network elements defined for Catalyst 8400 series and Catalyst 8500 series switches, which have QoS features that require a named source and destination interface pair on the device.

Use this page to:

- View, create, edit, and delete source-destination pairs on a device.
- Assign source-destination pairs to or remove them from a policy group.

To open this page, select **Devices > Manage**. The Device Table page appears. Then select **Device Information > Source-Dest Pair** from the TOC.

Table A-16 Source-Dest Pair Page

Field	Description
Pair Name column	Displays the source-destination pair name.
Source Interface column	Displays the source interface name.
Target Interface column	Displays the target (destination) interface name.

Table A-16 Source-Dest Pair Page (continued)

Field	Description
Policy Group column	Displays the policy group in the current deployment group to which the source-destination pair is assigned. The current deployment group is displayed in the Deployment Group field in the context area at the top of the page.
Create button	Click to create a new source-destination pair. The Source-Dest Pair Properties Page appears.
Edit button	Click to edit the selected source-destination pair. The Source-Dest Pair Properties Page appears.
Delete button	Click to delete the selected source-destination pair. The Source-Dest Pair Properties Page appears.
Set Policy Group button	Click to set the policy group assignment of the selected source-destination pair. The Policy Group Assignment dialog box Policy Group Assignment Dialog Box opens.

Related Topics

- Working with Source-Destination Pairs, page 4-28
- Source-Dest Pair Properties Page, page A-19

Source-Dest Pair Properties Page

Source-destination pairs are logical (not physical) user-supplied network elements defined for Catalyst 8400 and Catalyst 8500 switches, which have QoS features that require a named source and destination interface pair on the device.

Use this page to view and edit source-destination pair properties.

To open this page, do any of the following in the Source-Dest Pairs page:

- Click a source-destination pair name.
- Click **Create**.
- Select a source-destination pair, then click **Edit**.

Table A-17 Source-Dest Pair Properties Page

Field	Description
Pair Name field	Enter the source-destination pair name.
Source Interface list box	Select the source interface.
Target Interface list box	Select the target interface.
Save button	Click to save changes.

Related Topics

- Working with Source-Destination Pairs, page 4-28
- Source-Dest Pair Page, page A-18

VLANs Page

Use this page to:

- View VLANs that are configured on a device.
- Assign VLANs to or remove them from a policy group.

To open this page, select **Devices > Manage**. The Device Table page opens. Then select **Device Information > VLANs** from the TOC.

Table A-18 VLANs Page

Field	Description
Name column	Displays the VLAN name.
Index column	Displays the VLAN index.
Type column	Displays the VLAN type.

Table A-18 VLANs Page (continued)

Field	Description
Status column	Displays the VLAN status. The possible statuses are: • Operational—The VLAN is operational. • Suspended—The VLAN was suspended by the administrator. • mtuTooBigForDevice—The device cannot participate in the VLAN because the VLAN MTU is larger than the device can support. • mtuTooBigForTrunk—The VLAN MTU is supported by the device, but it is too large for one or more of the device trunk ports.
MTU column	Displays the VLAN MTU.
Policy Group column	Displays the policy group in the current deployment group to which the VLAN is assigned. The current deployment group is displayed in the Deployment Group field in the context area at the top of the page.
Interfaces column	Click the Interfaces icon in this column to view the interfaces that are assigned to the VLAN.
Set Policy Group button	Click to assign the selected VLANs to a policy group. The Policy Group Assignment Dialog Box opens.

Related Topics

- Viewing and Editing Network Element Properties, page 4-25
- Setting Network Element Policy Group Assignments, page 4-26

VLAN Properties Page

Use this page to view and edit a VLAN's properties.

Click the VLAN name in the VLANs page to open.

General Information Area

Table A-19 VLAN Properties Page - General Information Area

Field	Description
Name column	Displays the VLAN name.
Index column	Displays the VLAN index.
IP column	Displays the VLAN IP address.
Subnet Mask column	Displays the IP address subnet mask.
MTU column	Displays the VLAN MTU.
Rate column	Displays the VLAN rate.
Type column	Displays the VLAN type.

VLAN Interfaces Association Area

Table A-20 VLAN Properties Page - VLAN Interfaces Association Area

Field	Description
Interface Name column	Displays the names of the interfaces that are associated to the VLAN.
Is Trunk column	Indicates whether the interface is configured as a trunk.
Is Auxiliary column	Indicates whether the interface is configured as an auxiliary.

Related Topics

- Viewing and Editing Network Element Properties, page 4-25

Import Devices Wizard

Use the Import Devices wizard to import devices into the inventory.

The Import Devices wizard contains the following pages:

- Import Devices Wizard - General Page, page A-23
- Import Devices Wizard - Select Devices Page, page A-26

Import Devices Wizard - General Page

Use this page to import new devices into the inventory. For all the import types except virtual devices (which are not physical devices), QPM discovers the devices to import them. Therefore, devices you attempt to import must be online and connected to the network. You cannot use device DNS names that contain the backslash (\) character to import devices into QPM.

To open this page, select **Devices > Manage**. The Device Table page appears. Then select **Add Device** from the TOC.

This contents of the page vary depending on which radio button is selected.

Import Options

The following radio buttons determine the source of the device import operation and the content of the rest of the page.

Table A-21 Import Devices Wizard - General Page

Field	Description
Manual radio button	Select to import one device manually. The content of the page is described in Manual Import Option, page A-23.
Import from CSV file radio button	Select to import devices from a CSV file created by RME. The content of the page is described in Import from CSV File Option, page A-24.
Import from RME radio button	Select to import devices directly from RME. The content of the page is described in Import from RME Option, page A-25.
Import Virtual Devices from file radio button	Select to import a virtual device from a virtual device file created by QPM. The content of the page is described in Import Virtual Devices from File Option, page A-25.
Import from Qpm 2.x radio button	Select to import devices from QPM version 2.x. The content of the page is described in Import from Qpm 2.x Option, page A-25.
Next button	Click to proceed to the next step.

Manual Import Option

When importing a device manually, you can use the QPM default device access parameters that are configured for the device group to which the device belongs to connect to the device for discovery. In this case, you only must enter the device

IP address or DNS name. If the device does not use the defaults, or you have not configured defaults, you must enter all of the device access parameters necessary to connect to the device.

Table A-22 Import Devices Wizard - General Page - Manual Import Page

Field	Description
IP Address / DNS field	Enter the IP address or the DNS name of the device to import. You cannot use device DNS names that contain the backslash (\) character.
Read Community String field	Enter the device read community string.
Login Mode radio buttons	Select the type of username, password, and enable password you are entering in the page—either Telnet, TACACS, or Local authentication. **Note** This selection affects only how the device credentials you enter are stored in QPM. QPM attempts to discover the device by trying all of the authentication methods.
User Name field	Enter the username to use for connecting to the device.
Password field	Enter the password to use for connecting to the device.
Enable Password field	Enter the enable or enable secret password to use for connecting to the device.

Import from CSV File Option

Table A-23 Import Devices Wizard - General Page - Import from CSV File Option

Field	Description
File field	Enter the path on the client system to the CSV file created by RME from which to import devices.
Browse button	Click to browse to the CSV file instead of typing the path in the File field.
Do not re-import devices that were previously imported, but not added to the QPM inventory. check box	Select to import only those devices that have not been previously imported. Devices that have been imported but not added to the inventory are also not imported if you select this option.

Import from RME Option

Table A-24 Import Devices Wizard - General Page - Import from RME Option

Field	Description
Host Location field	Enter the DNS name or IP address of the RME server from which to import.
Port field	Enter the IP port number of the RME server.
User Name field	Enter the RME username to use to log into the RME server.
Password field	Enter the password for the RME username.
Import only new RME devices check box	Click to import only those devices that have not been previously imported. Devices that have been imported but not added to the inventory are also not imported if you select this option.

Import Virtual Devices from File Option

Table A-25 Import Devices Wizard - General Page - Import Virtual Devices from File Option

Field	Description
File field	Enter the path on the client system to the virtual device file created by QPM from which to import.
Browse button	Click to browse to the virtual device file instead of typing the path in the File field.

Import from Qpm 2.x Option

Table A-26 Import Devices Wizard - General Page - Import from Qpm 2.x Option

Field	Description
File field	Enter the path on the client system to the import file created by QPM 2.x from which to import.
Browse button	Click to browse to the virtual device file instead of typing the path in the File field.

Related Topics

- Import Devices Wizard - Select Devices Page, page A-26
- Adding Devices to the Device Inventory, page 4-3
- Adding a Single Device, page 4-5
- Importing Devices from a Device Inventory CSV File, page 4-6
- Importing Devices from RME, page 4-8
- Importing Virtual Devices, page 4-9
- Importing Devices from QPM 2.1x, page 4-10
- Configuring Default Device Access Parameters, page 4-12

Import Devices Wizard - Select Devices Page

Use this page to select devices to import into the inventory.

To open this page, in the Import Devices Wizard - General page, click the **Next** button.

Table A-27 Import Devices Wizard - Select Devices Page

Field	Description
No User Authorization column	Displays the number of imported devices that you do not have sufficient permissions to add to the QPM inventory. This field does not appear if you are importing devices manually or are importing virtual devices.
Exists in QPM column	Displays the number of devices that are already in the QPM inventory, and therefore cannot be imported again. This field does not appear if you are importing devices manually or are importing virtual devices.
Previously Ignored column	Displays the number of devices that were previously imported but were not added to the QPM inventory. There devices are not available to add to the inventory if you selected the Import only new RME devices check box in the previous step. This field does not appear if you are importing devices manually or are importing virtual devices.

Table A-27 Import Devices Wizard - Select Devices Page (continued)

Field	Description
Total Devices column	Displays the total number of devices that were imported. This field does not appear if you are importing devices manually or are importing virtual devices.
Check box column	Select a check box to select its row.
Primary Device Name column	Displays the device IP address or DNS name entered to identify the device when it was added to the inventory.
Model column	Displays the device model.

Table A-27 Import Devices Wizard - Select Devices Page (continued)

Field	Description
Status column	Displays the device status. The following statuses indicate that the device is working properly: • OK • Virtual—The device is a virtual device. The following statuses indicate a problem with the device. Devices with these statuses are not usable in QPM: • Unreachable—The QPM server cannot establish basic network connectivity to the device. • SNMP Error—The device has an SNMP error that is preventing QPM from gathering the data it needs to work with the device. These are the common causes: – The device public community string entered in QPM is incorrect. – QPM can't read all of the necessary SNMP information from the device, possibly because there are corrupted or missing MIBs. – The device does not have a functioning SNMP engine. – The SNMP request timed out, typically because the device or network was too congested to respond before the timeout limit. The possible resolutions are to increase the SNMP timeout value and to increase the number of SNMP retries. • Telnet Error—QPM cannot connect to the device using Telnet. These are the common causes: – The device Telnet password entered in QPM is incorrect. Correct the Telnet password in QPM. – SSH is enabled but SSH login failed because SSH is not configured correctly on the device. Fix the SSH configuration on the device. – The login to the device failed. – There is no Telnet connection to the device.

Table A-27 Import Devices Wizard - Select Devices Page (continued)

Field	Description
Device Group column	Displays the device group to which the device is assigned.
Back button	Click to return to the previous step.
Finish button	Click to finish the wizard, importing the selected devices.
Cancel button	Click to cancel the wizard.

Related Topics

- Import Devices Wizard - General Page, page A-23
- Adding Devices to the Device Inventory, page 4-3
- Adding a Single Device, page 4-5
- Importing Devices from a Device Inventory CSV File, page 4-6
- Importing Devices from RME, page 4-8
- Importing Virtual Devices, page 4-9
- Importing Devices from QPM 2.1x, page 4-10
- Configuring Default Device Access Parameters, page 4-12

Discovery Status Page

Use this page to view the status of device discovery jobs.

To open this page, do one of the following:

- Select **Devices > Manage**. The Device Table page appears. Then select **Discovery Status** from the TOC.
- Finish the Add Device wizard. The Discovery Status page appears automatically.

Table A-28 Discovery Status Page

Field	Description
Check box column	Select a check box to select its row.
Job Type column	Displays the job type.

Table A-28 Discovery Status Page (continued)

Field	Description
Start column	Displays the job start time.
End column	Displays the job end time.
In Progress column	Displays the number of devices that are in the process of being discovered. Click the number to view details about discovery of these devices. The Discovery Status Devices List Dialog Box opens.
Completed column	Displays the number of devices that have been discovered. Click the number to view details about discovery of these devices. The Discovery Status Devices List Dialog Box opens.
Total column	Displays the number of devices that are in the process of being discovered or have been discovered. Click the number to view details about discovery of these devices. The Discovery Status Devices List Dialog Box opens.
User column	Displays the user who started the job.
Delete button	Click to delete the selected jobs. This does not stop the discovery job.
Refresh Rate list box	Select a page refresh rate from the list. The refresh rate determines how often the page refreshes with updated information.

Related Topics

- Discovery Status Devices List Dialog Box, page A-30
- Viewing Device Discovery Status, page 4-13
- Rediscovering Device Information, page 4-18

Discovery Status Devices List Dialog Box

Use this dialog box to get detailed information about devices in the Discovery Status report.

To open, click the number in the In Progress, Completed, or Total columns in the Discovery Status report.

Table A-29 Discovery Status Devices List Dialog Box.

Field	Description
Primary Device Name column	Displays the device IP address or DNS name entered to identify the device when it was added to the inventory.
Model column	Displays the device model.

Table A-29 Discovery Status Devices List Dialog Box. (continued)

Field	Description
Status column	Displays the device status. The following statuses indicate that the device is working properly: • OK • Virtual—The device is a virtual device. The following statuses indicate a problem with the device. Devices with these statuses are not usable in QPM: • Unreachable—The QPM server cannot establish basic network connectivity to the device. • SNMP Error—The device has an SNMP error that is preventing QPM from gathering the data it needs to work with the device. These are the common causes: – The device public community string entered in QPM is incorrect. – QPM can't read all of the necessary SNMP information from the device, possibly because there are corrupted or missing MIBs. – The device does not have a functioning SNMP engine. – The SNMP request timed out, typically because the device or network was too congested to respond before the timeout limit. The possible resolutions are to increase the SNMP timeout value and to increase the number of SNMP retries. • Telnet Error—QPM cannot connect to the device using Telnet. These are the common causes: – The device Telnet password entered in QPM is incorrect. Correct the Telnet password in QPM. – SSH is enabled but SSH login failed because SSH is not configured correctly on the device. Fix the SSH configuration on the device. – The login to the device failed. – There is no Telnet connection to the device.

Table A-29 Discovery Status Devices List Dialog Box. (continued)

Field	Description
OS column	Displays the device operating system (OS) version.
Mapped OS column	Displays the OS version that QPM has mapped to the device. See Adding Devices to the Device Inventory, page 4-3 for information about mapped OS versions.
Close button	Click to close the dialog box.

Related Topics

- Discovery Status Page, page A-29
- Viewing Device Discovery Status, page 4-13
- Rediscovering Device Information, page 4-18

Device Groups Page

Device groups are groups of devices (and their network elements) within the inventory that are created and maintained in ACS, except the default device group, which exists and is maintained only in QPM.

Use this page to:

- View the device groups in the inventory.
- Edit device group properties.

To open this page, select **Devices > Manage**. The Device Table page appears. Then select **Device Groups** from the TOC.

Table A-30 Device Groups Page

Field	Description
Radio button column	Select a radio button to select its row.
Name column	Displays the device group name.
Description column	Displays the device group description.
Active Device Group column	Indicates whether the device group is the active device group. The active device group has a check mark in this column.

Table A-30 Device Groups Page (continued)

Field	Description
Device Folders column	Click the Device Folders icon in the column to view the device folders that exist within the device group. The Device Folders page appears.
Edit button	Click to edit the properties of the selected device group. The Device Group Properties Page appears.
Set Active button	Click to set the selected device group as the active device group. This setting takes effect throughout the QPM UI. Only the devices, deployment groups, and policy groups in the active device group appear in the UI. To work with items from another device group in the QPM UI, set that device group to be the active device group.
Delete button	Click to delete the selected device group. Any deployment groups and policy groups contained in the device group are also deleted. This feature is useful because device groups are not automatically deleted from QPM when you delete them in ACS, even when you synchronize device group information with ACS. This gives you the opportunity to edit your QPM deployment groups and policy groups before manually deleting the device group.

Related Topics

- Device Group Properties Page, page A-35
- Working with Device Groups, page 4-34
- Understanding Device Groups, page 4-34
- Setting the Active Device Group, page 4-35
- Synchronizing Permissions and Device Group Information, page 4-36
- Editing Device Group Properties, page 4-37

Device Group Properties Page

Device groups are groups of devices (and their network elements) within the inventory that are created and maintained in ACS, except the default device group, which exists and is maintained only in QPM.

Many of the device group properties are the same properties that QPM maintains for devices. These device group properties are assigned to all devices in the device group by default. You can override these defaults by entering different device properties for an individual device.

Use this page to view and edit device group properties.

To open this page, do any of the following in the Device Groups page:

- Click a device group name.
- Select the check box next to a device group, then click **Edit**.

General Information Area

Table A-31 Device Group Properties Page - General Information Area

Field	Description
Device Group Name field	Displays the device group name.
Description field	Displays the device group description. Edit the text in this field to change the description.

Device Settings Area

Table A-32 Device Group Properties Page - Device Settings Area

Field	Description
Enable Access Control Policies check box	Select to enable creation and modification of access control policies.
Enable Write Memory check box	Select to enable writing device configuration changes to the device's memory.
Enable NBAR Port Mapping check box	Select to enable NBAR port mapping.

Default Access Parameters Area

For security, fields that contain passwords do not display the text you enter.

Table A-33 Device Group Properties Page - Default Access Parameters Area

Field	Description
Read Community String field	Contains the device read community string that QPM uses to access the device. You can change it by entering a new value in the field.
Blind login check box	Select to enable blind login to the device, in which QPM sends login information to the device (including access parameters) without waiting for or evaluating return prompts from the device. You can use any characters for the blind login, except $, ^, and \.
Use SSH connection check box	Select to enable support for SSH when connecting to the device.
TACACS User field	Contains the TACACS username that QPM uses to access the device. You can change it by entering a new value in the field.
TACACS Password field	Contains the TACACS password that QPM uses to access the device. You can change it by entering a new value in the field.
TACACS Enable Password field	Contains the TACACS enable password that QPM uses to access the device. You can change it by entering a new value in the field.
User Name field	Contains the username that QPM uses to access the device. You can change it by entering a new value in the field.
Enable Password field	Contains the enable or enable secret password that QPM uses to access the device. You can change it by entering a new value in the field.
Telnet Password field	Contains the Telnet password that QPM uses to access the device. You can change it by entering a new value in the field.
Local Password field	Contains the local password that QPM uses to access the device. You can change it by entering a new value in the field.

ACL Ranges Area

Select ACL ranges for translation of QPM policies to CLI commands.

Note QPM supports only extended ACLs. QPM can upload standard ACLs, and on deployment, they are converted to extended ACLs.

Table A-34 Device Group Properties Page - ACL Ranges Area

Field	Description
Range 1 From list box	Enter the starting ACL number for range 1.
Range 1 To list box	Enter the end ACL number for range 1.
Range 2 From list box	Enter the starting ACL number for range 2.
Range 2 To list box	Enter the end ACL number for range 2.
Range 3 From list box	Enter the starting ACL number for range 2.
Range 3 To list box	Enter the end ACL number for range 2.

Buttons

Table A-35 Device Group Properties Page - Buttons

Field	Description
Save button	Click to save any changes you have made in the page.

Related Topics

- Device Groups Page, page A-33
- Working with Device Groups, page 4-34
- Understanding Device Groups, page 4-34
- Setting the Active Device Group, page 4-35
- Synchronizing Permissions and Device Group Information, page 4-36
- Editing Device Group Properties, page 4-37

Device Folders Page

Device folders are groups of devices, used for organizational purposes.

Use this page to view, create, edit, and delete device folders.

To open this page, do any of the following:

- From the Device Groups page, click the Device Folders icon in the Device Folders column of a device group.
- Select **Devices > Manage**. The Device Table page appears. Then select **Device Folders** from the TOC.

Table A-36 Device Folders Page

Field	Description
Check box column	Select a check box to select its row.
Name column	Displays the device folder name. Click a device folder name to view or edit the device folder properties.
Description column	Displays the device folder description.
Devices column	Click the Devices icon in the Devices column to view the devices in a device folder. The Device Table page appears.
Create button	Click to create a new device folder. The Device Folder Properties Page appears.
Edit button	Click to edit the selected device folder. The Device Folder Properties Page appears.
Delete button	Click to delete the selected device folder.

Related Topics

- Device Folder Properties Page, page A-39
- Working with Device Folders, page 4-19
- Creating Device Folders, page 4-20
- Organizing Devices with Device Folders, page 4-21
- Editing Device Folders, page 4-21
- Deleting Device Folders, page 4-22

Device Folder Properties Page

Device folders are groups of devices, used for organizational purposes.

Use this page to view and edit device folders properties, and create new device folders.

To open this page, do any of the following from the Device Folders page:

- Click a device folder name.
- Select the check box next to a device folder name, then click **Edit**.

Table A-37 Device Folder Properties Page

Field	Description
Device Folder Name field	Displays the device folder name. Change the name by editing this field.
Description field	Displays the device folder description. Change the description by editing this field.
Save button	Click to save any changes you have made in the page.

Related Topics

- Device Folders Page, page A-38
- Working with Device Folders, page 4-19
- Creating Device Folders, page 4-20
- Organizing Devices with Device Folders, page 4-21
- Editing Device Folders, page 4-21
- Deleting Device Folders, page 4-22

Search

The following topics describe the fields in the pages that are accessed from the Search option:

Related Topics

Search for Devices Page

Use this page to search for devices.

To open this page, select **Devices > Search**.

Network Element Criteria Area

Table A-38 Search for Devices Page, Network Element Criteria Area

Field	Description
Contains or belongs to column	Select a source for the search criteria statement. The list entries are qualities of the network element. For example, to search for devices that have serial interfaces, select **Interface**.
Attribute column	Select an attribute of the source selected in the Source column. For example, to search for devices that have serial interfaces, select **Type**.
Operator column	Select an operator that describes the relationship between the attribute and the value. For example, to search for devices that have serial interfaces, select **Contains**.
Value column	Enter values on which to search. Separate multiple values with commas. If you enter multiple values, they are connected by logical OR, meaning that the search will find network elements that match any of the values. QPM will search for devices by evaluating the relationship between the values you enter and the source attribute you select. Network elements on which the relationship between the values and the source attribute are related as specified by the operator you select will appear in the search results. For example, to search for devices that have serial interfaces, enter **s**, because all serial interface names will contain that character.

Assignment Criteria Area

Table A-39 Search for Devices Page, Assignment Criteria Area

Field	Description
Operator column	Select an operator that describes the relationship of the network element to the assignment criteria. Assigned means that a network element must be assigned to the selected policy group(s). Not Assigned means that a network element must not be assigned to the selected policy group(s).
Deployment Group column	Select the deployment group for the search criteria. The selection in this list determines which policy groups will appear in the Policy Group list. Select **Any** to select all deployment groups on the system, which automatically selects Any in the Policy Group list.
Policy Group column	Select the policy group for the search criteria. Which policy groups are available in this list depends on your selection in the Deployment Group list. Select **Any** to select all policy groups in the selected deployment group.

Other Controls

Table A-40 Search for Devices Page, Other Controls

Field	Description
Match All radio button	Select to connect all search criteria statements by logical AND, meaning that the search will find network elements that match all of the criteria statements.
Match Any radio button	Select to connect all search criteria statements by logical OR, meaning that the search will find network elements that match any of the criteria statements.
Refresh Summary button	Click to see the search criteria expressed as a sentence in the Summary field.
Summary field	Displays the search criteria expressed as a sentence.

Table A-40 Search for Devices Page, Other Controls (continued)

Field	Description
Search Now button	Click to run the currently configured search. The results appear in the Devices Search Result Page.
Reset button	Click to clear all search criteria.

Related Topics

- Searching for Devices and Network Elements, page 4-32

Devices Search Result Page

Use this page to view the results of a search for devices.

To open this page, click **Search Now** in the Search for Devices Page.

Table A-41 Devices Search Result Page

Field	Description
Check box column	Select a check box to select its row.
Sys Name column	Displays the system name, which is obtained from the SysName MIB variable. Click a name to display that device's properties.
Primary Device Name column	Displays the device IP address or DNS name entered to identify the device when it was added to the inventory.
Model column	Displays the device model. See the section Adding Devices to the Device Inventory, page 4-3 for information about unsupported models.
OS Version column	Displays the device operating system (OS) version.
Mapped OS Version column	Displays the OS version that QPM has mapped to the device. See the section Adding Devices to the Device Inventory, page 4-3 for information about mapped OS versions.

Table A-41 Devices Search Result Page (continued)

Field	Description
Status column	Displays the device status. The following statuses indicate that the device is working properly: • OK • Virtual—The device is a virtual device. The following statuses indicate a problem with the device. You cannot deploy to devices with these statuses: • Unreachable—The QPM server cannot establish basic network connectivity to the device. • SNMP Error—The device has an SNMP error that is preventing QPM from gathering the data it needs to work with the device. These are the common causes: – The device public community string entered in QPM is incorrect. – QPM can't read all of the necessary SNMP information from the device, possibly because there are corrupted or missing MIBs. – The device does not have a functioning SNMP engine. – The SNMP request timed out, typically because the device or network was too congested to respond before the timeout limit. The possible resolutions are to increase the SNMP timeout value and to increase the number of SNMP retries. • Telnet Error—QPM cannot connect to the device using Telnet. These are the common causes: – The device Telnet password entered in QPM is incorrect. Correct the Telnet password in QPM. – SSH is enabled but SSH login failed because SSH is not configured correctly on the device. Fix the SSH configuration on the device. – The login to the device failed. – There is no Telnet connection to the device.

Table A-41 Devices Search Result Page (continued)

Field	Description
Policy Group column	Displays the policy group to which the device is assigned in the active deployment group.
Device Folder column	Displays the device folder that contains the device.
Interfaces column	Click the icon for a device to display the Interfaces page for that device.
Edit button	Click to edit the device properties of the selected device. The Device Properties Page appears.
Rediscover button	Click to rediscover the selected devices. The Discovery Status Page appears.
Set Device Folder button	Click to assign the selected devices to a device folder or remove them from device folders. The Device Folder Setting Dialog Box appears.
Delete button	Click to delete the selected devices from the inventory. A confirmation prompt appears. When deletion is done, the device table refreshes. All of the deleted device's policy group assignments are also deleted.
Set Policy Group button	Click to assign the selected devices to a policy group or remove them from policy groups. The Policy Group Assignment Dialog Box opens.

Search for Interfaces Page

Use this page to search for interfaces.

To open this page, select **Devices > Search**. The Search for Devices page appears. Then select **Interfaces** from the TOC.

Network Element Criteria Area

Table A-42 Search for Interfaces Page, Network Element Criteria Area

Field	Description
Contains or belongs to column	Select a source for the search criteria statement. The list entries are qualities of the network element. For example, to search for interfaces that are members of a VLAN whose name contains the string “eng”, select **VLAN**.
Attribute column	Select an attribute of the source selected in the Source list box. For example, to search for interfaces that are members of a VLAN whose name contains the string “eng”, select **Name**.
Operator column	Select an operator that describes the relationship between the attribute and the value. For example, to search for interfaces that are members of a VLAN whose name contains the string “eng”, select **Contains**.
Value column	Enter values on which to search. Separate multiple values with commas. If you enter multiple values, they are connected by logical OR, meaning that the search will find network elements that match any of the values. QPM will search for network elements by evaluating the relationship between the values you enter and the source attribute you select. Network elements on which the relationship between the values and the source attribute are related as specified by the operator you select will appear in the search results. For example, to search for interfaces that are members of a VLAN whose name contains the string “eng”, enter **eng**.

Assignment Criteria Area

Table A-43 Search for Interfaces Page, Assignment Criteria Area

Field	Description
Operator column	Select an operator that describes the relationship of the network element to the assignment criteria. Assigned means that a network element must be assigned to the selected policy group(s). Not Assigned means that a network element must not be assigned to the selected policy group(s).
Deployment Group column	Select the deployment group for the search criteria. The selection in this list determines which policy groups will appear in the Policy Group list. Select **Any** to select all deployment groups on the system, which automatically selects Any in the Policy Group list.
Policy Group list column	Select the policy group for the search criteria. Which policy groups are available in this list depends on your selection in the Deployment Group list. Select **Any** to select all policy groups in the selected deployment group.

Other Controls

Table A-44 Search for Interfaces Page, Other Controls

Field	Description
Match All radio button	Select to connect all search criteria statements by logical AND, meaning that the search will find network elements that match all of the criteria statements.
Match Any radio button	Select to connect all search criteria statements by logical OR, meaning that the search will find network elements that match any of the criteria statements.
Refresh Summary button	Click to see the search criteria expressed as a sentence in the Summary field.
Summary field	Displays the search criteria expressed as a sentence.

Table A-44 Search for Interfaces Page, Other Controls (continued)

Field	Description
Search Now button	Click to run the currently configured search. The results appear in the Interfaces Search Result Page.
Reset button	Click to clear all search criteria.

Related Topics

- Searching for Devices and Network Elements, page 4-32

Interfaces Search Result Page

Use this page to view the results of a search for interfaces.

To open this page, click **Search Now** in the Search for Interfaces Page.

Table A-45 Interfaces Search Result Page

Field	Description
Check box column	Select a check box to select its row.
Name column	Displays the interface name.
Sys Name column	Displays the sys name of the device on which the interface is located.
Type column	Displays the interface type.
Description column	Displays the interface description.
Rate column	Displays the interface rate in kilobits per second.
Card Type column	Displays the interface card type.
Policy Group column	Displays the policy group in the current deployment group to which the interface is assigned.
Connected to Device column	Displays the IP address of the device to which the interface is connected.

Table A-45 Interfaces Search Result Page (continued)

Field	Description
Mark as Ignore button	Click to mark the selected interfaces as ignored, which causes them not to appear in the QPM UI. Ignored interfaces are not configured by QPM. Any DLCIs and VCs configured on ignored interfaces are also ignored. A confirmation dialog box opens. Click Yes to confirm the action. For information about hiding and displaying ignored interfaces, see Hiding and Displaying Interfaces, page 4-30.
Set Policy Group button	Click to set the policy group to which the interface is assigned. The Policy Group Assignment Dialog Box appears.

Search for VLANs Page

Use this page to search for VLANs.

To open this page, select **Devices > Search**. The Search for Device page appears. Then select **VLANs** from the TOC.

Network Element Criteria Area

Table A-46 Search for VLANs Page, Network Element Criteria Area

Field	Description
Contains or belongs to column	Select a source for the search criteria statement. The list entries are qualities of the network element. For example, to search for VLANs that contain Ethernet interfaces, select **Interface**.
Attribute column	Select an attribute of the source selected in the Source column. For example, to search for VLANs that contain Ethernet interfaces, select **Type**.

Table A-46 Search for VLANs Page, Network Element Criteria Area (continued)

Field	Description
Operator column	Select an operator that describes the relationship between the attribute and the value. For example, to search for VLANs that contain Ethernet interfaces, select **Contains**.
Value column	Enter values on which to search. Separate multiple values with commas. If you enter multiple values, they are connected by logical OR, meaning that the search will find network elements that match any of the values. QPM will search for network elements by evaluating the relationship between the values you enter and the source attribute you select. Network elements on which the relationship between the values and the source attribute are related as specified by the operator you select will appear in the search results. For example, to search for VLANs that contain Ethernet interfaces, enter **Ethernet**.

Assignment Criteria Area

Table A-47 Search for VLANs Page, Assignment Criteria Area

Field	Description
Operator column	Select an operator that describes the relationship of the network element to the assignment criteria. Assigned means that a network element must be assigned to the selected policy group(s). Not Assigned means that a network element must not be assigned to the selected policy group(s).

Table A-47 Search for VLANs Page, Assignment Criteria Area (continued)

Field	Description
Deployment Group column	Select the deployment group for the search criteria. The selection in this list determines which policy groups will appear in the Policy Group list. Select **Any** to select all deployment groups on the system, which automatically selects Any in the Policy Group list.
Policy Group column	Select the policy group for the search criteria. Which policy groups are available in this list depends on your selection in the Deployment Group list. Select **Any** to select all policy groups in the selected deployment group.

Other Controls

Table A-48 Search for VLANs Page, Other Controls

Field	Description
Match All radio button	Select to connect all search criteria statements by logical AND, meaning that the search will find network elements that match all of the criteria statements.
Match Any radio button	Select to connect all search criteria statements by logical OR, meaning that the search will find network elements that match any of the criteria statements.
Refresh Summary button	Click to see the search criteria expressed as a sentence in the Summary field.
Summary field	Displays the search criteria expressed as a sentence.
Search Now button	Click to run the currently configured search. The results appear in the VLANs Search Result Page.
Reset button	Click to clear all search criteria.

Related Topics

- Searching for Devices and Network Elements, page 4-32

VLANs Search Result Page

Use this page to view the results of a search for VLANs.

To open this page, click **Search Now** in the Search for VLANs Page.

Table A-49 VLANs Search Result Page

Field	Description
Check box column	Select a check box to select its row.
Name column	Displays the VLAN name.
Index column	Displays the VLAN index.
Type column	Displays the VLAN type.
Status column	Displays the VLAN status. The possible statuses are: • Operational—The VLAN is operational. • Suspended—The VLAN was suspended by the administrator. • mtuTooBigForDevice—The device cannot participate in the VLAN because the VLAN MTU is larger than the device can support. • mtuTooBigForTrunk—The VLAN MTU is supported by the device, but it is too large for one or more of the device trunk ports.
MTU column	Displays the VLAN MTU.
Policy Group column	Displays the policy group in the current deployment group to which the VLAN is assigned.
Interfaces column	Click the Interfaces icon in this column to view the interfaces that are assigned to the VLAN.
Set Policy Group button	Click to assign the selected VLANs to a policy group. The Policy Group Assignment Dialog Box opens.

Search for VCs Page

Use this page to search for VCs.

To open this page, select **Devices > Search**. The Search for Device page appears. Then select **VCs** from the TOC.

Network Element Criteria Area

Table A-50 Search for VCs Page, Network Element Criteria Area

Field	Description
Contains or belongs to column	Select a source for the search criteria statement. The list entries are qualities of the network element. For example, to search for VCs whose name contains the string "west", select **VC**.
Attribute column	Select an attribute of the source selected in the Source column. For example, to search for VCs whose name contains the string "west", select **Name**.
Operator column	Select an operator that describes the relationship between the attribute and the value. For example, to search for VCs whose name contains the string "west", select **Contains**.
Value column	Enter values on which to search. Separate multiple values with commas. If you enter multiple values, they are connected by logical OR, meaning that the search will find network elements that match any of the values. QPM will search for network elements by evaluating the relationship between the values you enter and the source attribute you select. Network elements on which the relationship between the values and the source attribute are related as specified by the operator you select will appear in the search results. For example, to search for VCs whose name contains the string "west", enter **west**.

Assignment Criteria Area

Table A-51 Search for VCs Page, Assignment Criteria Area

Field	Description
Operator column	Select an operator that describes the relationship of the network element to the assignment criteria. Assigned means that a network element must be assigned to the selected policy group(s). Not Assigned means that a network element must not be assigned to the selected policy group(s).
Deployment Group column	Select the deployment group for the search criteria. The selection in this list determines which policy groups will appear in the Policy Group list. Select **Any** to select all deployment groups on the system, which automatically selects Any in the Policy Group list.
Policy Group column	Select the policy group for the search criteria. Which policy groups are available in this list depends on your selection in the Deployment Group list. Select **Any** to select all policy groups in the selected deployment group.

Other Controls

Table A-52 Search for VCs Page, Other Controls

Field	Description
Match All radio button	Select to connect all search criteria statements by logical AND, meaning that the search will find network elements that match all of the criteria statements.
Match Any radio button	Select to connect all search criteria statements by logical OR, meaning that the search will find network elements that match any of the criteria statements.
Refresh Summary button	Click to see the search criteria expressed as a sentence in the Summary field.
Summary field	Displays the search criteria expressed as a sentence.

Table A-52 Search for VCs Page, Other Controls (continued)

Field	Description
Search Now button	Click to run the currently configured search. The results appear in the VCs Search Result Page.
Reset button	Click to clear all search criteria.

Related Topics

- Searching for Devices and Network Elements, page 4-32

VCs Search Result Page

Use this page to view the results of a search for VCs.

To open this page, click **Search Now** in the Search for VCs Page.

Table A-53 VCs Search Result Page

Field	Description
Check box column	Click a check box to select its row.
Name column	Displays the VC name.
Interface Name column	Displays the name of the interface on which the VC exists.
Sys Name column	Displays the sys name of the device on which the VC exists.
Policy Group column	Displays the policy group in the current deployment group to which the VC is assigned.
Set Policy Group button	Click to assign the selected VCs to policy groups. The Policy Group Assignment Dialog Box opens.

Search for DLCIs Page

Use this page to search for DLCIs.

To open this page, select **Devices > Search**. The Search for Device page appears. Then select **DLCIs** from the TOC.

Network Element Criteria Area

Table A-54 Search for DLCIs Page, Network Element Criteria Area

Field	Description
Contains or belongs to column	Select a source for the search criteria statement. The list entries are qualities of the network element. For example, to search for all DLCIs that are on devices that are members of a device folder named "West Coast", select **Device Folder**.
Attribute column	Select an attribute of the source selected in the Source column. For example, to search for all DLCIs that are on devices that are members of a device folder named "West Coast", select **Name**.
Operator column	Select an operator that describes the relationship between the attribute and the value. For example, to search for all DLCIs that are on devices that are members of a device folder named "West Coast", select **Equals**.
Value column	Enter values on which to search. Separate multiple values with commas. If you enter multiple values, they are connected by logical OR, meaning that the search will find network elements that match any of the values. QPM will search for network elements by evaluating the relationship between the values you enter and the source attribute you select. Network elements on which the relationship between the values and the source attribute are related as specified by the operator you select will appear in the search results. For example, to search for all DLCIs that are on devices that are members of a device folder named "West Coast", enter **West Coast**.

Assignment Criteria Area

Table A-55 Search for DLCIs Page, Assignment Criteria Area

Field	Description
Operator column	Select an operator that describes the relationship of the network element to the assignment criteria. Assigned means that a network element must be assigned to the selected policy group(s). Not Assigned means that a network element must not be assigned to the selected policy group(s).
Deployment Group column	Select the deployment group for the search criteria. The selection in this list determines which policy groups will appear in the Policy Group list. Select **Any** to select all deployment groups on the system, which automatically selects Any in the Policy Group list.
Policy Group column	Select the policy group for the search criteria. Which policy groups are available in this list depends on your selection in the Deployment Group list. Select **Any** to select all policy groups in the selected deployment group.

Other Controls

Table A-56 Search for DLCIs Page, Other Controls

Field	Description
Match All radio button	Select to connect all search criteria statements by logical AND, meaning that the search will find network elements that match all of the criteria statements.
Match Any radio button	Select to connect all search criteria statements by logical OR, meaning that the search will find network elements that match any of the criteria statements.
Refresh Summary button	Click to see the search criteria expressed as a sentence in the Summary field.
Summary field	Displays the search criteria expressed as a sentence.

Table A-56 Search for DLCIs Page, Other Controls (continued)

Field	Description
Search Now button	Click to run the currently configured search. The results appear in the DLCIs Search Result Page.
Reset button	Click to clear all search criteria.

Related Topics

- Searching for Devices and Network Elements, page 4-32

DLCIs Search Result Page

Use this page to view the results of a search for DLCIs.

To open this page, click **Search Now** in the Search for DLCIs Page.

Table A-57 DLCIs Search Result Page

Field	Description
Check box column	Select a check box to select its row.
Name column	Displays the DLCI name.
Interface Name column	Displays the interface name.
Sys Name column	Displays the sys name of the device.
Policy Group column	Displays the policy group to which the DLCI is assigned in the current deployment group.
Set Policy Group button	Click to set the policy group to which the selected DLCI is assigned. The Policy Group Assignment Dialog Box opens.

Search for Source-Dest Pairs Page

Use this page to search for Source-Dest Pairs.

To open this page, select **Devices > Search**. The Search for Device page appears. Then select **Source-Dest Pairs** from the TOC.

Network Element Criteria Area

Table A-58 Search for Source-Dest Pairs Page, Network Element Criteria Area

Field	Description
Contains or belongs to column	Select a source for the search criteria statement. The list entries are qualities of the network element. For example, to search for all source-destination pairs that are on Cisco 8400 series devices, select **Device**.
Attribute column	Select an attribute of the source selected in the Source column. For example, to search for all source-destination pairs that are on Cisco 8400 series devices, select **Model**.
Operator column	Select an operator that describes the relationship between the attribute and the value. For example, to search for all source-destination pairs that are on Cisco 8400 series devices, select **Contains**.
Value column	Enter values on which to search. Separate multiple values with commas. If you enter multiple values, they are connected by logical OR, meaning that the search will find network elements that match any of the values. QPM will search for network elements by evaluating the relationship between the values you enter and the source attribute you select. Network elements on which the relationship between the values and the source attribute are related as specified by the operator you select will appear in the search results. For example, to search for all source-destination pairs that are on Cisco 8400 series devices, enter **8400**.

Assignment Criteria Area

Table A-59 Search for Source-Dest Pairs Page, Assignment Criteria Area

Field	Description
Operator column	Select an operator that describes the relationship of the network element to the assignment criteria. Assigned means that a network element must be assigned to the selected policy group(s). Not Assigned means that a network element must not be assigned to the selected policy group(s).
Deployment Group column	Select the deployment group for the search criteria. The selection in this list determines which policy groups will appear in the Policy Group list. Select **Any** to select all deployment groups on the system, which automatically selects Any in the Policy Group list.
Policy Group column	Select the policy group for the search criteria. Which policy groups are available in this list depends on your selection in the Deployment Group list. Select **Any** to select all policy groups in the selected deployment group.

Other Controls

Table A-60 Search for Source-Dest Pairs Page, Other Controls

Field	Description
Match All radio button	Select to connect all search criteria statements by logical AND, meaning that the search will find network elements that match all of the criteria statements.
Match Any radio button	Select to connect all search criteria statements by logical OR, meaning that the search will find network elements that match any of the criteria statements.
Refresh Summary button	Click to see the search criteria expressed as a sentence in the Summary field.
Summary field	Displays the search criteria expressed as a sentence.

Table A-60 Search for Source-Dest Pairs Page, Other Controls (continued)

Field	Description
Search Now button	Click to run the currently configured search. The results appear in the Source-Dest Pairs Search Result Page.
Reset button	Click to clear all search criteria.

Related Topics

- Searching for Devices and Network Elements, page 4-32

Source-Dest Pairs Search Result Page

Use this page to view the results of a search for source-dest pairs.

To open this page, click **Search Now** in the Search for Source-Dest Pairs Page.

Table A-61 Source-Dest Pair Page

Field	Description
Pair Name column	Displays the source-destination pair name.
Source Interface column	Displays the source interface name.
Target Interface column	Displays the target (destination) interface name.
Policy Group column	Displays the policy group in the current deployment group to which the source-destination pair is assigned.
Edit button	Click to edit the selected source-destination pair.The Source-Dest Pair Properties Page appears.
Delete button	Click to delete the selected source-destination pair. The Source-Dest Pair Properties Page appears.
Set Policy Group button	Click to set the policy group assignment of the selected source-destination pair. The Policy Group Assignment dialog box Policy Group Assignment Dialog Box opens.

Options

The following topics describe the fields in the pages that are accessed from the Options option:

- Update Passwords (RME) Page, page A-62
- Sync Privileges Page, page A-65
- Import Device Roles Page, page A-66

Update Passwords (RME) Page

Use this page to update device passwords from the Resource Manager Essentials (RME) inventory.

To open this page, Select **Devices > Options**.

Table A-62 Update Passwords (RME) Page

Field	Description
Host Location field	Enter the RME server DNS name or IP address.
Port field	Enter the RME server port number.
User Name field	Enter the username with which to log into the RME server.
Password field	Enter the password for the RME username.
Device group list box	Lists the device groups on the system. Select a device group from the list to filter the table to include only devices in that device group.
Check box column	Select a check box to select its row.
Sys Name column	Displays the system name, which is obtained from the SysName MIB variable. Click a name to display that device's properties.
Primary Device Name column	Displays the device IP address or DNS name entered to identify the device when it was added to the inventory.
Model column	Displays the device model. See the section Adding Devices to the Device Inventory, page 4-3 for information about unsupported models.
OS column	Displays the device operating system (OS) version.

Table A-62 Update Passwords (RME) Page (continued)

Field	Description
Mapped OS column	Displays the OS version that QPM has mapped to the device. See the section Adding Devices to the Device Inventory, page 4-3 for information about mapped OS versions.

Table A-62 Update Passwords (RME) Page (continued)

Field	Description
Status column	Displays the device status. The following statuses indicate that the device is working properly: • OK • Virtual—The device is a virtual device. The following statuses indicate a problem with the device. You cannot deploy to devices with these statuses: • Unreachable—The QPM server cannot establish basic network connectivity to the device. • SNMP Error—The device has an SNMP error that is preventing QPM from gathering the data it needs to work with the device. These are the common causes: – The device public community string entered in QPM is incorrect. – QPM can't read all of the necessary SNMP information from the device, possibly because there are corrupted or missing MIBs. – The device does not have a functioning SNMP engine. – The SNMP request timed out, typically because the device or network was too congested to respond before the timeout limit. The possible resolutions are to increase the SNMP timeout value and to increase the number of SNMP retries. • Telnet Error—QPM cannot connect to the device using Telnet. These are the common causes: – The device Telnet password entered in QPM is incorrect. Correct the Telnet password in QPM. – SSH is enabled but SSH login failed because SSH is not configured correctly on the device. Fix the SSH configuration on the device. – The login to the device failed. – There is no Telnet connection to the device.

Table A-62 Update Passwords (RME) Page (continued)

Field	Description
Update Passwords button	Click to update the passwords of the selected devices from RME.

Related Topics

- Updating Device Access Parameters from RME, page 4-23

Sync Privileges Page

Use this page to synchronize the QPM device group configuration with the ACS or CFM device group configuration.

To open this page, select **Devices > Options**. The Update Passwords page appears. Then select **Sync Device Groups (ACS)** from the TOC.

Table A-63 Sync Privileges Page

Field	Description
Server mode field	Displays which server type is being used to administer user permissions and device groups, either ACS or CiscoWorks.
Privilege Summary table	Displays the permissions you have to the QPM device groups. The possible permissions you can have are View, Modify, and Deploy. A check mark indicates that you have that permission, while a dash indicates that you do not.
Sync button	Click to synchronize the QPM inventory device group configuration with the ACS or CFM device group configuration.

Related Topics

- Synchronizing Permissions and Device Group Information, page 4-36

Import Device Roles Page

A device role is a device property that specifies the network point for a device in the AVVID network.

Use this page to import device roles from a file.

To open this page, select **Devices > Options**. The Update Passwords page appears. Then select **Import Device Roles** from the TOC.

Table A-64 Import Device Roles Page

Field	Description
File field	Enter the path on the client system to the file containing voice roles to import.
Browse button	Click to browse to the file instead of typing it in the File field.
Import button	Click to import voice roles.

Related Topics

- Importing Device Roles, page 4-23

Configure Tab Reference

The following topics describe the pages in the Configure tab. Topics are organized according to the following Configure tab options:

Deployment Groups

The following topics describe the fields in the pages that are accessed from the Deployment Groups option:

Deployment Groups Page

Deployment groups contain policy groups and associated information required to deploy policies to devices.

Open this page to:

- View a list of the deployment groups in a device group.
- Create a new deployment group.
- Edit the name and description of a deployment group.
- Copy a deployment group.
- Delete deployment groups.

To open this page, select **Configure > Deployment Groups**.

Table B-1 Deployment Groups Page

Field	Description
Name	Displays the names of the deployment groups. Click a deployment group's name to open the Deployment Group page to change its name and description.
Description	Displays deployment group descriptions.
Policy Groups	Click the icon for a deployment group to display the Policy Groups page for that deployment group.
Create button	Click to create a new deployment group. The Deployment Group page appears.
Edit button	Click to edit the selected deployment group's name and description. The Deployment Group page appears.
Copy button	Click to make a copy of the selected deployment group. The Copy Deployment Group dialog box opens. See Copy Deployment Group Dialog Box, page B-4 for details.
Delete button	Click to delete the selected deployment groups and all their policy groups.

Related Topics

- Deployment Group Page, page B-3

- Policy Groups Page, page B-14
- Chapter 8, "Working with Deployment Groups"
- Using QPM Tables, page 3-8

Deployment Group Page

Open this page to:

- Change the name and description of an existing deployment group.
- Define a new deployment group.

To open this page, do any of the following in the Deployment Groups page:

- Click the name of a deployment group.
- Select a deployment group, and click **Edit**.
- Click **Create**.

Table B-2 Deployment Group Page

Field	Description
Name	The deployment group name.
Description	A description of the deployment group.

Related Topics

- Deployment Groups Page, page B-2
- Creating a New Deployment Group, page 8-4
- Renaming a Deployment Group, page 8-6

Copy Deployment Group Dialog Box

Open this dialog box to make a copy of a deployment group. The new deployment group is given the default name "Copy of <*source deployment group*>," which you can change to a more meaningful name.

To open the Copy Deployment Group dialog box, in the Deployment Groups page, select a deployment group and click **Copy**.

Table B-3 Copy Deployment Group Dialog Box

Field	Description
Device Group	Select the name of the target device group, to which you want to copy.
Copy with network element assignments	Select this check box to copy the network element assignments of the policy groups in the source deployment group to the policy groups in the new deployment group. This option is available only when you copy within the same device group.

Related Topics

- Deployment Groups Page, page B-2
- Copying a Deployment Group, page 8-5

Libraries

The following topics describe the fields in the pages that are accessed from the Libraries option:

- IP Aliases Page, page B-5
- IP Alias Dialog Box, page B-5
- Applications Page, page B-6
- Application Alias Dialog Box, page B-7
- Policy Group Templates Page, page B-8
- Attached Policy Groups Page, page B-10

IP Aliases Page

An IP alias is an alias for a named group of IP addresses (including masks) or hostnames. It can be used for both source IP and destination IP conditions within a filter.

Open this page to view, edit, and create IP aliases in the IP Aliases library.

To open the IP Aliases page, select **Configure > Libraries**, or select **IP Aliases** in the Libraries navigation TOC.

Table B-4 IP Aliases Page

Field	Description
Name	Displays the names of the IP aliases in the IP Aliases library. Click a name to open the IP Alias dialog box for viewing or editing. See IP Alias Dialog Box, page B-5 for details.
Values	Displays the hostnames and IP addresses in the alias.
Create button	Click to create a new IP alias. The IP Alias dialog box opens. See IP Alias Dialog Box, page B-5 for details.
Edit button	Click to edit a selected IP alias. The IP Alias dialog box opens. See IP Alias Dialog Box, page B-5 for details.
Delete button	Click to delete selected IP aliases.

Related Topics

- Policy Wizard: Rule Setting Page, page B-73
- Defining IP Aliases, page 6-38

IP Alias Dialog Box

Open this dialog box to create or change an IP alias.

To open the IP Alias dialog box, do any of the following in the IP Aliases page:

- Click an IP alias name.
- Select an IP alias and click the Edit button.
- Click the Create button.

Table B-5 IP Alias Dialog Box

Field	Description
Name	The name of the IP alias.
Network Host	• Select IP to specify the IP address and mask of the network host. Enter the IP address and mask. • Select Host to specify the host name. Enter the host name. The Mask field will be disabled.
Add button	Click to add the IP definition to the IP alias definition.
Remove button	Click to remove the selected IP definition from the current IP alias definition.
IP list	Displays the IP addresses in the current IP alias definition.

Related Topics

- IP Aliases Page, page B-5

Applications Page

An application alias is an alias for a defined protocol and port (or range of ports). It can be used in a filter definition for source and destination protocol conditions.

Open this page to view, edit and create application aliases in the Application Aliases library.

To open the Application Aliases page, select **Configure > Libraries**, then select **Application Aliases** in the Libraries navigation TOC.

Table B-6 Application Aliases Page

Field	Description
Name	Displays the names of the application aliases in the Application Aliases library. Click a name to open the Application Alias dialog box for viewing or editing. See Application Alias Dialog Box, page B-7 for details.
Protocol	Displays the application protocol defined in the alias.

Table B-6 Application Aliases Page (continued)

Field	Description
Ports	Displays the port or group of ports defined in the alias.
Create button	Click to create a new application alias. The Application Alias dialog box opens. See Application Alias Dialog Box, page B-7 for details.
Edit button	Click to edit a selected application alias. The Application Alias dialog box opens. See Application Alias Dialog Box, page B-7 for details.
Delete button	Click to delete selected application aliases.

Related Topics

- Policy Wizard: Rule Setting Page, page B-73
- Defining Application Aliases, page 6-39

Application Alias Dialog Box

Open this dialog box to create or change an application alias.

To open the Application Alias dialog box, do any of the following in the Application Aliases page:

- Click an application alias name.
- Select an application alias and click the Edit button.
- Click the Create button.

Table B-7 Application Alias Dialog Box

Field	Description
Name	The name of the application alias.

Table B-7 Application Alias Dialog Box (continued)

Field	Description
Protocol	Define the protocol in one of the following ways: • Enter the number or name of the protocol used by the packets. Valid protocol numbers are 0 through 255. Valid names appear in the Protocol list. • Click the Protocol button, and select a protocol from the Protocol list.
TCP/UDP port or range	For TCP or UDP protocols, enter the TCP or UDP port number or range of ports that the application uses.

Related Topics

- Applications Page, page B-6

Policy Group Templates Page

Policy group templates contain QoS policies and properties.

Open this page to:

- View a list of the policy group templates in the library
- Create a new policy group template
- Edit the properties or policies of a policy group template
- Delete policy group templates

To open this page, select **Configure > Libraries,** then select Policy Group Templates in the Libraries TOC.

Table B-8 Policy Group Templates Page

Field	Description
Name	Displays the names of policy group templates in the Templates library. Click a template name to open the General page for that template.
Description	Displays the policy group template descriptions.

Table B-8 Policy Group Templates Page (continued)

Field	Description
Voice Role	Displays the voice role for voice policy group templates. The voice role specifies the role of an interface in the IP telephony network, according to its type, function, and location on the network.
QoS Properties	This column displays the number of QoS properties. Click the number to open the QoS Properties page for the corresponding policy group template.
In Policies	This column displays the number of policies for inbound traffic. Click the number to open the In Policies page for the corresponding policy group template.
Out Policies	This column displays the number of policies for outbound traffic. Click the number to open the Out Policies page for the corresponding policy group template.
Attached Policy Groups	This column displays the number of policy groups attached to the template. Click to open the Attached Policy Groups page for the corresponding policy group template.
Create button	Click to create a new policy group template. The Policy Group Template Definition wizard opens.
Edit button	Click to edit the selected template. The Policy Group Template General page appears.
Delete button	Click to delete the selected policy group templates. The selected templates will be deleted with all their content.

Related Topics

- General Page (Policy Group and Template), page B-17
- QoS Properties Page, page B-20
- In Policies/Out Policies Page, page B-32
- Attached Policy Groups Page, page B-10
- Template Definition Wizard, page B-11
- Using QPM Tables, page 3-8

Attached Policy Groups Page

Open this page to:

- View a list of the policy groups that are attached to a policy group template.
- Disconnect policy groups from a policy group template. (You can also do this from the Policy Groups - General page.)

To open this page, click the number in the Attached Policy Groups column in the Policy Group Templates page.

Table B-9 Attached Policy Groups Page

Field	Description
Name	Displays the names of the policy groups attached to the template.
Deployment Group	Displays the names of the deployment groups to which the attached policy groups belong. Click the deployment group name to display the Policy Groups page for that deployment group.
Description	Displays the descriptions of the policy groups.
Assigned Network Elements	Displays the types of network elements assigned to the policy groups. Click a network element type to display the Assigned Network Elements page for the policy group.
Disconnect button	Click to disconnect the selected policy groups from the policy group template.

Related Topics

- General Page (Policy Group and Template), page B-17
- Policy Groups Page, page B-14
- Assigned Network Elements Page, page B-35
- Using QPM Tables, page 3-8

Template Definition Wizard

The Template Definition wizard guides you through the steps required to create a new policy group template, and define or edit its device constraints.

To create a new policy group template, open the Template Definition wizard in any of the following ways:

- Click **Create** in the Templates page.
- In the Template General page, click **Edit**.

The Policy Group Template Definition wizard contains the following pages:

- Template Definition Wizard: General Definition Page, page B-11
- Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43
- Manual Constraint Definition Page, page B-45
- Constraint Definition from Inventory Page, page B-47
- Policy Group Definition Wizard: Capabilities Report Page, page B-49

Related Topics

- Policy Group Templates Page, page B-8
- General Page (Policy Group and Template), page B-17
- Using QPM Wizards, page 3-10

Template Definition Wizard: General Definition Page

Use this page to create a new policy group template, or to edit the general definition of a policy group template.

To open this page, do any of the following:

- Click **Create** in the Templates page.
- In the Template General page, click **Edit**.

To open this page in the wizard, select **General Definition** in the wizard navigation TOC.

Table B-10 Template Definition Wizard - General Definition Page

Field	Description
Template Name	The name of the policy group template.
Template Description	The description of the policy group template.
Advanced	This field is collapsed by default. Click the triangle to expand the field. The options in this field offer alternative ways of defining the policy group template: • Continue with the wizard—This is the default and defines the device constraints using the wizard. • Copy from Policy Group Template—Copies a template's device constraints, QoS properties and policies. – Select a template from the list box. Click **View** to display the template details in a separate browser window. • Copy from Policy group—Copies a policy group's device constraints, and optionally, its properties and policies. – Select the source device group in the Device Group list box. – Select the source deployment group in the Deployment Group list box. – Select the policy group to copy in the Policy Group list box. Click **View** to display the policy group in a separate browser window. – Select **Copy policies and properties** to copy the source policy group's policies and properties.
Next button	Click to proceed to the next step. If you chose Continue with wizard, the Constraints Definition page appears. Otherwise the Capabilities Report page appears.
Finish button	Click to complete the wizard. The QoS Properties page appears.

Related Topics

- Policy Group Templates Page, page B-8
- General Page (Policy Group and Template), page B-17

- Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43
- Policy Group Definition Wizard: Capabilities Report Page, page B-49

Policy Groups

The following topics describe the fields in the pages that are accessed from the Policy Groups option:

- Policy Groups Page, page B-14
- Copy Policy Group Dialog Box, page B-17
- General Page (Policy Group and Template), page B-17
- Device Constraints Page, page B-19
- QoS Properties Page, page B-20
- NBAR Port Mappings Page, page B-22
- NBAR Port Mapping Dialog Box, page B-23
- DSCP to CoS Mappings Page, page B-24
- DSCP to CoS Mapping Dialog Box, page B-25
- CoS to DSCP Mappings Page, page B-25
- CoS to DSCP Mapping Dialog Box, page B-26
- IP Precedence to DSCP Mappings Page, page B-27
- IP Precedence to DSCP Mapping Dialog Box, page B-28
- DSCP to Markdown Mappings Page, page B-28
- DSCP to Markdown Mapping Dialog Box, page B-30
- Excess Markdown Mappings Page, page B-30
- Excess Markdown Mapping Dialog Box, page B-31
- In Policies/Out Policies Page, page B-32
- Policy Summary Page, page B-34
- Reorder Policies Dialog Box, page B-35
- Assigned Network Elements Page, page B-35

- Add Assignment Dialog Box, page B-38
- Policy Group Definition Wizard, page B-40
- QoS Properties Definition Wizard, page B-50
- Policy Wizard, page B-70
- Policy Translation Page, page B-91
- Upload QoS Configuration Page, page B-92

Policy Groups Page

Policy groups contain QoS policies and the assigned network elements to which the policies will be applied.

Open this page to:

- View a list of the policy groups in a deployment group.
- Create a new policy group.
- Edit the properties or policies of a policy group.
- Edit network assignments for policy groups.
- Copy a policy group.
- Delete policy groups.

To open this page, do any of the following:

- Select **Configure > Policy Groups**. The Policy Groups page displays the policy groups for the last opened deployment group.
- Select **Configure > Deployment Groups**, then click the Policy Groups icon for the required deployment group.
- Select **Policy Groups** in the Policy Groups TOC, which appears after you have used one of the previous options to open this page.

Table B-11 Policy Groups Page

Field	Description
Deployment Group	Displays the current deployment group. To work with policy groups in a different deployment group, select the required deployment group.

Table B-11 Policy Groups Page (continued)

Field	Description
Name	Displays the names of policy groups in the current deployment group. Click a policy group name to open the General page for that policy group.
Description	Displays the policy group descriptions.
Policy Group Template	Displays the policy group template name, if the policy group is linked to a template. Click the template name to display the General page for the policy group template.
Voice Role	If the policy group is not attached to a template, this column displays the voice role for voice policy groups. The voice role specifies the role of an interface in the IP telephony network, according to its type, function and location on the network. If the policy group is attached to a policy group template, this column displays “inherited.”
QoS Properties	If the policy group is not attached to a template, this column displays the number of QoS properties. Click the number to open the QoS Properties page for the corresponding policy group. If the policy group is attached to a policy group template, this column displays “inherited.”
In Policies	If the policy group is not attached to a template, this column displays the number of policies in policy groups for inbound traffic. Click the number to open the In Policies page for the corresponding policy group. If the policy group is attached to a policy group template, this column displays “inherited.”
Out Policies	If the policy group is not attached to a template, this column displays the number of policies in policy groups for outbound traffic. Click the number to open the Out Policies page for the corresponding policy group. If the policy group is attached to a policy group template, this column displays “inherited.”

Table B-11 Policy Groups Page (continued)

Field	Description
Network Elements	Displays the number and type of network elements that are assigned to each policy group. Click the network element type to display the Assigned Network Elements page for the corresponding policy group.
Create button	Click to create a new policy group in the current deployment group. The Policy Group Definition wizard opens.
Edit button	Click to edit the selected policy group. The Policy Group general information page appears.
Copy button	Click to make a copy of a selected policy group. The Copy Policy Group dialog box opens. See Copy Policy Group Dialog Box, page B-17 for details.
Delete button	Click to delete the selected policy groups. The selected policy groups will be deleted with all their content.

Related Topics

- General Page (Policy Group and Template), page B-17
- QoS Properties Page, page B-20
- In Policies/Out Policies Page, page B-32
- Assigned Network Elements Page, page B-35
- Policy Group Definition Wizard, page B-40
- Working with Policy Groups, page 6-2
- More Information on Policy Configuration, page 6-50
- Using QPM Tables, page 3-8

Copy Policy Group Dialog Box

Open this dialog box to make a copy of a policy group. The new policy group is given the default name "Copy of <*policy group*>," which you can change to a more meaningful name.

To open the Copy Policy Group dialog box, in the Policy Groups page, select a policy group, and click **Copy**.

Table B-12 Copy Policy Group Dialog Box

Field	Description
Device Group	Select the name of the target device group, to which you want to copy.
Deployment Group	Select the name of the target deployment group, to which you want to copy.
Copy with policies and properties	Select this check box to copy the source policy group with its policies and properties.
Copy with network element assignments	Select this check box to copy the source policy group with its network element assignments. This option is available only when you copy to a different deployment group within the same device group.

Related Topics

- Policy Groups Page, page B-14
- Copying Policy Groups, page 6-15

General Page (Policy Group and Template)

Open this page to:

- View and edit the general definitions of a policy group or policy group template.
- Disconnect a policy group from its linked policy group template.
- Access other policy group or template pages.

To open the page, do any of the following:

- In the Policy Groups page, click a policy group name, or select a policy group and click **Edit**.
- In the Policy Group Templates page, click a template name, or select a template and click **Edit**.
- Select **General** in the Policy Group or Template TOC.

Note This TOC appears only after you have opened a policy group or template page.

Table B-13 General Page (Policy Group and Template)

Field	Description
Name	Displays the policy group or policy group template name.
Description	Displays the policy group or policy group template description.
Total policies and properties	Displays the total number of policies and properties in the policy group or policy group template.
Assigned to	Displays the number and type of network elements to which the policy group is assigned. (This field does not appear for a policy group template.)
Attached to template	Displays the name of the policy group template to which the policy group is attached. (This field does not appear for a policy group template.) If the policy group is attached to a template, a Disconnect button is displayed. Click **Disconnect** to disconnect the policy group from the template.
Voice Role	Displays the voice role for a voice policy group. The voice role specifies the role of an interface in the IP telephony network, according to its type, function, and location on the network. This field appears only for a voice policy group or voice policy group template.

Table B-13 General Page (Policy Group and Template) (continued)

Field	Description
Edit button	Click to edit the general definitions of the policy group or template. The Policy Group Definition wizard opens. **Note** For policy groups that are attached to a policy group template, you can edit only the policy group name and definition. **Note** For voice policy groups, if you modify the device constraints, the policy group will lose its voice role.

Related Topics

- Policy Groups Page, page B-14
- Policy Group Templates Page, page B-8
- Policy Group Definition Wizard, page B-40
- Viewing Policy Group Information, page 6-18
- Modifying a Policy Group, page 6-19

Device Constraints Page

Use this page to view and edit device constraint definitions for a policy group or policy group template.

To open this page, select **Device Constraints** in the Policy Group or Template TOC.

Note This TOC appears only after you have opened a policy group or policy group template.

Table B-14 Device Constraints Page

Field	Description
Constraint No.	Serial number of the device constraint definition.

Table B-14 Device Constraints Page (continued)

Field	Description
Model	The device model number.
OS Version	The version of the operating system software running on the device.
Compatible IOSs	The IOS versions that have compatible QoS capabilities with the specified OS version.
Interface Type	The type of interface, for example, Ethernet.
Card Type	(Interfaces, VCs, and DLCIs only) The type of card on which the interface or switch port resides.
Network Element	The type of network element, for example, device, or interface.
Capabilities Report button	Click to view a summary of the device constraint capabilities in a separate browser window.
Edit button	Click to edit the policy group constraint definitions. The Constraint Definitions page of the Policy Group Definition wizard appears.

Related Topics

- Policy Groups Page, page B-14
- Policy Group Templates Page, page B-8
- Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43
- Policy Group Definition Wizard: Capabilities Report Page, page B-49
- Viewing Policy Group Information, page 6-18

QoS Properties Page

Open this page to:

- View and edit QoS Property and mapping definitions for a policy group.
- View and edit QoS Property and mapping definitions for a policy group template.

To open this page, do any of the following:

- Click the number in the Properties column in the Policy Groups or Templates page.
- Select **Properties** in the Policy Group or Template TOC.

Note This TOC appears only after you have opened a policy group or template page.

Table B-15 QoS Properties Page

Field	Description
QoS Properties	Displays the defined QoS properties, and the QoS properties that can be configured for the policy group or policy group template. This field is displayed only when there are configurable QoS properties.
Edit button	Click to edit or add QoS properties. The QoS Properties wizard opens. The Edit button is disabled for policy groups that are attached to a policy group template.
Mappings	Displays the QoS mappings that can be defined for the policy group or policy group template: • Not configured—Mappings have not been defined in QPM. Assigned network elements will use the mappings that are currently configured on the device. • User defined—Mappings have been defined in QPM, and will be configured on the network elements on deployment.
Edit button (for each type of mapping)	Click to change the mapping settings for the policy group or template. The corresponding Mappings page appears.

Related Topics

- Policy Groups Page, page B-14
- Policy Group Templates Page, page B-8
- QoS Properties Definition Wizard, page B-50

- NBAR Port Mappings Page, page B-22
- DSCP to CoS Mappings Page, page B-24
- CoS to DSCP Mappings Page, page B-25
- IP Precedence to DSCP Mappings Page, page B-27
- DSCP to Markdown Mappings Page, page B-28
- Excess Markdown Mappings Page, page B-30
- Viewing Policy Group Information, page 6-18
- Defining QoS Properties and Mappings, page 6-8

NBAR Port Mappings Page

Network Based Application Recognition (NBAR) is a classification engine that recognizes a wide variety of applications, including web-based and other difficult-to-classify protocols that utilize dynamic TCP/UDP port assignments. NBAR classification uses protocol names that refer to their well-known port number.

Open this page to view, add, or edit NBAR port mappings for a policy group or template.

To open the NBAR Port Mappings page, in the QoS Properties page, click **Edit** in the NBAR Port Mappings field.

Table B-16 NBAR Port Mappings Page

Field	Description
Name	The NBAR application name.
Protocol	The protocol name: TCP or UDP.
Ports	The ports to which the application is mapped.
Create button	Click to add a new NBAR port mapping. The NBAR Port Mapping dialog box opens. See NBAR Port Mapping Dialog Box, page B-23 for details.
Edit button	Click to edit the properties of the selected NBAR mapping. The NBAR Port Mapping dialog box opens. See NBAR Port Mapping Dialog Box, page B-23 for details.

Table B-16 NBAR Port Mappings Page (continued)

Field	Description
Reset button	Click to delete all existing NBAR port mappings. The NBAR port mappings configuration is now "Not configured."
Delete button	Click to delete the selected NBAR mapping.

Related Topics

- QoS Properties Page, page B-20
- Defining QoS Properties and Mappings, page 6-8

NBAR Port Mapping Dialog Box

Open this dialog box to map port numbers to NBAR protocols for a policy group or template.

To open the NBAR Port Mapping dialog box, click **Add**, or **Edit** in the NBAR Port Mappings page.

Table B-17 NBAR Port Mapping Dialog Box

Field	Description
NBAR Protocol	The application protocol.
TCP/UDP	The application's layer 4 protocol name: TCP or UDP.
Ports	The ports to which the application is mapped. Enter port numbers separated by a space or comma.

Related Topics

- NBAR Port Mappings Page, page B-22
- QoS Properties Page, page B-20

DSCP to CoS Mappings Page

Open this page to view, or edit the DSCP to CoS mapping values.

To open the DSCP to CoS Mappings page, in the QoS Properties page, click **Edit** in the DSCP to CoS Mappings field.

Table B-18 DSCP to CoS Mappings Page

Field	Description
DSCP	Lists the 64 DSCP values each of which can be mapped to one of eight CoS values.
CoS	Displays the mapped CoS values for each DSCP value. If there is no mapping configured ("Not configured" is displayed in the QoS Properties page), default values are displayed. To configure the default values, click the Save Defaults button.
Edit button	Click to edit the mapping of the selected DSCP value. The DSCP to CoS Mapping dialog box opens. See DSCP to CoS Mapping Dialog Box, page B-25 for more details.
Reset button	Click to delete the entire mapping configuration. The default mapping values are displayed. To configure the default mapping values, click **Save Defaults**.
Delete button	Click to delete the entire mapping configuration. The QoS Properties page appears displaying "Not configured" for this mapping. This button is disabled if the mapping is not configured.
Save Defaults button	Click to save the displayed default settings. This button is enabled when the default settings are displayed.
Done button	Click to return to the QoS Properties page.

Related Topics

- QoS Properties Page, page B-20
- Defining QoS Properties and Mappings, page 6-8

DSCP to CoS Mapping Dialog Box

Open this dialog box to edit a DSCP mapping.

To open the DSCP to CoS Mappings dialog box, in the DSCP to CoS Mappings page, select a DSCP value, and click **Edit**.

Table B-19 DSCP to CoS Mapping Dialog Box

Field	Description
DSCP	Displays the selected DSCP value to be mapped.
CoS	Enter the CoS value to which you want the DSCP value to be mapped.

Related Topics

- QoS Properties Page, page B-20
- DSCP to CoS Mappings Page, page B-24
- Defining QoS Properties and Mappings, page 6-8

CoS to DSCP Mappings Page

Open this page to view or edit the CoS to DSCP mapping values.

To open the CoS to DSCP Mappings page, in the QoS Properties page, click **Edit** in the CoS to DSCP Mappings field.

Table B-20 CoS to DSCP Mappings Page

Field	Description
CoS	Lists the eight CoS values, each of which can be mapped to one of the 64 DSCP values.
DSCP	Displays the mapped DSCP values for each CoS value. If there is no mapping configured ("Not configured" is displayed in the QoS Properties page), default values are displayed. To configure the default values, click the Save Defaults button.

Table B-20 CoS to DSCP Mappings Page (continued)

Field	Description
Edit button	Click to edit the mapping of the selected CoS value. The CoS to DSCP Mapping dialog box opens. See CoS to DSCP Mapping Dialog Box, page B-26 for details.
Reset button	Click to delete the entire mapping configuration. The default mapping values are displayed. To configure the default mapping values, click **Save Defaults**.
Delete button	Click to delete the entire mapping configuration. The QoS Properties page appears displaying "Not configured" for this mapping. This button is disabled if the mapping is not configured.
Save Defaults button	Click to save the displayed default settings. This button is enabled when the default settings are displayed.
Done button	Click to return to the QoS Properties page.

Related Topics

- QoS Properties Page, page B-20
- Defining QoS Properties and Mappings, page 6-8

CoS to DSCP Mapping Dialog Box

Open this dialog box to edit a CoS mapping.

To open the CoS to DSCP Mappings dialog box, in the CoS to DSCP Mappings page, select a CoS value, and click **Edit**.

Table B-21 CoS to DSCP Mapping Dialog Box

Field	Description
CoS	Displays the selected CoS value to be mapped.
DSCP	Enter the DSCP value to which you want the CoS value to be mapped.

Related Topics

- QoS Properties Page, page B-20
- CoS to DSCP Mappings Page, page B-25
- Defining QoS Properties and Mappings, page 6-8

IP Precedence to DSCP Mappings Page

Open this page to view, or edit the IP Precedence to DSCP mapping values.

To open the IP Precedence to DSCP Mappings page, in the QoS Properties page, click **Edit** in the IP Precedence to DSCP Mappings field.

Table B-22 IP Precedence to DSCP Mappings Page

Field	Description
IP Precedence	Lists the eight IP Precedence values each of which can be mapped to one of the 64 DSCP values.
DSCP	Displays the mapped DSCP values for each IP precedence value. If there is no mapping configured ("Not configured" is displayed in the QoS Properties page), default values are displayed. To configure the default values, click the Save Defaults button.
Edit button	Click to edit the mapping of the selected IP Precedence value. The IP Precedence to DSCP Mapping dialog box opens. See IP Precedence to DSCP Mapping Dialog Box, page B-28 for details.
Reset button	Click to delete the entire mapping configuration. The default mapping values are displayed. To configure the default mapping values, click **Save Defaults**.
Delete button	Click to delete the entire mapping configuration. The QoS Properties page appears displaying "Not configured" for this mapping. This button is disabled if the mapping is not configured.
Save Defaults button	Click to save the displayed default settings. This button is enabled when the default settings are displayed.
Done button	Click to return to the QoS Properties page.

Related Topics

- QoS Properties Page, page B-20
- Defining QoS Properties and Mappings, page 6-8

IP Precedence to DSCP Mapping Dialog Box

Open this dialog box to edit a IP Precedence mapping.

To open the IP Precedence to DSCP Mappings dialog box, in the IP Precedence to DSCP Mappings page, select a IP Precedence value, and click **Edit**.

Table B-23 IP Precedence to DSCP Mapping Dialog Box

Field	Description
IP Precedence	Displays the selected IP Precedence value to be mapped.
DSCP	Enter the DSCP value to which you want the IP Precedence value to be mapped.

Related Topics

- QoS Properties Page, page B-20
- IP Precedence to DSCP Mappings Page, page B-27
- Defining QoS Properties and Mappings, page 6-8

DSCP to Markdown Mappings Page

Open this page to view, or edit the DSCP to Markdown mapping values. These values are used by QPM to reduce the DSCP priority of specific packets when you deploy a policing policy in which markdown is the selected exceed action for out-of-profile packets.

To open the DSCP to Markdown page, in the QoS Properties page, click **Edit** in the DSCP to Markdown field.

Table B-24 DSCP to Markdown Page

Field	Description
DSCP	Lists the 64 DSCP values each of which can be marked down.
Markdown	Displays the markdown values for each DSCP value. If there is no mapping configured ("Not configured" is displayed in the QoS Properties page), default values are displayed. To configure the default values, click the Save Defaults button.
Edit button	Click to edit the mapping of the selected DSCP value. The DSCP to Markdown dialog box opens. See DSCP to Markdown Mapping Dialog Box, page B-30 for details.
Reset button	Click to delete the entire mapping configuration. The default mapping values are displayed. To configure the default mapping values, click **Save Defaults**.
Delete button	Click to delete the entire mapping configuration. The QoS Properties page appears displaying "Not configured" for this mapping. This button is disabled if the mapping is not configured.
Save Defaults button	Click to save the displayed default settings. This button is enabled when the default settings are displayed.
Done button	Click to return to the QoS Properties page.

Related Topics

- QoS Properties Page, page B-20
- Defining QoS Properties and Mappings, page 6-8

DSCP to Markdown Mapping Dialog Box

Open this dialog box to edit a DSCP markdown value used by QPM when marking down DSCP values.

To open the DSCP to Markdown dialog box, in the DSCP to Markdown page, select a DSCP value, and click **Edit**.

Table B-25 DSCP to CoS Mapping Dialog Box

Field	Description
DSCP	Displays the selected DSCP value to be marked down.
Markdown	Enter the Markdown value to which you want the DSCP value to be mapped.

Related Topics

- QoS Properties Page, page B-20
- DSCP to Markdown Mappings Page, page B-28
- Defining QoS Properties and Mappings, page 6-8

Excess Markdown Mappings Page

Open this page to view, or edit the DSCP to Markdown mapping values. These values are used by QPM to reduce the DSCP priority of specific packets when you deploy a policing policy in which excess markdown is the selected violate action for out-of-profile packets.

To open the Excess Markdown Mappings page, in the QoS Properties page, click **Edit** in the Excess Markdown field.

Table B-26 Excess Markdown Mappings Page

Field	Description
DSCP	Lists the 64 DSCP values each of which can be marked down.

Table B-26 Excess Markdown Mappings Page (continued)

Field	Description
Excess Markdown	Displays the excess markdown values for each DSCP value. If there is no mapping configured ("Not configured" is displayed in the QoS Properties page), default values are displayed. To configure the default values, click the Save Defaults button.
Edit button	Click to edit the mapping of the selected DSCP value. The DSCP to Excess Markdown dialog box opens. See Excess Markdown Mapping Dialog Box, page B-31 for details.
Reset button	Click to delete the entire mapping configuration. The default mapping values are displayed. To configure the default mapping values, click **Save Defaults**.
Delete button	Click to delete the entire mapping configuration. The QoS Properties page appears displaying "Not configured" for this mapping. This button is disabled if the mapping is not configured.
Save Defaults button	Click to save the displayed default settings. This button is enabled when the default settings are displayed.
Done button	Click to return to the QoS Properties page.

Related Topics

- QoS Properties Page, page B-20
- Defining QoS Properties and Mappings, page 6-8

Excess Markdown Mapping Dialog Box

Open this dialog box to edit an excess markdown value used by QPM.

To open the Excess Markdown dialog box, in the Excess Markdown page, select a DSCP value, and click **Edit**.

Table B-27 Excess Markdown Mapping Dialog Box

Field	Description
DSCP	Displays the selected DSCP value to be marked down.

Table B-27 Excess Markdown Mapping Dialog Box (continued)

Field	Description
Markdown	Enter the Excess Markdown value to which you want the DSCP value to be mapped.

Related Topics

- QoS Properties Page, page B-20
- Excess Markdown Mappings Page, page B-30
- Defining QoS Properties and Mappings, page 6-8

In Policies/Out Policies Page

Open these pages to:

- View and edit policies in a policy group or policy group template.
- Create new policies.
- Enable or disable policies.
- Change the order of policies within a policy group or policy group template.
- Delete policies in a policy group or policy group template.

To open the In Policies page, do any of the following:

- Click the number in the In Policies column in the Policy Groups or Templates page.
- Select **In Policies** in the Policy Group or Template TOC.

To open the Out Policies page, do any of the following:

- Click the number in the Out Policies column in the Policy Groups or Templates page.
- Select **Out Policies** in the Policy Group or Template TOC.

Note This TOC appears only after you have opened a policy group or template page.

Table B-28 In Policies/Out Policies Page

Field	Description
Policy Order	The order of the policy within the policy group or template. Policies are checked in the order they appear in the list. When a policy filter matches the traffic flow, the policy actions are applied.
Enable	Enabled policies are distributed to network elements on deployment, and are indicated by a checkmark. Disabled policies are indicated by a minus sign (-).
Policy Name	Displays the name of each policy in the policy group or template. Click a policy name to view a summary of that policy.
Filter	Displays the policy's filter details.
Action	Displays the policy's action details.
Create button	Click to create a new policy. The Policy wizard opens. This button is disabled for: • Policy groups defined for interfaces on a VLAN, and the QoS style is VLAN-based. (When you want to define VLAN-based policies, you must create an additional policy group for a VLAN, and define the policies in this policy group.) • Any policy group for which you cannot configure policies in the specified direction. • Policy groups that are attached to a policy group template.
Disable button	Click to disable selected enabled policies.
Enable button	Click to enable selected disabled policies.
Reorder button	Click to change the order of the policies in the policy group or template. The Reorder Policies dialog box opens. See Reorder Policies Dialog Box, page B-35 for details.
Edit button	Click to edit a selected policy. The Policy wizard opens.
Delete button	Click to delete the selected policies.

Related Topics

- Policy Groups Page, page B-14
- Policy Group Templates Page, page B-8

- Policy Summary Page, page B-34
- Policy Wizard, page B-70
- Working with Policies, page 6-24
- Using QPM Tables, page 3-8

Policy Summary Page

Open this page to display a summary of a policy.

To open the Policy Summary page, click on a policy name in the In Policies or Out Policies page.

Table B-29 Policy Summary Page

Field	Description
Name	Displays the name of the policy.
Description	Displays the policy description.
Type	Displays the type of policy—QoS policy, or Access control policy.
Status	Displays the status of the policy—Enabled, or Disabled.
Direction	Displays the direction of the policy—In, or Out.
Filter	Displays a summary of the policy's filter definition.
Policy actions	Displays a summary of the policy's actions.
Edit button	Click to edit the policy. The Policy wizard opens.

Related Topics

- In Policies/Out Policies Page, page B-32
- Policy Wizard, page B-70
- Working with Policies, page 6-24

Reorder Policies Dialog Box

Open this dialog box to change the order of policies in a policy group or template.

To open the Reorder Policies dialog box, in the In Policies or Out Policies page, click **Reorder**.

Table B-30 Reorder Policies Dialog Box

Field	Description
Available policies	Lists the current policies. Select a policy and click the Up or Down button to change its priority in the list.

Related Topics

- In Policies/Out Policies Page, page B-32
- Changing the Priority of Policies, page 6-36

Assigned Network Elements Page

Use this page to view and edit the network element assignments for the current policy group.

To open this page, do any of the following:

- Click the entry in the Network Elements column in the Policy Groups page, or the Attached Policy Groups page.
- Select **Assigned Network Elements** in the Policy Group TOC.

Note This TOC appears only after you have opened a policy group page.

The fields that appear in the Assigned Network Elements page depend on the type of assigned device or network element. Table B-31 describes all the available fields.

Table B-31 Assigned Network Elements Page

Field	Description
Sys Name	Displays the system name of the assigned devices, or of the devices to which the assigned network element belongs. This column does not appear for source-destination pairs.
Name	Displays the names of the assigned network elements.
Device Folder	Displays the name of the device folder to which the device belongs, if relevant.
Fields for assigned devices only	
Primary Device Name	Displays the main IP addresses or hostnames of the assigned devices.
Model	Displays the device models.
OS Version	Displays the versions of the operating system on the devices.
Mapped OS Version	Displays the OS versions that QPM uses to determine QoS capabilities that can be configured.
Status	Displays the status of the devices.
Fields for assigned interfaces and VLANs only	
Type	Displays the types of interface.
Rate	Displays the interface rates.
Fields for assigned interfaces only	
Card type	Displays the types of card on which the interface resides: • VIP • 1P2Q2T • 2Q2T • NA—This refers to other cards that do not affect the QoS capabilities of the policy group.
Description	Displays the descriptions of the assigned interfaces.

Table B-31 Assigned Network Elements Page (continued)

Field	Description
Fields for assigned VLANs only	
Status	Displays the status of the assigned VLANs—operational, or suspended.
IP	Displays the IP address of the VLAN.
Fields for assigned VCs and DLCIs only	
Interface Name	Displays the names of the interfaces to which the VCs or DLCIs belong.
Fields for assigned source-destination pairs only	
Pair name	Displays the names of the source-destination pairs.
Source interface	Displays the source interfaces of the source-destination pairs.
Target interface	Displays the target interfaces of the source-destination pairs.
Action buttons	
Add button	Click to assign a network element to the policy group. The Add Assignment dialog box opens. See Add Assignment Dialog Box, page B-38 for details.
Remove button	Click to remove the assignment of the selected network elements.

Related Topics

- Policy Groups Page, page B-14
- Setting Network Element Assignments, page 6-13
- Using QPM Tables, page 3-8

Add Assignment Dialog Box

Open this dialog box to assign network elements to a policy group.

To open the Add Assignment dialog box, in the Assigned Network Elements page, click **Add**.

Table B-32 Add Assignment Dialog Box

Field	Description
Sys Name	Displays the system names of devices. This column does not appear for source-destination pairs.
Name	Displays the names of network elements.
Policy Groups	Displays the names of the policy groups to which the network elements are assigned.
Device Folder	Displays the name of the device folder to which the device belongs, if relevant.
Fields for devices only	
Primary Device Name	Displays the main IP addresses or hostnames of the devices.
Model	Displays the device models.
OS Version	Displays the versions of the operating system on the devices.
Mapped OS Version	Displays the OS versions that QPM uses to determine QoS capabilities that can be configured.
Status	Displays the status of the devices.
Fields for interfaces and VLANs only	
Type	Displays the types of interface.
Rate	Displays the interface rates.

Table B-32 Add Assignment Dialog Box (continued)

Field	Description
Fields for interfaces only	
Card type	Displays the types of card on which the interface resides: • VIP • 1P2Q2T • 2Q2T • NA—This refers to other cards that do not affect the QoS capabilities of the policy group.
Description	Displays the descriptions of the interfaces.
Fields for VLANs only	
Status	Displays the status of VLANs—operational, or suspended.
IP	Displays the IP address of the VLAN.
Fields for assigned VCs and DLCIs only	
Interface Name	Displays the names of the interfaces to which the VCs or DLCIs belong.
Fields for source-destination pairs only	
Pair name	Displays the names of the source-destination pairs.
Source interface	Displays the source interfaces of the source-destination pairs.
Target interface	Displays the target interfaces of the source-destination pairs.
Action buttons	
Assign button	Click to assign a network element to the policy group.

Related Topics

- Policy Groups Page, page B-14
- Assigned Network Elements Page, page B-35
- Setting Network Element Assignments, page 6-13
- Using QPM Tables, page 3-8

Policy Group Definition Wizard

The Policy Group Definition wizard guides you through the steps required to create a new policy group, and define or edit its device constraints.

To create a new policy group, open the Policy Group Definition wizard in any of the following ways:

- Click **Create** in the Policy Groups page.
- In the Policy Group General page, click **Edit**.

The Policy Group Definition wizard contains the following pages:

- Policy Group Definition Wizard: General Definition Page, page B-40
- Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43
- Manual Constraint Definition Page, page B-45
- Constraint Definition from Inventory Page, page B-47
- Policy Group Definition Wizard: Capabilities Report Page, page B-49

Related Topics

- Policy Groups Page, page B-14
- Policy Group Templates Page, page B-8
- General Page (Policy Group and Template), page B-17
- More Information on Policy Configuration, page 6-50
- Using QPM Wizards, page 3-10

Policy Group Definition Wizard: General Definition Page

Use this page to create a new policy group, or to edit the general definition of a policy group.

To open this page, do any of the following:

- Click **Create** in the Policy Groups page.
- In the Policy Group General page, click **Edit**.

To open this page in the wizard, select **General Definition** in the wizard navigation TOC.

Table B-33 Policy Group Definition Wizard - General Definition Page

Field	Description
Policy Group Name	The name of the policy group.
Policy Group Description	The description of the policy group.

Table B-33 Policy Group Definition Wizard - General Definition Page (continued)

Field	Description
Advanced	This field appears only when creating a policy group, and is collapsed by default. Click the triangle to expand the field. The options in this field offer alternative ways of defining the policy group or template: • Continue with the wizard—This is the default and defines the device constraints using the wizard. • Attach Policy Group Template —Uses a template to define the policy group's device constraints, QoS properties and policies. The template remains attached until disconnected, and any changes to the template affect the policy group. – Select a template from the list box. Click **View** to display the template details in a separate browser window. • Copy from Policy Group Template—Copies a template's device constraints, QoS properties, and policies. The template is not attached, and any changes to it do not affect the new policy group or template. – Select a template from the list box. Click **View** to display the template details in a separate browser window. • Copy from Policy group—Copies a policy group's device constraints, and optionally, its properties and policies. – Select the source device group in the Device Group list box. – Select the source deployment group in the Deployment Group list box. – Select the policy group to copy in the Policy Group list box. Click **View** to display the policy group in a separate browser window. – Select **Copy policies and properties** to copy the source policy group's policies and properties. – Select **Copy network element assignment** to copy the source policy group's network element assignment. This field appears only if you are copying to a different deployment group in the same device group.

Table B-33 Policy Group Definition Wizard - General Definition Page (continued)

Field	Description
Next button	Click to proceed to the next step. If you chose Continue with wizard, the Constraints Definition page appears. Otherwise the QoS Properties page appears.
Finish button	Click to complete the wizard. The QoS Properties page appears.

Related Topics

- Policy Groups Page, page B-14
- Policy Group Templates Page, page B-8
- General Page (Policy Group and Template), page B-17
- Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43
- Policy Group Definition Wizard: Capabilities Report Page, page B-49
- Creating a Policy Group, page 6-5
- Modifying a Policy Group, page 6-19
- More Information on Policy Configuration, page 6-50

Policy Group/Template Definition Wizard: Constraint Definitions Page

Use this page to define device constraints for a policy group or policy group template. The device constraint definitions determine the available QoS capabilities for the policy group or template.

To open this page, do any of the following:

- In the Policy Group/Template Wizard—General Definition page, click **Next**.
- In the Policy Group/Template Wizard navigation menu, select **Constraints Definition**.

Note If you are creating a policy group by attaching a template, this page does not open.

- In the Policy Group Device Constraints page or Template Device Constraints page, click **Edit**.

Table B-34 Policy Group/Template Definition Wizard - Constraint Definitions Page

Field	Description
Constraint No.	Serial number of the device constraint definition.
Model	The device model number.
OS Version	The version of the device operating system software.
Compatible IOSs	The IOS versions that have compatible QoS capabilities with the specified OS version.
Interface Type	The type of interface.
Card Type	The type of card on which the interface or switch port resides.
Network Element	The type of network element, for example, device, or interface.
Define Manually button	Click this button to create a new device constraint definition manually. The Manual Constraint Definition page appears.
Define from Inventory button	Click this button to create a new device constraint definition from a set of selected network elements. The Define from Inventory page appears.
Edit button	Click to edit the selected constraint definition. You cannot edit the network element type. If you want to change the network element type, you must create a new policy group.
Delete button	Click to delete the selected constraint definition. A policy group must contain at least one constraint definition. You cannot delete a constraint definition if it is the only constraint definition for the policy group.
Back button	Click to return to the previous step in the wizard.
Next button	Click to proceed to the next step. The Capabilities Report page appears.
Finish button	Click to complete the wizard. The QoS Properties page appears.

Related Topics

- Policy Group Definition Wizard: General Definition Page, page B-40
- Device Constraints Page, page B-19
- Manual Constraint Definition Page, page B-45
- Define from Inventory Page, page B-46
- Policy Group Definition Wizard: Capabilities Report Page, page B-49
- Creating a Policy Group, page 6-5
- Modifying a Policy Group, page 6-19

Manual Constraint Definition Page

Use this page to create a device constraint definition manually.

To open this page, click **Define Manually** in the Policy Group Definition Wizard—Constraint Definitions page.

Note The fields in this page change according to each selection you make.

Table B-35 Manual Constraint Definition Page

Field	Description
Model	Select the device model.
OS version	Select the version of the operating system software running on the device.
Network element type	Select the type of network element, for example, device or interface. After you create the first constraint in a policy group, you cannot change the network element type. All constraints in a policy group must be for the same network element type. If you want to change the network element type, you must create a new policy group.
Interface type	Select the type of interface, for example, Ethernet.

Table B-35 Manual Constraint Definition Page (continued)

Field	Description
Card type	Select the type of card on which the interface or switch port resides: • VIP • 1P2Q2T • 2Q2T • NA—This refers to other cards that do not affect the QoS capabilities of the policy group.

Related Topics

- Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43
- Define from Inventory Page, page B-46
- Policy Group Definition Wizard: Capabilities Report Page, page B-49
- Creating a Policy Group, page 6-5
- Modifying a Policy Group, page 6-19

Define from Inventory Page

Use this page to select the type of network element you want to use to create a device constraint.

To open this page, click **Define from Inventory** in the Policy Group Definition Wizard: Constraint Definitions page.

Table B-36 Define from Inventory Page

Field	Description
Model	Select the device model.
Network element type	Select the type of network element, for example, device or interface. After you create the first constraint in a policy group, you cannot change the network element type. All constraints in a policy group must be for the same network element type. If you want to change the network element type, you must create a new policy group.

Related Topics

- Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43
- Constraint Definition from Inventory Page, page B-47
- Manual Constraint Definition Page, page B-45
- Policy Group Definition Wizard: Capabilities Report Page, page B-49
- Creating a Policy Group, page 6-5
- Modifying a Policy Group, page 6-19

Constraint Definition from Inventory Page

Use this page to create a device constraint definition from a set of selected devices.

To open this page, click **OK** in the Policy Group Definition Wizard—Define from Inventory page.

Table B-37 Constraint Definition from Inventory Page

Field	Description
Sys Name	Displays the system names of devices.
Name	Displays the names of network elements.
Fields for devices only	
Primary Device Name	Displays the main IP addresses or hostnames of the devices.
Model	Displays the device models.
OS Version	Displays the versions of the operating system on the devices.
Mapped OS Version	Displays the OS versions that QPM uses to determine QoS capabilities that can be configured.
Status	Displays the status of the devices.
Fields for interfaces and VLANs only	
Type	Displays the types of interface.
Rate	Displays the interface rates.

Table B-37 Constraint Definition from Inventory Page (continued)

Field	Description
Fields for interfaces only	
Card type	Displays the types of card on which the interface resides: • VIP • 1P2Q2T • 2Q2T • NA—This refers to other cards that do not affect the QoS capabilities of the policy group.
Description	Displays the descriptions of the interfaces.
Fields for VLANs only	
Status	Displays the status of VLANs—operational, or suspended.
IP	Displays the IP address of the VLAN.
Fields for assigned VCs and DLCIs only	
Interface Name	Displays the names of the interfaces to which the VCs or DLCIs belong.
Fields for source-destination pairs only	
Pair name	Displays the names of the source-destination pairs.
Source interface	Displays the source interfaces of the source-destination pairs.
Target interface	Displays the target interfaces of the source-destination pairs.
Action buttons	
Define Constraint button	Click to create a constraint definition from the selected network elements.

Related Topics

- Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43
- Define from Inventory Page, page B-46
- Manual Constraint Definition Page, page B-45
- Policy Group Definition Wizard: Capabilities Report Page, page B-49

- Creating a Policy Group, page 6-5
- Modifying a Policy Group, page 6-19

Policy Group Definition Wizard: Capabilities Report Page

Use this page to review the QoS capabilities available for the policy group or template, and for each device constraint.

To open this page, in the Policy Group Definition Wizard, select Capabilities Report in the wizard navigation TOC.

Table B-38 Capabilities Report

Field	Description
Capability	Lists all available QoS capabilities.
Capabilities Summary	Displays the summary of QoS capabilities for the policy group or template. These are the common capabilities for all device constraints.
Device Constraint columns	Each column displays the QoS capabilities available for a single device constraint definition.
Back button	Click to return to the previous step in the wizard.
Finish button	Click to complete the wizard. The Policy Groups QoS Properties page appears.

Related Topics

- Policy Group Definition Wizard: General Definition Page, page B-40
- Policy Group/Template Definition Wizard: Constraint Definitions Page, page B-43
- QoS Properties Page, page B-20

QoS Properties Definition Wizard

The QoS Properties Definition wizard guides you through the steps required to add and edit QoS properties for a policy group or template.

To open the QoS Properties Definition wizard for a policy group or template, in the QoS Properties page, click **Edit** in the Properties table.

The QoS Properties wizard contains the following pages:

- QoS Properties Wizard: Congestion Management Page, page B-51
- QoS Properties Wizard: Shaping Settings Page, page B-59
- QoS Properties Wizard: Traffic Control Settings Page, page B-61
- QoS Properties Wizard: Congestion Avoidance Page, page B-66
- QoS Properties Wizard: Summary Page, page B-69

Note Some wizard pages might be disabled, according to the device constraint definitions for the policy group or template.

Related Topics

- QoS Properties Page, page B-20
- Using QPM Wizards, page 3-10

QoS Properties Wizard: Congestion Management Page

Use the Congestion Management page to define the type of scheduling, and the scheduling parameters for a policy group or template.

To open the Congestion Management page in the QoS Properties Definition wizard, select **Congestion Management** in the wizard navigation TOC.

Table B-39 Congestion Management Page

Field	Description
Select a scheduling method	Select a scheduling method for the policy group or template. Select Default scheduling to use the default scheduling method on the device. Additional fields might appear according to the scheduling method you choose.
Packet size (optional)	(CQ only) The typical packet size, in bytes, that traverses the interface. QPM uses this value to calculate the byte size of the custom queues, the queues being a multiple of this packet size.
Queue limits (optional)	(PQ only) The limit for the number of packets allowed in each priority queue. After the limit is reached, packets are dropped.
Configure the distributed Weighted Fair Queuing properties (optional)	(dWFQ only) • Aggregate Limit—The limit for the total number of packets allowed in all queues. • Individual Limit—The limit for the number of packets allowed in each individual queue.
Configure the Fair Queuing properties (optional)	(FQ only) • Aggregate Limit—The limit for the total number of packets allowed in all queues. • Individual Limit—The limit for the number of packets allowed in each individual queue.

Table B-39 Congestion Management Page (continued)

Field	Description
Configure the WFQ properties (optional)	(WFQ only, and only when the device constraints are defined for frame relay interfaces) Enable FRTS—Select to enable FRTS. The following options are displayed: • Discard Threshold—The number of messages allowed in a weighted fair queue. For high-bandwidth conversations, once this threshold is met, additional high-bandwidth messages are discarded. The threshold can be from 1 to 4096. • Dynamic Conversation—The number of dynamic queues to use for conversations that do not require special network services ("best-effort conversations"). The dynamic conversation can be 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096. • Reservable Conversation—The number of reservable queues used for RSVP reserved conversations. The reservable conversation can be from 0 to 100, unless you configure a fragment size for FRTS voice configuration, in which case the value can be from 2 to 100. • Max Buffer Size [MAX.]—The maximum buffer size for the weighted fair queues, in number of messages. The buffer size can be from 0 to 4096.

Table B-39 Congestion Management Page (continued)

Field	Description
Configure the transmit 1P2Q2T/2Q2T queues	(1P2Q2T/2Q2T only) These properties configure the transmit queues used for outbound traffic based on the IP precedence setting in the packets. • Queue Length—The percentage of the port's bandwidth allocated to each queue. The minimum queue percentage is 1. The values for the queues must add up to 100%. Although all characteristics of these queues have default values, you must configure all values to change any value. • Weight—The relative weight for the queue. This weight is used to determine how much traffic is transmitted from the queue using the weighted round-robin (WRR) technique before servicing the next queue. The weight is from 1 to 255. The higher the weight, the more traffic is transmitted from the queue before servicing the next queue. For 1P2Q2T, Queue 3 does not have an associated weight because it is a strict priority queue that transmits traffic whenever it is detected.
Configure the transmit 1P2Q2T/2Q2T queues (continued)	• Threshold1—The percentage of the queue's bandwidth to use as the first threshold limit. In the mapping table, you assign traffic to this limit. Any assigned traffic that exceeds the limit is dropped. Queue 3 does not have a threshold because it is a strict priority queue. Traffic is only dropped when this queue's buffer is 100% full. Threshold 1 and 2 are not exclusive: they do not have to add up to 100. • Threshold 2—The percentage of the queue's bandwidth to use as the second threshold limit. In the mapping table, you assign traffic to this limit. Any assigned traffic that exceeds the limit is dropped. Queue 3 does not have a threshold because it is a strict priority queue. Traffic is only dropped when this queue's buffer is 100% full. Threshold 2 is typically larger than threshold 1. The difference between threshold 2 and 1 is the amount of the queue's bandwidth that is exclusively reserved for threshold 2 traffic. For example, if threshold 2 is 100% and threshold 1 is 40%, 60% of the queue's bandwidth can be used only by traffic assigned to threshold 2.

Table B-39 Congestion Management Page (continued)

Field	Description
Mappings button	(1P2Q2T/2Q2T only) Click to open the Mappings page to define the queues to which packets are assigned based on their marking.
CoS Mapping	(2Q1T queuing only) Each pair of CoS values is associated with either queue 1 or queue 2. For each pair of CoS values, select the queue to which packets with those CoS values will be directed.
Configure the weights of the 4 queues	(4Q1T queuing only) Enter the weights for the WRR scheduling.
Map the packets to one of the 4 queues, based on the COS value of the packet	(4Q1T queuing only) Maps packets to queues, based on their CoS value: • CoS Value—The CoS value to be mapped. • Queues—Select the queue to which the CoS value is mapped.
Configure the transmit 4Q2T queues	(4Q2T only) These properties configure the transmit queues used for outbound traffic based on the IP precedence setting in the packets. • Queue Length—The percentage of the port's bandwidth allocated to each queue. The values for the queues must add up to 100%. Although all characteristics of these queues have default values, you must configure all values to change any value. • Weight—The relative weight for the queue. This weight is used to determine how much traffic is transmitted from the queue using the weighted round-robin (WRR) technique before servicing the next queue. The higher the weight, the more traffic is transmitted from the queue before servicing the next queue. When Queue 4 is defined as a strict priority queue, it does not have an associated weight, because it transmits traffic whenever it is detected. • Threshold—The percentage of the queue's bandwidth to use as a threshold limit. In the mapping table, you assign traffic to this limit. Any assigned traffic that exceeds the limit is dropped. The default threshold is 100 percent for thresholds 1 and 2. • RED/Tail—Choose the Drop method for each queue.

Table B-39 Congestion Management Page (continued)

Field	Description
Is Priority	(4Q2T queuing only) Select this check box to configure Queue 4 as a strict priority queue, which will transmit traffic whenever it is detected.
Edit CoS Mappings button	(4Q2T queuing only) Click to open the CoS Mappings page to define the queues to which packets are assigned based on their CoS value.
Edit DSCP Mappings button	(4Q2T queuing only) Click to open the DSCP Mappings page to define the thresholds to which packets are assigned based on their DSCP value.
Configure the WRR queues	(WRR queuing only) These values configure the weights of the WRR queues used for an interface or pair of interfaces on layer 3 switches. The weight implies a bandwidth for the queue, although the queue is not given an explicit bandwidth. The higher the weight, the higher the implied bandwidth. You can calculate the implied bandwidth using this equation: $\frac{W}{S} \times B = n$ where: • W is the weight • S is the sum of the weight on all active queues on the port • B is the bandwidth for the port in Mbps • *n* is the bandwidth for the queue in Mbps For example, if the queue weight is 4, the sum of the queue weights is 15, and the bandwidth on the interface is 100 Mbps, then the bandwidth for the queue is 26 Mbps.
Back button	Click to return to the previous step in the wizard.
Next button	Click to proceed to the next step in the wizard.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- QoS Properties Page, page B-20
- QoS Properties Definition Wizard, page B-50
- QoS Properties Wizard: Shaping Settings Page, page B-59

- QoS Properties Wizard: Traffic Control Settings Page, page B-61
- QoS Properties Wizard: Congestion Avoidance Page, page B-66
- QoS Properties Wizard: Summary Page, page B-69

QoS Properties Wizard: 1P2Q2T/2Q2T Mappings Page

Use this page to view, add, and edit the assignment of packets to queues, based on their CoS value. All packets of a particular CoS value must be assigned to the same queue and threshold limit.

Table B-40 1P2Q2T / 2Q2T Mappings Page

Field	Description
CoS Value	The CoS value to be mapped.
Queue No.	Displays the queue to which the CoS value is mapped.
Threshold 1	Displays whether the CoS value is mapped to threshold 1.
Threshold 2	Displays whether the CoS value is mapped to threshold 2.
Create button	Click to create a new mapping. The 1P2Q2T Mapping dialog box appears. See 1P2Q2T/2Q2T Mapping Dialog Box, page B-57.
Edit button	Click to edit a selected mapping. The 1P2Q2T Mapping dialog box appears. See 1P2Q2T/2Q2T Mapping Dialog Box, page B-57.
Delete button	Click to delete selected mappings.
Done button	Click to return to the Congestion Management page.

Related Topics

- QoS Properties Wizard: Congestion Management Page, page B-51

1P2Q2T/2Q2T Mapping Dialog Box

Use this dialog box to create or change the assignment of packets to queues, based on their CoS value.

Table B-41 1P2Q2T / 2Q2T Mapping Dialog Box

Field	Description
Value	Select the CoS value to be mapped.
Queue No.	Select this radio button to assign the packets with the selected CoS value to either queue 1 or queue 2: • Select the queue to which you want to map the CoS value. • Select the threshold to which you want to map the CoS value.
Priority Queue	(1P2Q2T only) Select this radio button to assign the packets with the selected CoS value to the priority queue (queue 3). The priority queue does not have a threshold.

Related Topics

- QoS Properties Wizard: 1P2Q2T/2Q2T Mappings Page, page B-56

QoS Properties Wizard: 4Q2T CoS Mappings Page

Use this page to view and edit the assignment of packets to queues, based on their CoS value. All packets of a particular CoS value must be assigned to the same queue.

Table B-42 4Q2T CoS Mappings Page

Field	Description
CoS Value	The CoS value to be mapped.
Queues	Select the queue to which the CoS value is mapped.
Done button	Click to return to the Congestion Management page.

Related Topics

- QoS Properties Wizard: Congestion Management Page, page B-51

QoS Properties Wizard: 4Q2T DSCP Mappings Page

Use this page to view, add, and edit the assignment of packets to thresholds, based on their DSCP value. All packets of a particular DSCP value must be assigned to the same threshold.

Table B-43 4Q2T DSCP Mappings Page

Field	Description
DSCP	Displays all the DSCP values.
Threshold 1	Displays whether the DSCP value is mapped to threshold 1.
Threshold 2	Displays whether the DSCP value is mapped to threshold 2.
Edit button	Click to edit a selected mapping. The 4Q2T DSCP Mapping dialog box appears. See QoS Properties Wizard: 4Q2T DSCP Mapping Dialog Box, page B-58.
Reset button	Click to delete the entire mappings configuration.
Done button	Click to return to the Congestion Management page.

Related Topics

- QoS Properties Wizard: Congestion Management Page, page B-51

QoS Properties Wizard: 4Q2T DSCP Mapping Dialog Box

Use this dialog box to change the assignment of packets to thresholds, based on their DSCP value.

Table B-44 4Q2T DSCP Mapping Dialog Box

Field	Description
Value	Select the CoS value to be mapped.
Threshold	Select a radio button to assign the packets with the selected DSCP value to either threshold 1 or threshold 2.

Related Topics

- QoS Properties Wizard: 4Q2T DSCP Mappings Page, page B-58

QoS Properties Wizard: Shaping Settings Page

Use the Shaping Settings page to define shaping parameters for a policy group or template.

To open the Shaping Settings page in the QoS Properties Definition wizard, select **Shaping Settings** in the wizard navigation TOC.

Table B-45 Shaping Settings Page

Field	Description
Frame Relay Traffic Shaping Properties	• Enable FRTS—Select this to use the rate control features of Frame Relay traffic shaping (FRTS). **Note** To configure FRTS on subinterfaces and DLCIs, you must also enable FRTS on the parent interfaces, without configuring any FRTS properties. See Configuring FRTS Policies, page 6-56 for more information. • Rate—The committed information rate (CIR), which is typically the rate you are committed to provide on the circuit. Enter the average kilobits per second rate for the virtual circuit or interface. The default is 56. The rate should be less than or equal to the rate of the interface. • MinCIR—The minimum CIR (minCIR) value to be used when congestion occurs. The default minimum rate is half of the CIR. The actual bandwidth allocation during times of congestion is a percentage of the minimum rate, rather than a percentage of the CIR. • Burst Size—Optionally, the sustained number of kilobits that can be transmitted per interval over the virtual circuit. The burst size can be from 0.3 to 16000. The default is 7. The interval is determined by dividing the burst size by the rate. For example, if the rate is 128, and the burst size is 16, the interval is 0.125 seconds. • Exceed Burst Size—Optionally, the maximum number of kilobits in excess of the burst size that can be transmitted during the first interval when congestion occurs. The exceed burst size can be from 0 to 16000. The default is 7.

Table B-45 Shaping Settings Page (continued)

Field	Description
Modular Shaping Properties	• Enable Modular Shaping—Select to enable shaping on all traffic flows on the interface. • Shaping type—Choose the type of shaping action: – Average—The interface sends no more than the committed burst (Bc) for each interval. – Peak—The interface sends the committed burst (Bc) plus the excess burst (Be) in each interval. • Rate (kbit/sec or ratio%)—The target average rate for the traffic, in kilobits per second, or as a percentage. • Burst size (optional) KBits—The sustained number of kilobits that can be transmitted per interval over the interface. The interval is determined by dividing the burst size by the rate. • Exceed Burst size (optional) KBits—The maximum number of kilobits in excess of the burst size that can be transmitted during the first interval when congestion occurs.
Adaptive Shaping Properties	• Adaptive Shaping—Select this check box to have the interface reduce the traffic rate when it is notified that congestion is occurring at other interfaces along the path. • Rate—Specify the traffic rate to be used when the interface is notified about congestion. • Mark traffic with FECN—Select this check box to use the forward explicit congestion notification (FECN) to adjust the traffic descriptors, to approximate the rate to the available bandwidth along the path.
Back button	Click to return to the previous step in the wizard.
Next button	Click to proceed to the next step in the wizard.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- QoS Properties Page, page B-20
- QoS Properties Definition Wizard, page B-50

- QoS Properties Wizard: Congestion Management Page, page B-51
- QoS Properties Wizard: Traffic Control Settings Page, page B-61
- QoS Properties Wizard: Congestion Avoidance Page, page B-66
- QoS Properties Wizard: Summary Page, page B-69
- Configuring FRTS Policies, page 6-56

QoS Properties Wizard: Traffic Control Settings Page

Use the Traffic Control Settings page to define traffic control parameters for a policy group or template.

To open the Traffic Control Settings page in the QoS Properties Definition wizard, select **Traffic Control Settings** in the wizard navigation TOC.

Table B-46 Traffic Control Settings Page

Field	Description
Configure IP RTP Priority properties	IP RTP Priority is mainly useful on interfaces whose speed is less than 1.544 Mbps. Voice typically uses 24 Kbps. However, IP RTP Priority ignores voice compression, so a 12 Kbps stream is treated like a 24 Kbps stream. Because of overhead, ensure that the bandwidth percentage you select accommodates at least 25 Kbps per call. You can use the **max-reserved-bandwidth** IOS software command to change the maximum allocatable bandwidth. • Port Range—The starting and ending RTP port numbers. RTP traffic for these ports is placed in the strict-priority queue. Other traffic is handled by the interface's standard queuing mechanism. The start port can be 2000 or higher, and the end port can be 65536 or lower. The maximum range is 16383. There is no default port range, but the voice ports range is from 16384 to 32767. • Bandwidth—The percentage of the interface's bandwidth for the strict-priority queue. All packets in the queue are transmitted before any other queues are handled. To determine the bandwidth required, estimate the number of concurrent calls that must be supported on the interface, and multiply by 25 Kbps. Then divide by the interface's bandwidth to get the bandwidth percentage. Do not set the bandwidth too low. Any traffic for the queue that exceeds the bandwidth is dropped. Although voice traffic typically uses 24 kbps, there is occasional overhead requiring 25 kbps service. If you select a bandwidth percentage that equates to 24 kbps, the interface is likely to drop voice packets occasionally, which will give you poor voice quality. Any unused bandwidth is available to the other queues on the interface. The bandwidth can be between 0 and 75. There is no default. On interfaces configured with class-based QoS, this bandwidth is added to the combined queue bandwidths, and the total must be 75% or less.

Table B-46 Traffic Control Settings Page (continued)

Field	Description
IP RTP Header Compression Properties	• Enable IP RTP Header Compression—Select this to compress the IP/UDP/RTP header in an RTP data packet from 40 bytes to approximately two to five. This is typically used to help reduce delay for voice traffic. • Passive—Select this to compress outgoing RTP packets only if incoming RTP packets on the same interface are compressed. Leaving this check box clear when Enable IP RTP Header Compression is selected will compress all RTP headers.
Link Fragmentation and Interleaving properties	• Enable LFI—Select this check box to reduce delay on slower-speed links for delay-sensitive traffic. • Maximum delay—Enter the maximum fragmentation delay in milliseconds.
Voice configuration properties (FRF)	• Enable voice configuration—Select this check box to configure the bandwidth and fragmentation for Voice over Frame Relay. These settings help you ensure that real-time, delay-sensitive voice traffic can be carried over Frame Relay links. • Bandwidth—The percentage of the bandwidth configured for minCIR on the interface to reserve for voice traffic. • Fragment (optional)—The frame size, in bytes, used when fragmenting data frames, not including Frame Relay headers and fragmentation headers. Long data frames are fragmented and interleaved with real-time voice frames, so that data and voice can share the link while maintaining the required voice quality. Voice over Frame Relay frames are never fragmented. The fragment size is in bytes, and can be from 16 to 1600. The default is 53 bytes. Fragment is only available when you select WFQ or Class Based QoS for scheduling.

Table B-46 Traffic Control Settings Page (continued)

Field	Description
Configure Signaling Properties	• Enable RSVP—Select this to allow applications to make RSVP reservations on the interface. Some applications, such as VoIP, video, or audio broadcasts, use RSVP reservations to ensure that sufficient bandwidth is available at network devices along a traffic flow. This ensures that real-time traffic can flow through the network reliably, without delay and packet loss that can make the traffic flow useless. When defined on interfaces configured with class-based QoS, RSVP and class-based QoS work independently, as if the other technique were not configured on the interface. When configured on WFQ interfaces, RSVP provides guaranteed rate service, which is good for delay-sensitive applications like voice over IP. When configured on WRED interfaces, RSVP provides controlled load service, which is good for adaptive real-time applications like the playback of a recorded conference call. • UDP Encapsulation—Select this to have the interface produce a UDP-encapsulated multicast packet whenever it receives an IP-encapsulated multicast packet. If you do not select this field, the interface only uses UDP-encapsulated packets if it receives a UDP-encapsulated RSVP message (some hosts depend on the router to initiate UDP-encapsulation). The interface uses the 224.0.0.14 multicast address and UDP port 1699. – Individual Limit—The percentage of the interface's bandwidth that one traffic flow can reserve. The single flow limit can be from 1 to the aggregate limit. The default is 75. – Aggregate Limit—The percentage of the interface's bandwidth that all traffic flows combined can reserve. The aggregate limit can be from 1 to 75. The default is 75. **Note** You must understand the bandwidth requirements of the RSVP-enabled applications on your network to make reasonable bandwidth settings.

Table B-46 Traffic Control Settings Page (continued)

Field	Description
Set QoS style	• Enable QoS style—Select this to choose the type of QoS configuration, for ports or for VLANs. • VLAN-based—Select this when you want to configure VLAN-based policies on the ports. When you choose this option, do not define policies in this policy group. You must create an additional policy group for the VLAN, containing the policies for the VLAN. See Configuring VLAN Policies, page 6-58 for more information. • Port-based—Select this when you want to configure port-based policies.
Configure the Trust state properties	Enable Trust state—Select this to enable the trust state for the Catalyst switch port. The trust state affects how frames are marked when they enter the port. • Untrusted—Change the frame's class of service (CoS) and type of service (ToS) values to the ones defined for the port. This is the switch's default trust state. • Trust CoS—Trust the CoS value on the packet and use it to change the packet's ToS value. • Trust DSCP—Trust the packet's DSCP values without change. • Trust IP Precedence—Trust the IP precedence value in the ToS byte.
Configure the Trust-ext properties	Enable Trust-ext—Select to enable the trust extension settings for the Catalyst switch ports. These settings effectively extend the trust boundary of the switch to the IP phone and determine how packets at the trust extension boundary are marked. • Untrusted—Negate the existing CoS settings. This is useful for a VoIP network where you have a PC-IP phone-Cat6K setup. To ensure that data from the PC gets no priority, you can set the trust extension to untrusted and then change CoS value of VoIP traffic to 5 and data traffic to 0. This ensures highest priority for voice traffic. • Trust CoS—Trust the packet's existing CoS value.

Table B-46 Traffic Control Settings Page (continued)

Field	Description
Set TX Ring	Enable Tx Ring—Select to configure the size of the transmit rings (Tx-ring), which are buffer control structures for transmitting packets. The primary reason to adjust the transmit ring is to reduce latency caused by queuing. • Buffer Size—Enter the buffer size of the transmit ring. This value should be small enough to avoid introducing latency due to queuing, but large enough to avoid drops, and a resulting impact to TCP-based flows.
Set inline power	Enable Inline Power—Select this to implement inline power on power-enabled Ethernet line cards.
Back button	Click to return to the previous step in the wizard.
Next button	Click to proceed to the next step in the wizard.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- QoS Properties Page, page B-20
- QoS Properties Definition Wizard, page B-50
- QoS Properties Wizard: Congestion Management Page, page B-51
- QoS Properties Wizard: Shaping Settings Page, page B-59
- QoS Properties Wizard: Congestion Avoidance Page, page B-66
- QoS Properties Wizard: Summary Page, page B-69

QoS Properties Wizard: Congestion Avoidance Page

Use this page to define congestion avoidance properties for the policy group or template.

Table B-47 QoS Properties Wizard Congestion Avoidance Page

Field	Description
Enable WRED	Select the check box to enable WRED.

Table B-47 QoS Properties Wizard Congestion Avoidance Page (continued)

Field	Description
WRED Weight	Enter the factor used to determine the rate at which packets are dropped when traffic congestion occurs. The weight must be between 1 and 16.
Value	The IP precedence value in the packet, or RSVP if it is part of an RSVP flow.
Min. Threshold	The minimum number of packets held in the queue. When the average queue length falls between the minimum and maximum thresholds, packets are dropped based on the probability denominator. If the average queue size is lower than the minimum threshold, all packets are queued.
Max. Threshold	The maximum threshold for the queue. When the average queue length exceeds the maximum threshold, all new packets for the queue are dropped until the queue drops below the maximum threshold.
Probability Denominator	The denominator for the number of packets that are dropped if the queue length reaches the minimum threshold. The higher the denominator, the fewer packets are dropped from the queue.
Create button	Click to create a new WRED mapping. The Mapping Editing dialog box opens. See WRED Mapping Dialog Box, page B-68 for details.
Edit button	Click to edit the selected WRED mapping. The Mapping Editing dialog box opens. See WRED Mapping Dialog Box, page B-68 for details.
Delete button	Click to delete the selected WRED mapping.
Back button	Click to return to the previous step in the wizard.
Next button	Click to proceed to the next step in the wizard.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- QoS Properties Page, page B-20
- QoS Properties Definition Wizard, page B-50
- QoS Properties Wizard: Congestion Management Page, page B-51

- QoS Properties Wizard: Shaping Settings Page, page B-59
- QoS Properties Wizard: Traffic Control Settings Page, page B-61
- QoS Properties Wizard: Summary Page, page B-69

WRED Mapping Dialog Box

Use this dialog box to define WRED mappings for QoS properties and policies.

Table B-48 WRED Mapping Dialog Box

Field	Description
Value	Select the value for which you want to define threshold values—an IP precedence value, or RSVP. Precedence values that do not have settings are handled using default values.
Min. Threshold	The minimum number of packets held in the queue. When the average queue length falls between the minimum and maximum thresholds, packets are dropped based on the probability denominator. If the average queue size is lower than the minimum threshold, all packets are queued. The minimum threshold in QPM can be from 1 to 4096. The default minimum threshold for precedence 0 is half the maximum threshold. The default minimums for the remaining values fall at even intervals between this value and the max threshold. The average queue size is based on the current size of the queue, the last calculated average queue size, and the WRED weighting factor for the interface. See the IOS software documentation for the exact formula.
Max. Threshold	The maximum threshold for the queue. When the average queue length exceeds the maximum threshold, all new packets for the queue are dropped until the queue drops below the max threshold. The maximum threshold must be larger than the minimum threshold up to 4096. The default is based on the output buffer capacity of the device and the speed of the interface.

Table B-48 WRED Mapping Dialog Box (continued)

Field	Description
Probability Denominator	The denominator for the number of packets that are dropped if the queue length reaches the minimum threshold. The higher the denominator, the fewer packets are dropped from the queue. The probability denominator can be from 1 to 65536. The default is 10, that is, one packet in every 10 is dropped from a queue once the minimum threshold is reached. The higher you set the probability denominator, the higher the chance that the maximum threshold will be reached.

Related Topics

- QoS Properties Definition Wizard, page B-50
- QoS Properties Wizard: Congestion Avoidance Page, page B-66

QoS Properties Wizard: Summary Page

This page displays a summary of the QoS properties defined for the policy group or template.

To open the QoS Properties Summary page, click **Finish** in any of the wizard pages, or select Summary in the wizard TOC.

Table B-49 QoS Properties Summary Page

Field	Description
Properties Summary	Displays a summary of each of the configured QoS properties.
Back button	Click to return to the previous page in the wizard, if you want to make changes.
Finish button	Click to finish the QoS Properties wizard and return to the QoS Properties page.

Related Topics

- QoS Properties Page, page B-20
- QoS Properties Definition Wizard, page B-50

- QoS Properties Wizard: Congestion Management Page, page B-51
- QoS Properties Wizard: Shaping Settings Page, page B-59
- QoS Properties Wizard: Traffic Control Settings Page, page B-61
- QoS Properties Wizard: Congestion Avoidance Page, page B-66

Policy Wizard

The Policy wizard guides you through the steps required to define a QoS policy or access control policy. These steps include defining the policy filter and the policy actions.

To open the Policy wizard, do any of the following in the In Policies or Out Policies page:

- To add a new policy, click **Create**.
- To edit a selected policy, click **Edit**.

The Policy wizard contains the following pages:

- Policy Wizard: General Page, page B-71
- Policy Wizard: Filter Page, page B-72
- Policy Wizard: Rule Setting Page, page B-73
- Application Dialog Box, page B-74
- Protocol Dialog Box, page B-75
- Source IP / Destination IP Dialog Box, page B-77
- Service Dialog Box, page B-78
- CoS Dialog Box, page B-78
- MPLS Dialog Box, page B-79
- IP-RTP Port Range Dialog Box, page B-79
- Policy Wizard: Marking Actions Page, page B-80
- Policy Wizard: Microflow Policing Actions Page, page B-81
- Policy Wizard: Policing Actions Page, page B-83
- Policy Wizard: Shaping Actions Page, page B-86
- Policy Wizard: Queuing Actions Page, page B-87

- Policy Wizard: Congestion Avoidance Actions Page, page B-90
- Policy Wizard: Summary Page, page B-91

Policy Wizard: General Page

Use this page to create a new policy, or to edit the general definition of a policy.

To open this page, do any of the following:

- Click **Create** in the In Policies or Out Policies page.
- Select a policy in the In Policies or Out Policies page, and click **Edit**.
- Select **General** in the wizard navigation TOC.

Table B-50 Policy Wizard General Page

Field	Description
Policy Name	The name of the policy
Description	The description of the policy
Type of Policy	Select the type of policy you want to create: • QoS Policy—Contains a filter and actions. • Access Control Policy—Contains only a filter.
Next button	Click to proceed to the next step. The Filter page appears.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- In Policies/Out Policies Page, page B-32
- Policy Wizard: Filter Page, page B-72
- Policy Wizard: Summary Page, page B-91

Policy Wizard: Filter Page

Use this page to define a filter for the policy. The filter can contain one or more rules. Traffic must match any of the rules to satisfy the filter. Each rule consists of a set of conditions.

To open this page, select **Filter** in the wizard navigation TOC.

Table B-51 Policy Wizard Filter Page

Field	Description
Select how to define traffic type for policy	• Create a new filter—Select to define a new filter for the policy. • Class Default—Select to define a policy for all traffic that does not match any policy filter in the policy group. When you cannot define a class default policy, the New Filter check box is selected by default. When you cannot define a new filter, the Class Default check box is selected by default.
Filter name	Enter a name for the filter. This name is used for class-based policies when the filter conditions are translated into CLI commands.
Filter Rules table	Displays the rules defined for the filter.
Create button	Click to create a new rule for the filter. The Rule Setting page appears.
Edit button	Click to edit a selected rule. The Rule Setting page appears.
Delete button	Click to delete a selected rule.
Back button	Click to return to the previous step in the wizard.
Next button	Click to proceed to the next step in the wizard to define a policy action.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Policy Wizard: Rule Setting Page, page B-73
- Policy Wizard: Marking Actions Page, page B-80
- Policy Wizard: Summary Page, page B-91

Policy Wizard: Rule Setting Page

Use this page to define conditions for a filter rule. A flow must match all conditions in a rule to satisfy the filter. The conditions that you can defined depend on the device constraints defined for the policy group.

Table B-52 Policy Wizard Rule Setting Page

Field	Description
Does not match check box	Select this check box if the flow should not match all the specified conditions in the rule.
Deny check box	Select this check box to deny traffic that matches the conditions in the rule.
Application	Application that produces the traffic, identified by Network-based Application Recognition (NBAR). Click **Edit** to edit the NBAR properties used to define the filter condition. The Application dialog box opens. See Application Dialog Box, page B-74 for details. When you define a condition using NBAR, the Protocol condition is disabled.
Protocol	The traffic protocol. Click **Edit** to edit the protocol parameters. The Protocol dialog box opens. See Protocol Dialog Box, page B-75 for details. When you define a Protocol condition, the NBAR condition is disabled.
Source IP	The source address of the packet. Click **Edit** to edit the source IP parameters. The Source IP dialog box opens. See Source IP / Destination IP Dialog Box, page B-77 for details.
Destination IP	The destination address of the packet. Click **Edit** to edit the destination IP parameters. The Destination IP dialog box opens. See Source IP / Destination IP Dialog Box, page B-77 for details.
Service	The IP precedence or DSCP value of the packets. Click **Edit** to edit the service parameters. The Service dialog box opens. See Service Dialog Box, page B-78 for details.
CoS	The CoS value of the packets. Click **Edit** to edit the CoS parameters. The CoS dialog box opens. See CoS Dialog Box, page B-78 for details.

Table B-52 Policy Wizard Rule Setting Page (continued)

Field	Description
MPLS	The MPLS value of the packets. Click **Edit** to edit the MPLS parameters. The MPLS dialog box opens. See MPLS Dialog Box, page B-79 for details.
IP-RTP	The IP RTP ports used by the packets. Click **Edit** to edit the IP RTP port range. The IP-RTP Port Range dialog box opens. See IP-RTP Port Range Dialog Box, page B-79 for details.
Done button	Click this button when you have defined all conditions in the rule. The Filter page appears displaying the new rule.

Related Topics

- Policy Wizard: Filter Page, page B-72

Application Dialog Box

Use the Application dialog box to define or remove an NBAR condition in the current filter rule.

To open the Application dialog box, click **Edit** next to the Application filter condition in the Policy wizard Rule Setting page.

Table B-53 Application Dialog Box

Field	Description
NBAR Application	Select the NBAR protocol for filtering.
Edit the NBAR parameters	Parameter—Select a parameter for the selected protocol. Value—Enter a value for the selected parameter. Add button—Click to add the NBAR parameter to the NBAR condition. Remove button—Click to remove the selected NBAR parameter from the NBAR condition. Parameters list—Displays the NBAR parameters in the NBAR condition.
Delete button	Click to delete the NBAR condition from the current rule.

Related Topics

- Policy Wizard: Rule Setting Page, page B-73

Protocol Dialog Box

Use the Protocol dialog box to define or remove a protocol condition in the current filter rule. You can choose a protocol definition from the Applications library. For a complete list of protocols and their port numbers, see http://www.iana.org/assignments/port-numbers

To open the Protocol dialog box, click **Edit** next to the Protocol filter condition in the Policy wizard Rule Setting page.

Table B-54 Protocol Dialog Box

Field	Description
From Library	Select this radio button to define a protocol condition from the QPM Applications library. Choose a source and /or destination protocol from the QPM Applications library: • Source—Select the source protocol. • Destination—Select the destination protocol.

Table B-54 Protocol Dialog Box (continued)

Field	Description
Manually Defined	Select this radio button to define the protocol condition manually. • Protocol—Define the protocol in one of the following ways: – Enter the number or name of the protocol used by the packets. Valid protocol numbers are 0 through 255. Valid names appear in the Protocol list. – Click the Protocol button, and select a protocol from the Protocol list. • Source TCP/UDP port or range—Enter the TCP or UDP port number or range of ports from which the packets originate. – Save protocol and source ports in library—Select to save the protocol definition in the Applications library. – Application Alias Name—Enter a name for the application alias. • Destination TCP/UDP port or range—Enter the destination TCP or UDP port number or range of the packets. – Save protocol and destination ports in library—Select to save the protocol definition in the Applications library. – Application Alias Name—Enter a name for the application alias.
Delete button	Click to delete the current protocol definition from the filter rule.

Related Topics

- Policy Wizard: Rule Setting Page, page B-73

Source IP / Destination IP Dialog Box

Use the Source IP or Destination IP dialog box to define or remove an IP condition in the current filter rule. The IP condition can consist of one or more IP addresses. You can choose an IP definition from the IP aliases library.

To open the Source IP dialog box, click **Edit** next to the Source IP filter condition in the Policy wizard Rule Setting page.

To open the Destination IP dialog box, click **Edit** next to the Destination IP filter condition in the Policy wizard Rule Setting page.

Table B-55 Source IP / Destination IP Dialog Box

Field	Description
IP Address / Host name list	Select this radio button to define manually a set of IP addresses for the source or destination traffic: • IP/ host—The IP address or hostname of a network host: – Select the Host check box when you enter a host name. – Leave the Host check box empty when you enter an IP address. • Mask—The subnet mask for the specified IP address. • Add button—Click to add the IP definition to the IP list. • Remove button—Click to remove the selected IP definition from the IP list. • IP list—Displays the IP addresses in the current IP condition. • Save list in library—Select the check box to save the IP list in the IP aliases library. Enter the name of the alias in the IP Alias name field.
IP Alias	Select this radio button to use an IP alias from the IP aliases library: • Select an alias—Choose an IP alias from the library. • View button—Click to view details of the displayed IP alias.
Delete button	Click to delete the current IP condition from the filter rule.

Related Topics

- Policy Wizard: Rule Setting Page, page B-73

Service Dialog Box

Use the Service dialog box to define or remove a service condition in the current filter rule.

To open the Service dialog box, click **Edit** next to the Service filter condition in the Policy wizard Rule Setting page.

Table B-56 Service Dialog Box

Field	Description
Value	The IP precedence or DSCP value of the packets.
Delete button	Click to delete the current service condition in the filter rule.

Related Topics

- Policy Wizard: Rule Setting Page, page B-73

CoS Dialog Box

Use the CoS dialog box to define or remove a CoS condition in the current filter rule.

To open the CoS dialog box, click **Edit** next to the CoS filter condition in the Policy wizard Rule Setting page.

Table B-57 CoS Dialog Box

Field	Description
CoS	The CoS value of the packets.
Delete button	Click to delete the current CoS condition in the filter rule.

Related Topics

- Policy Wizard: Rule Setting Page, page B-73

MPLS Dialog Box

Use the MPLS dialog box to define or remove a MPLS condition in the current filter rule.

To open the MPLS dialog box, click **Edit** next to the MPLS filter condition in the Policy wizard Rule Setting page.

Table B-58 MPLS Dialog Box

Field	Description
MPLS	Select one or more MPLS values for the MPLS condition.
Delete button	Click to delete the current MPLS condition in the filter rule.

Related Topics

- Policy Wizard: Rule Setting Page, page B-73

IP-RTP Port Range Dialog Box

Use the IP-RTP Port Range dialog box to define or remove an IP-RTP Port Range condition in the current filter rule.

To open the IP-RTP Port Range dialog box, click **Edit** next to the IP-RTP Port Range filter condition in the Policy wizard Rule Setting page.

Table B-59 IP-RTP Port Range Dialog Box

Field	Description
Port Range	Enter the first and last port in the port range in the From and To fields.
Delete button	Click to delete the current IP-RTP Port Range condition in the filter rule.

Related Topics

- Policy Wizard: Rule Setting Page, page B-73

Policy Wizard: Marking Actions Page

Use this page to mark packets to define their relative importance.

To open this page, select **Actions > Marking** in the wizard navigation TOC.

Table B-60 Policy Wizard Marking Actions Page

Field	Description
Enable Marking	Select to enable marking actions. This check box will automatically be selected after you define settings in this page.
Select the packet marking	• Value—Specify the IP precedence or DSCP value to mark the matching packets. • Trust—Select how to trust the existing marking on matching packets: – trust-cos—Trust the existing CoS value – trust-ipprec—Trust the existing IP precedence value – trust-dscp—Trust the existing DSCP value **Note** The available trust options depend on the policy group constraints. • Mark Trust Ext—Select how to extend the trust on matching packets: – IP precedence values—Select an IP precedence value from 0 to 7. – Trust CoS—Trust the packet's existing CoS value. • CoS—Specify the CoS value to mark the matching packets.
Mark MPLS	The Multiprotocol Label Switching (MPLS) experimental value defines the priority for packets as they travel through the MPLS network. The MPLS experimental value does not overwrite the IP precedence value in the IP header. Select the MPLS value to mark the matching packets.

Table B-60 Policy Wizard Marking Actions Page (continued)

Field	Description
Frame relay DE-Bit	Select this check box to set the Discard Eligibility (DE) bit to 1. If congestion occurs in a frame relay network, frames with the DE bit set at 1 are discarded before frames with the DE bit set at 0. The default setting is 0.
Back button	Click to return to the previous step in the wizard.
Next button	Click to proceed to the next Actions page.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Policy Wizard: General Page, page B-71
- Policy Wizard: Filter Page, page B-72
- Policy Wizard: Microflow Policing Actions Page, page B-81

Policy Wizard: Microflow Policing Actions Page

Use this page to define policing actions on single traffic flows. You can limit and mark traffic that conforms to or exceeds specified rates.

To open this page, select **Actions > Microflow Policing** in the wizard navigation TOC.

Table B-61 Policy Wizard Microflow Policing Actions Page

Field	Description
Enable Microflow Policing	Select to enable policing actions on single flows. This check box will automatically be selected after you define settings in this page.
Rate	The target average rate for the traffic that the policy covers in kilobits per second. Enter the desired rate limit.

Table B-61 Policy Wizard Microflow Policing Actions Page (continued)

Field	Description
Burst size	The amount of kilobytes allowed to the traffic flow to accommodate bursty traffic. The minimum burst size is the rate divided by 2000. The recommended burst size is greater than the normal rate.
Conform action	Select one of the following actions for traffic flows that conform to the normal rate limit: • Transmit—Transmits the packet. • Drop—Drops the packet. • Mark and transmit—Marks the packet according to the specified IP precedence or DSCP value, and then transmits. – Mark with— Select the value to mark the packet. • Trust—Marks the packet according to the trust setting in the Trust Value field: – Trust Value—Select the trust value for the action.
Exceed action	Select one of the following actions for traffic flows that exceed the normal rate limit: • Transmit—Transmits the flow. • Drop—Drops the flow. • Mark and transmit—Marks the flow according to the specified IP precedence or DSCP value, and then transmits. – Mark with— Select the value to mark the flow. • Markdown—Reduces the marking value of the flow according to the markdown table definitions for the device.
Back button	Click to return to the previous step in the wizard.
Next button	Click to proceed to the next Actions page.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Policy Wizard: General Page, page B-71

- Policy Wizard: Filter Page, page B-72
- Policy Wizard: Policing Actions Page, page B-83

Policy Wizard: Policing Actions Page

Use this page to define policing actions on aggregate or cross-interface flows.

To open this page, select **Actions > Policing** in the wizard navigation TOC.

Table B-62 Policy Wizard Policing Actions Page

Field	Description
Type of policing	Select the type of policing: • Aggregate—Define rate limits and policing actions for aggregate flows on an interface. • Cross-interface—Define rate limits and policing actions for aggregate flows across several interfaces.
Enable Policing / Enable Cross aggregate Policing	Select to enable the selected type of policing actions on aggregate flows. This check box will automatically be selected after you define settings in this page.
Rate	The average rate for the traffic that the policy covers in kilobits per second.
Burst Size	The amount of kilobytes allowed to the traffic flow to accommodate bursty traffic. The minimum burst size is the rate divided by 2000. The recommended burst size is greater than the normal rate.
Exceed Burst	The amount of kilobytes allowed to the traffic flow to accommodate bursty traffic in excess of the normal burst size. The recommended exceed burst size is greater than the burst size.
Exceed Rate	(Two-rate policing only) The maximum rate for traffic that is in excess of the normal rate.

Table B-62 Policy Wizard Policing Actions Page (continued)

Field	Description
Conform action	Select one of the following actions for traffic flows that conform to the normal rate limit: • Transmit—Transmits the flow. • Drop—Drops the flow. • Mark and transmit—Marks the flow according to the specified IP precedence or DSCP value, and then transmits. – Mark with— Select the value to mark the flow. – Continue—Select to specify that subsequent policies should be examined after the policing policy is applied. Ensure that the policing policy appears before the subsequent policies in the policy group's policy table. • Trust—Marks the packet according to the trust setting in the Trust Value field: – Trust Value—Select the trust value for the action. • Markdown—Reduces the marking value of the traffic according to the markdown table definitions for the device.
Exceed action	Select one of the following actions for traffic flows that exceeds the normal rate limit: • Transmit—Transmits the flow. • Drop—Drops the flow. • Mark and transmit—Marks the flow according to the specified IP precedence or DSCP value, and then transmits. – Mark with—Select the value to mark the flow. – Continue—Select to specify that subsequent policies should be examined after the policing policy is applied. Ensure that the policing policy appears before the subsequent policies in the policy group's policy table. • Markdown—Reduces the marking value of the traffic according to the markdown table definitions for the device.

Table B-62 Policy Wizard Policing Actions Page (continued)

Field	Description
Violate Action	(Single-rate policing) The action to be performed for traffic that violates the normal and excess burst sizes. (Dual-rate policing) The action to be performed for traffic that exceeds the Excess Rate. • Transmit—Transmits the flow. • Drop—Drops the flow. • Mark and transmit—Marks the flow according to the specified IP precedence or DSCP value, and then transmits. – Mark with— Select the value to mark the flow. – Continue—Select to specify that subsequent policies should be examined after the policing policy is applied. Ensure that the policing policy appears before the subsequent policies in the policy group's policy table. • Markdown—Marks the flow according to the policy group's markdown table definitions. (If the Violate Action option is specified, the token bucket algorithm works with two token buckets, and the Excess rate must be specified.)
Back button	Click to return to the previous step in the wizard.
Next button	Click to proceed to the next Actions page.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Policy Wizard: General Page, page B-71
- Policy Wizard: Filter Page, page B-72
- Policy Wizard: Shaping Actions Page, page B-86

Policy Wizard: Shaping Actions Page

Use this page to smooth the rate of an outbound traffic flow.

To open this page, select **Actions > Shaping** in the wizard navigation TOC.

Table B-63 Policy Wizard Shaping Actions Page

Field	Description
Enable Shaping	Select to enable shaping actions in the policy. This check box will automatically be selected after you define settings in this page.
Shaping type	Choose the type of shaping action: • Peak—The interface sends the committed burst (Bc) plus the excess burst (Be) in each interval. • Average—The interface sends no more than the committed burst (Bc) for each interval.
Rate	The target average rate for the traffic that the policy covers, in kilobits per second.
Burst Size (optional)	The sustained number of kilobits that can be transmitted per interval over the interface. The interval is determined by dividing the burst size by the rate.
Excess Burst (optional)	The maximum number of kilobits in excess of the burst size that can be transmitted during the first interval when congestion occurs.
Adaptive Shaping	(Frame relay interfaces only) • Enable—Select this check box to have the interface reduce the traffic rate when it is notified that congestion is occurring at other interfaces along the path. • Rate—Specify the traffic rate to be used when the interface is notified about congestion. • Mark traffic with FECN—Select this check box to use the forward explicit congestion notification (FECN) to adjust the traffic descriptors, to approximate the rate to the available bandwidth along the path.
Back button	Click to return to the previous step in the wizard.

Table B-63 Policy Wizard Shaping Actions Page (continued)

Field	Description
Next button	Click to proceed to the next Actions page.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Policy Wizard: General Page, page B-71
- Policy Wizard: Filter Page, page B-72
- Policy Wizard: Queuing Actions Page, page B-87

Policy Wizard: Queuing Actions Page

Queuing actions manage congestion for outbound traffic. The queuing options differ according to the type of scheduling property chosen for the policy group.

To open this page, select **Actions > Queuing** in the wizard navigation TOC.

Table B-64 Policy Wizard Queuing Actions Page

Field	Description
Specify the priority of the traffic	(Class-based QoS) Enable Priority (LLQ)—Select this check box to create a strict priority queue, for example, for voice traffic. • Optional burst—Enter a burst value in bytes, if required.

Table B-64 Policy Wizard Queuing Actions Page (continued)

Field	Description
Specify bandwidth allocation	(Class-based QoS) Enable Bandwidth allocation—Select to define a queuing action. • Bandwidth—Enter the minimum guaranteed rate or percentage of the interface's bandwidth you want to allocate to the traffic in the Bandwidth field. Unless you change the maximum allocatable bandwidth on the interface, the value must between 1% to 75%, and the total allocation of all class-based QoS policies in the policy group must not exceed 75%. If the interface is on a VIP card, the upper limit is 99%. • Kbits/sec or Ratio—Select whether to define the bandwidth as a rate or percentage. **Note** You cannot mix unit type within a policy group. In a single policy group, all policies must use only Kbits/sec or only Ratio.
Set WFQ Properties	Enable WFQ—Select this check box to use WFQ. One of the following fields is displayed. • Number of Queues—The number of hashed queues to be reserved for the default class policy. Traffic that ends up in the default class is placed in one of these queues and serviced using WFQ. The number can be from 16 to 4096. There is no default. • Individual Queue Limit—The limit on the number of packets that can be held in each queue after the queue limit (for Tail drop) is reached. If a queue has exceeded the individual limit during a congestion event, packets are not dropped from the queue, but additional packets are not added until the queue is beneath the individual limit. The limit can be from 1 to 32768. This field is displayed for filtered traffic on VIP cards.

Table B-64 Policy Wizard Queuing Actions Page (continued)

Field	Description
Specify the priority of the traffic	(Priority Queuing only) Enable Priority—Select this check box to create a policy that directs traffic to a priority queue. • Select the priority queue to which filtered traffic should be directed. These strict-priority queues are serviced from the highest to lowest queue, with higher queues being emptied before lower queues are serviced, in this order: If you do not create a class default policy, unfiltered traffic is placed in the normal queue.
Specify bandwidth allocation	(Custom Queuing (CQ) only) Enable Bandwidth allocation—Select to define a queuing action. • Bandwidth—Enter the rate or percentage of the interface's bandwidth you want to allocate to the traffic in the Bandwidth field. The percentage value can be from 5% to 95%, and the total allocation of all custom queue policies on the interface or device group must not exceed 95%. The remaining 5% is used for unfiltered traffic.
Back button	Click to return to the previous step in the wizard.
Next button	Click to proceed to the next Actions page.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Policy Wizard: General Page, page B-71
- Policy Wizard: Filter Page, page B-72
- Policy Wizard: Congestion Avoidance Actions Page, page B-90

Policy Wizard: Congestion Avoidance Actions Page

Define drop actions for congestion avoidance. Select the drop mechanism used to determine how packets are dropped when congestion occurs.

To open this page, select **Actions > Congestion Avoidance** in the wizard navigation TOC.

Table B-65 Policy Wizard Congestion Avoidance Actions Page

Field	Description
Enable Congestion Avoidance	Select this check box to enable drop actions in the policy. This check box will automatically be selected after you define settings in this page.
Type of drop mechanism	• Tail drop—All packets are treated equally. Enter the queue limit. • WRED—Uses the precedence setting in the packets to selectively drop low priority packets before high priority packets. Specify the weight used to determine the length of the queues (Cisco recommends 10). See WRED Mapping Dialog Box, page B-68 for information about WRED mapping settings.
Back button	Click to return to the previous step in the wizard.
Next button	Click to proceed to the next step in the wizard. The Summary page appears.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Policy Wizard: General Page, page B-71
- Policy Wizard: Filter Page, page B-72
- Policy Wizard: Summary Page, page B-91

Policy Wizard: Summary Page

This page displays a summary of the QoS policy.

To open this page, select **Actions > Summary** in the wizard navigation TOC.

Table B-66 Policy Wizard Summary Page

Field	Description
Policy Summary	Displays a summary of the policy definition.
Back button	Click to return to the previous page in the wizard, if you want to make changes.
Finish button	Click to finish the Policy wizard and return to the Policies page.

Related Topics

- Policy Wizard: General Page, page B-71
- In Policies/Out Policies Page, page B-32

Policy Translation Page

Use this page to select the devices for which you want to view the CLI translation of the current deployment group's policies.

To open the Policy Translation page, select **Configure >Policy Groups**, then select **View CLI Translation** in the navigation TOC.

Table B-67 Policy Translation Page

Field	Description
Sys Name	System name of device.
Primary Device Name	The main IP address or hostname of the device.
Model	Device model.
OS Version	Version of the operating system on the device.
Mapped OS Version	OS version that QPM uses to determine QoS capabilities that can be configured.

Table B-67 Policy Translation Page (continued)

Field	Description
Status	Status of the device.
Translate button	Click to display the translation for the selected devices. The Translation page appears.

Related Topics

- Policy Groups Page, page B-14

Translation Report Page

This page displays the CLI translation of the current deployment group's policies for the selected devices.

To open this page, click **Translate** in the Policy Translation page.

Related Topics

- Policy Translation Page, page B-91

Upload QoS Configuration Page

Use this page to select the devices whose QoS configuration you want to upload into the current deployment group.

Table B-68 Upload QoS Configuration Page

Field	Description
Sys Name	System name of device.
Primary Device Name	The main IP address or hostname of the device.
Model	Device model.
OS Version	Version of the operating system on the device.
Mapped OS Version	OS version that QPM uses to determine QoS capabilities that can be configured.

Table B-68 Upload QoS Configuration Page (continued)

Field	Description
Policy Group	Policy groups to which the device is assigned.
Upload button	Click to start the upload operation. A dialog box opens informing you that the upload operation has started. See Upload Dialog Box, page B-93.

Related Topics

- Upload Reports Page, page D-3

Upload Dialog Box

Use this dialog box to go to the Upload Reports page, or continue editing policies, after the upload operation has started.

Table B-69 Upload Dialog Box

Field	Description
View button	Click to display the Upload Reports page.
Continue button	Click to display the Policy Groups page to continue editing policy groups and policies.

Related Topics

- Upload Reports Page, page D-3
- Policy Groups Page, page B-14

IP Telephony

The IP Telephony option contains the IP Telephony wizard that guides you through the process of configuring QoS for your IP telephony network.

To open the IP Telephony wizard, select **Configure > IP Telephony**.

The IP Telephony wizard contains the following pages:

IP Telephony Wizard: Introduction Page

Use this page to select the deployment group that will be used by the wizard for defining the IP telephony policies. This page also provides information of how the wizard will guide you to configure QoS for IP telephony.

To open this page, select **Configure > IP Telephony**.

Table B-70 IP Telephony Wizard - Introduction Page

Field	Description
Tell me more...	Click this link to open an information window describing how the wizard configures QoS for IP telephony.
Before you run the wizard for the first time...	Click this link if you are running the wizard for the first time. A window opens, prompting you to check the following: **a.** If you opened the wizard before adding or importing your devices into QPM's device inventory: – Click **Cancel** to exit the wizard. – Add/import your network devices to the device inventory. – Select **Configure > IP Telephony** to reopen the Introduction page of the wizard. **b.** Check if your devices support voice QoS by viewing the Voice Ready report. You can open this report in one of the following ways: – Click the Voice Ready Report link in step 2 of the wizard. – Select **Reports > IP Telephony**.
Deployment Group	Select the required deployment group from the list box, if it isn't already displayed.
Next button	Click to proceed to the next step. The IP Telephony wizard—Select IP Telephony Devices page appears.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- Import Devices Wizard, page A-22

- IP Telephony, page B-94
- IP Telephony Wizard: Select IP Telephony Devices Page, page B-96
- IP Telephony Wizard: End Page, page B-121
- Voice Ready Report Page, page D-2
- Introduction, page 5-10

IP Telephony Wizard: Select IP Telephony Devices Page

Use this page to select the devices that are part of your IP telephony network that require QoS configuration. The wizard assigns the selected devices to the appropriate voice policy groups with a Voice Device voice role.

To open this page, do any of the following:

- In the Introduction page of the IP Telephony wizard, click **Next**.
- In the IP Telephony wizard navigation TOC, select **Select Devices**.

Table B-71 IP Telephony Wizard - Select IP Telephony Devices Page

Field	Description
Voice Ready Report	Click this link to open a Voice Ready report to check if your devices are ready for QoS voice configuration.
Tell me more...	Click this link to open an information window describing global device configuration for Catalyst switches.
Display Configuration Info.	Select this check box to view summary information about the assignments made in this configuration step of the wizard. Deselect this check box if you don't want to view the assignments summary at this configuration step of the wizard.
System Name	Displays the system name of the device.
IP Address	Displays the IP address of the device.
Model	Displays the device model.
OS	Displays the version of the operating system on the device.
Back button	Click to return to the previous step of the wizard.

Table B-71 IP Telephony Wizard - Select IP Telephony Devices Page (continued)

Field	Description
Next button	Click to proceed to the next step. If you selected the Display Configuration Info. check box, the IP Telephony wizard—Assignment Summary page appears for this configuration step. If you deselected the Display Configuration Info. check box, the voice policy groups and the network element assignments for the current voice role will be saved to the deployment group, and the next configuration step of the wizard will appear.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- IP Telephony Wizard: Introduction Page, page B-95
- Import Devices Wizard, page A-22
- Voice Ready Report Page, page D-2
- IP Telephony Wizard: Assignment Summary Page, page B-97
- IP Telephony Wizard: Select IP Phone Connections Page, page B-99
- Selecting Devices for QoS Configuration, page 5-11

IP Telephony Wizard: Assignment Summary Page

Use this page to view summary information about the voice policy groups that were created for the voice role in the current configuration step, and the number of network elements that were assigned to the voice policy groups.

The following information may be displayed:

- Total number of network elements selected in the current step.
- Number of network elements that were selected, but previously assigned to voice policy groups with this voice role.
- Number of network elements that were newly assigned to voice policy groups with this voice role.

- Number of elements that were selected but not assigned to voice policy groups with this voice role, because they have no policies for this voice role. (For example, GigabitEthernet interfaces have the same interface type as FastEthernet interfaces, but they cannot be connected to an IP phone.)
- The number of related assignment elements (elements that were not selected, but were assigned to voice policy groups to complete the configuration correctly).
- The number of reassigned network elements.

To open this page, select the Display Configuration Info. check box in a configuration step of the IP Telephony wizard, and click **Next**.

Table B-72 IP Telephony Wizard - Assignment Summary Page

Field	Description
Name	Displays the name of the voice policy group. Click the Name link to view the properties and policies that are configured for the voice policy group. The General page opens for the voice policy group, in read-only mode. You cannot edit any of the properties and policies for the voice policy group.
Description	Displays a description of the voice policy group.
New Network Elements	Displays the number of network elements that were newly assigned to the voice policy group. Click the New Network Elements number link to view a list of the network elements that were newly assigned to the voice policy group.
Back button	Click to return to the previous page (selection step) to change your selection and assignments for the current voice role.
Next button	Click to save the voice policy groups and the network element assignments made for the current voice role to the deployment group, and proceed to the next selection step of the wizard.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- Assignment Summary, page 5-8
- General Page (Policy Group and Template), page B-17

IP Telephony Wizard: Select IP Phone Connections Page

Use this page to select the switch ports on which to configure QoS for your IP phones. The wizard assigns the selected ports to the appropriate voice policy groups with an IP Phone voice role.

To open this page, do any of the following:

- In the Select Devices page of the IP Telephony wizard, click **Next**.
- In the Assignment Summary page of the Select Devices configuration step, click **Next**.
- In the IP Telephony wizard navigation TOC, select **IP Phone**.

Table B-73 IP Telephony Wizard - Select IP Phone Connections Page

Field	Description
Description	This section is collapsed by default. Click the triangle to open a description of the QoS policies that will be configured on the interfaces for the IP Phone voice role.

Table B-73 IP Telephony Wizard - Select IP Phone Connections Page (continued)

Field	Description
Advanced	This section is collapsed by default. Click the triangle to open the Advanced section of the configuration step page, which provides the following two buttons: • Remove—Click this button to open a page in which you can remove network elements that were assigned for a voice role. This option lets you change your selection of network elements after they have been assigned to voice policy groups. The wizard removes the assignment of selected elements from the voice policy group. • Recommend—If QPM recommended rules are available for a specific voice role, clicking this button activates the wizard to accept the recommended selection of network elements for the current voice role. A list of the rules for the current voice role is displayed.
Selection Table	This section is expanded by default. It displays the table in which you select the network elements for QoS configuration. You can collapse this section, if required, by clicking the triangle.
Display Configuration Info.	Select this check box to view summary information about the assignments made in this configuration step of the wizard. Deselect this check box if you don't want to view the assignments summary at this configuration step of the wizard.
Name	Displays the interface or switch port name.
Type	Displays the interface or switch port type.
Description	Displays the interface or switch port description.
Card Type	Displays the type of card on which the interface or switch port resides.
Rate	Displays the interface or switch port rate.
Device Name	Displays the system name of the device.
Voice Role	Displays the voice role associated with the voice policy groups to which the interface or switch port is currently assigned.
Peer Model	Displays the neighboring interface's device name.
Back button	Click to return to the previous step of the wizard.

Table B-73 IP Telephony Wizard - Select IP Phone Connections Page (continued)

Field	Description
Next button	Click to proceed to the next step. If you selected the Display Configuration Info. check box, the IP Telephony wizard—Assignment Summary page appears for this configuration step. If you deselected the Display Configuration Info. check box, the voice policy groups and the network element assignments for the current voice role will be saved to the deployment group, and the next configuration step of the wizard will appear.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- IP Telephony Wizard: Select IP Telephony Devices Page, page B-96
- IP Telephony Wizard: Assignment Summary Page, page B-97
- IP Telephony Wizard: Remove Network Elements Page, page B-101
- IP Telephony Wizard: Select SoftPhone Connections Page, page B-103
- Selecting the IP Phone Connections, page 5-13

IP Telephony Wizard: Remove Network Elements Page

Use this page to remove network elements that were assigned for a voice role. This option lets you change your selection of network elements after they have been assigned to voice policy groups. The wizard removes the assignment of the selected elements from the voice policy group.

To open this page, click **Remove** in the Advanced section in a configuration step of the IP Telephony wizard.

Table B-74 IP Telephony Wizard - Remove Network Elements Page

Field	Description
Name	Displays the network element name.

Table B-74 IP Telephony Wizard - Remove Network Elements Page (continued)

Field	Description
Type	Displays the network element type.
Description	Displays the network element description.
Card Type	Displays the type of card on which the network element resides.
Rate	Displays the network element rate.
Device Name	Displays the system name of the device to which the network element belongs.
Peer Model	Displays the neighboring interface's device name.
Remove button	Click to remove a selected network element(s) from the list, and close the page.

Related Topics

- IP Telephony Wizard: Select IP Phone Connections Page, page B-99
- IP Telephony Wizard: Select SoftPhone Connections Page, page B-103
- IP Telephony Wizard: Select CallManager Connections Page, page B-105
- IP Telephony Wizard: Select IntraLAN Connections Page, page B-107
- IP Telephony Wizard: Select Voice VLAN Connections Page, page B-110
- IP Telephony Wizard: Select Switch to WAN Router Connections Page, page B-112
- IP Telephony Wizard: Select Router WAN to Switch Connections Page, page B-114
- IP Telephony Wizard: Select WAN Point to Point Connections Page, page B-116
- IP Telephony Wizard: Select WAN Frame Relay Connections Page, page B-118

IP Telephony Wizard: Select SoftPhone Connections Page

Use this page to select the switch port(s) on which the wizard will configure QoS for the SoftPhone connection(s) in your network. The wizard assigns the selected ports to the appropriate voice policy groups with a SoftPhone voice role.

To open this page, do any of the following:

- In the Select IP Phone Connections page of the IP Telephony wizard, click **Next**.
- In the Assignment Summary page of the IP Phone configuration step, click **Next**.
- In the IP Telephony wizard navigation TOC, select **SoftPhone**.

Table B-75 IP Telephony Wizard - Select SoftPhone Connections Page

Field	Description
Description	This section is collapsed by default. Click the triangle to open a description of the QoS policies that will be configured on the interfaces for the SoftPhone voice role.
Advanced	This section is collapsed by default. Click the triangle to open the Advanced section of the configuration step page, which provides the following two buttons: • Remove—Click this button to open a page in which you can remove network elements that were assigned for a voice role. This option lets you change your selection of network elements after they have been assigned to voice policy groups. The wizard removes the assignment of selected elements from the voice policy group. • Recommend—If QPM recommended rules are available for a specific voice role, clicking this button activates the wizard to accept the recommended selection of network elements for the current voice role. A list of the rules for the current voice role is displayed.
Selection Table	This section is expanded by default. It displays the table in which you select the network elements for QoS configuration. You can collapse this section, if required, by clicking the triangle.

Table B-75 IP Telephony Wizard - Select SoftPhone Connections Page (continued)

Field	Description
Display Configuration Info.	Select this check box to view summary information about the assignments made in this configuration step of the wizard. Deselect this check box if you don't want to view the assignments summary at this configuration step of the wizard.
Name	Displays the interface or switch port name.
Type	Displays the interface or switch port type.
Description	Displays the interface or switch port description.
Card Type	Displays the type of card on which the interface or switch port resides.
Rate	Displays the interface or switch port rate.
Device Name	Displays the system name of the device.
Voice Role	Displays the voice role associated with the voice policy groups to which the interface or switch port is currently assigned.
Peer Model	Displays the neighboring interface's device name.
Back button	Click to return to the previous step of the wizard.
Next button	Click to proceed to the next step. If you selected the Display Configuration Info. check box, the IP Telephony wizard—Assignment Summary page appears for this configuration step. If you deselected the Display Configuration Info. check box, the voice policy groups and the network element assignments for the current voice role will be saved to the deployment group, and the next configuration step of the wizard will appear.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- IP Telephony Wizard: Select IP Phone Connections Page, page B-99
- IP Telephony Wizard: Assignment Summary Page, page B-97
- IP Telephony Wizard: Remove Network Elements Page, page B-101

- IP Telephony Wizard: Select CallManager Connections Page, page B-105
- Selecting the SoftPhone Connections, page 5-14

IP Telephony Wizard: Select CallManager Connections Page

Use this page to select the switch ports on which the wizard will configure the QoS settings for the CallManager and Voice Gateway connections in your network. The wizard assigns the selected ports to the appropriate voice policy groups with a CallManager voice role.

To open this page, do any of the following:

- In the Select SoftPhone Connections page of the IP Telephony wizard, click **Next**.
- In the Assignment Summary page of the SoftPhone configuration step, click **Next**.
- In the IP Telephony wizard navigation TOC, select **CallManager**.

Table B-76 IP Telephony Wizard - Select CallManager Connections Page

Field	Description
Description	This section is collapsed by default. Click the triangle to open a description of the QoS policies that will be configured on the interfaces for the CallManager voice role.

Table B-76 IP Telephony Wizard - Select CallManager Connections Page (continued)

Field	Description
Advanced	This section is collapsed by default. Click the triangle to open the Advanced section of the configuration step page, which provides the following two buttons: • Remove—Click this button to open a page in which you can remove network elements that were assigned for a voice role. This option lets you change your selection of network elements after they have been assigned to voice policy groups. The wizard removes the assignment of selected elements from the voice policy group. • Recommend—If QPM recommended rules are available for a specific voice role, clicking this button activates the wizard to accept the recommended selection of network elements for the current voice role. A list of the rules for the current voice role is displayed.
Selection Table	This section is expanded by default. It displays the table in which you select the network elements for QoS configuration. You can collapse this section, if required, by clicking the triangle.
Display Configuration Info.	Select this check box to view summary information about the assignments made in this configuration step of the wizard. Deselect this check box if you don't want to view the assignments summary at this configuration step of the wizard.
Name	Displays the interface or switch port name.
Type	Displays the interface or switch port type.
Description	Displays the interface or switch port description.
Card Type	Displays the type of card on which the interface or switch port resides.
Rate	Displays the interface or switch port rate.
Device Name	Displays the system name of the device.
Voice Role	Displays the voice role associated with the voice policy groups to which the interface or switch port is currently assigned.
Peer Model	Displays the neighboring interface's device name.
Back button	Click to return to the previous step of the wizard.

Table B-76 IP Telephony Wizard - Select CallManager Connections Page (continued)

Field	Description
Next button	Click to proceed to the next step. If you selected the Display Configuration Info. check box, the IP Telephony wizard—Assignment Summary page appears for this configuration step. If you deselected the Display Configuration Info. check box, the voice policy groups and the network element assignments for the current voice role will be saved to the deployment group, and the next configuration step of the wizard will appear.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- IP Telephony Wizard: Select SoftPhone Connections Page, page B-103
- IP Telephony Wizard: Assignment Summary Page, page B-97
- IP Telephony Wizard: Remove Network Elements Page, page B-101
- IP Telephony Wizard: Select IntraLAN Connections Page, page B-107
- Selecting the CallManager and Gateways Ready Ports, page 5-15

IP Telephony Wizard: Select IntraLAN Connections Page

Use this page to define the appropriate QoS for the internal LAN ports—the uplinks and downlinks in your network. The wizard will configure the QoS automatically according to the type of neighboring switch.

To open this page, do any of the following:

- In the Select CallManager Connections page of the IP Telephony wizard, click **Next**.
- In the Assignment Summary page of the CallManager configuration step, click **Next**.
- In the IP Telephony wizard navigation TOC, select **IntraLAN**.

Table B-77 IP Telephony Wizard - Select IntraLAN Connections Page

Field	Description
Description	This section is collapsed by default. Click the triangle to open a description of the QoS policies that will be configured on the interfaces for the IntraLAN voice role.
Advanced	This section is collapsed by default. Click the triangle to open the Advanced section of the configuration step page, which provides the following two buttons: • Remove—Click this button to open a page in which you can remove network elements that were assigned for a voice role. This option lets you change your selection of network elements after they have been assigned to voice policy groups. The wizard removes the assignment of selected elements from the voice policy group. • Recommend—If QPM recommended rules are available for a specific voice role, clicking this button activates the wizard to accept the recommended selection of network elements for the current voice role. A list of the rules for the current voice role is displayed.
Selection Table	This section is expanded by default. It displays the table in which you select the network elements for QoS configuration. You can collapse this section, if required, by clicking the triangle.
Display Configuration Info.	Select this check box to view summary information about the assignments made in this configuration step of the wizard. Deselect this check box if you don't want to view the assignments summary at this configuration step of the wizard.
Name	Displays the interface name.
Type	Displays the interface type.
Description	Displays the interface description.
Card Type	Displays the type of card on which the interface resides.
Rate	Displays the interface rate.
Device Name	Displays the system name of the device.

Table B-77 IP Telephony Wizard - Select IntraLAN Connections Page (continued)

Field	Description
Voice Role	Displays the voice role associated with the voice policy groups to which the interface is currently assigned.
Peer Model	Displays the neighboring interface's device name.
Back button	Click to return to the previous step of the wizard.
Next button	Click to proceed to the next step. If you selected the Display Configuration Info. check box, the IP Telephony wizard—Assignment Summary page appears for this configuration step. If you deselected the Display Configuration Info. check box, the voice policy groups and the network element assignments for the current voice role will be saved to the deployment group, and the next configuration step of the wizard will appear.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- IP Telephony Wizard: Select CallManager Connections Page, page B-105
- IP Telephony Wizard: Assignment Summary Page, page B-97
- IP Telephony Wizard: Remove Network Elements Page, page B-101
- IP Telephony Wizard: Select Voice VLAN Connections Page, page B-110
- Selecting the IntraLAN Connections, page 5-16

IP Telephony Wizard: Select Voice VLAN Connections Page

Use this page to select the auxiliary VLANs on which to configure QoS on both the access and distribution layer switches. The wizard configures VLAN based policies for the voice VLANs on which the IP phone ports and the Layer 2 switch to Layer 3 switch connections are configured.

To open this page, do any of the following:

- In the Select IntraLAN Connections page of the IP Telephony wizard, click **Next**.
- In the Assignment Summary page of the IntraLAN configuration step, click **Next**.
- In the IP Telephony wizard navigation TOC, select **Voice VLAN**.

Table B-78 IP Telephony Wizard - Select Voice VLAN Connections Page

Field	Description
Description	This section is collapsed by default. Click the triangle to open a description of the QoS policies that will be configured on the interfaces for the Voice VLAN voice role.
Advanced	This section is collapsed by default. Click the triangle to open the Advanced section of the configuration step page, which provides the following two buttons: • Remove—Click this button to open a page in which you can remove network elements that were assigned for a voice role. This option lets you change your selection of network elements after they have been assigned to voice policy groups. The wizard removes the assignment of selected elements from the voice policy group. • Recommend—If QPM recommended rules are available for a specific voice role, clicking this button activates the wizard to accept the recommended selection of network elements for the current voice role. A list of the rules for the current voice role is displayed.
Selection Table	This section is expanded by default. It displays the table in which you select the network elements for QoS configuration. You can collapse this section, if required, by clicking the triangle.

Table B-78 IP Telephony Wizard - Select Voice VLAN Connections Page (continued)

Field	Description
Display Configuration Info.	Select this check box to view summary information about the assignments made in this configuration step of the wizard. Deselect this check box if you don't want to view the assignments summary at this configuration step of the wizard.
Name	Displays the VLAN name.
Index	Displays the VLAN index.
Type	Displays the VLAN type.
Device Name	Displays the system name of the device.
Voice Role	Displays the voice role associated with the voice policy groups to which the VLAN is currently assigned.
Back button	Click to return to the previous step of the wizard.
Next button	Click to proceed to the next step. If you selected the Display Configuration Info. check box, the IP Telephony wizard—Assignment Summary page appears for this configuration step. If you deselected the Display Configuration Info. check box, the voice policy groups and the network element assignments for the current voice role will be saved to the deployment group, and the next configuration step of the wizard will appear.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- IP Telephony Wizard: Select IntraLAN Connections Page, page B-107
- IP Telephony Wizard: Assignment Summary Page, page B-97
- IP Telephony Wizard: Remove Network Elements Page, page B-101
- IP Telephony Wizard: Select Switch to WAN Router Connections Page, page B-112
- Selecting Voice VLAN Devices, page 5-17

IP Telephony Wizard: Select Switch to WAN Router Connections Page

Use this page to define QoS for the distribution switch interfaces to the WAN router in your network.

To open this page, do any of the following:

- In the Select Voice VLAN Connections page of the IP Telephony wizard, click **Next**.
- In the Assignment Summary page of the Voice VLAN configuration step, click **Next**.
- In the IP Telephony wizard navigation TOC, select **Switch to WAN Router**.

Table B-79 IP Telephony Wizard - Select Switch to WAN Router Connections Page

Field	Description
Description	This section is collapsed by default. Click the triangle to open a description of the QoS policies that will be configured on the interfaces for the Switch to WAN Router voice role.
Advanced	This section is collapsed by default. Click the triangle to open the Advanced section of the configuration step page, which provides the following two buttons: • Remove—Click this button to open a page in which you can remove network elements that were assigned for a voice role. This option lets you change your selection of network elements after they have been assigned to voice policy groups. The wizard removes the assignment of selected elements from the voice policy group. • Recommend—If QPM recommended rules are available for a specific voice role, clicking this button activates the wizard to accept the recommended selection of network elements for the current voice role. A list of the rules for the current voice role is displayed.
Selection Table	This section is expanded by default. It displays the table in which you select the network elements for QoS configuration. You can collapse this section, if required, by clicking the triangle.

Table B-79 IP Telephony Wizard - Select Switch to WAN Router Connections Page (continued)

Field	Description
Display Configuration Info.	Select this check box to view summary information about the assignments made in this configuration step of the wizard. Deselect this check box if you don't want to view the assignments summary at this configuration step of the wizard.
Name	Displays the interface name.
Type	Displays the interface type.
Description	Displays the interface description.
Card Type	Displays the type of card on which the interface resides.
Rate	Displays the interface rate.
Device Name	Displays the system name of the device.
Voice Role	Displays the voice role associated with the voice policy groups to which the interface is currently assigned.
Peer Model	Displays the neighboring interface's device name.
Back button	Click to return to the previous step of the wizard.
Next button	Click to proceed to the next step. If you selected the Display Configuration Info. check box, the IP Telephony wizard—Assignment Summary page appears for this configuration step. If you deselected the Display Configuration Info. check box, the voice policy groups and the network element assignments for the current voice role will be saved to the deployment group, and the next configuration step of the wizard will appear.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- IP Telephony Wizard: Select Voice VLAN Connections Page, page B-110
- IP Telephony Wizard: Assignment Summary Page, page B-97
- IP Telephony Wizard: Remove Network Elements Page, page B-101

- IP Telephony Wizard: Select Router WAN to Switch Connections Page, page B-114
- Selecting the Switch to the WAN Router Connections, page 5-18

IP Telephony Wizard: Select Router WAN to Switch Connections Page

Use this page to define QoS for the router interfaces to the distribution and access switches in your network.

To open this page, do any of the following:

- In the Select Switch to WAN Router Connections page of the IP Telephony wizard, click **Next**.
- In the Assignment Summary page of the Switch to WAN Router configuration step, click **Next**.
- In the IP Telephony wizard navigation TOC, select **Router WAN to Switch**.

Table B-80 IP Telephony Wizard - Select Router WAN to Switch Connections Page

Field	Description
Description	This section is collapsed by default. Click the triangle to open a description of the QoS policies that will be configured on the interfaces for the Router WAN to Switch voice role.

Table B-80 IP Telephony Wizard - Select Router WAN to Switch Connections Page (continued)

Field	Description
Advanced	This section is collapsed by default. Click the triangle to open the Advanced section of the configuration step page, which provides the following two buttons: • Remove—Click this button to open a page in which you can remove network elements that were assigned for a voice role. This option lets you change your selection of network elements after they have been assigned to voice policy groups. The wizard removes the assignment of selected elements from the voice policy group. • Recommend—If QPM recommended rules are available for a specific voice role, clicking this button activates the wizard to accept the recommended selection of network elements for the current voice role. A list of the rules for the current voice role is displayed.
Selection Table	This section is expanded by default. It displays the table in which you select the network elements for QoS configuration. You can collapse this section, if required, by clicking the triangle.
Display Configuration Info.	Select this check box to view summary information about the assignments made in this configuration step of the wizard. Deselect this check box if you don't want to view the assignments summary at this configuration step of the wizard.
Name	Displays the interface name.
Type	Displays the interface type.
Description	Displays the interface description.
Card Type	Displays the type of card on which the interface resides.
Rate	Displays the interface rate.
Device Name	Displays the system name of the device.
Voice Role	Displays the voice role associated with the voice policy groups to which the interface is currently assigned.
Peer Model	Displays the neighboring interface's device name.
Back button	Click to return to the previous step of the wizard.

Table B-80 IP Telephony Wizard - Select Router WAN to Switch Connections Page (continued)

Field	Description
Next button	Click to proceed to the next step. If you selected the Display Configuration Info. check box, the IP Telephony wizard—Assignment Summary page appears for this configuration step. If you deselected the Display Configuration Info. check box, the voice policy groups and the network element assignments for the current voice role will be saved to the deployment group, and the next configuration step of the wizard will appear.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- IP Telephony Wizard: Select Switch to WAN Router Connections Page, page B-112
- IP Telephony Wizard: Assignment Summary Page, page B-97
- IP Telephony Wizard: Remove Network Elements Page, page B-101
- IP Telephony Wizard: Select WAN Point to Point Connections Page, page B-116
- Selecting the Router WAN to Switch Connections, page 5-19

IP Telephony Wizard: Select WAN Point to Point Connections Page

Use this page to select the interfaces on which to configure QoS for the WAN Serial Point-to-Point links in your network.

To open this page, do any of the following:

- In the Select Router WAN to Switch Connections page of the IP Telephony wizard, click **Next**.
- In the Assignment Summary page of the Router WAN to Switch configuration step, click **Next**.

- In the IP Telephony wizard navigation TOC, select **WAN Point to Point**.

Table B-81 IP Telephony Wizard - Select WAN Point to Point Connections Page

Field	Description
Description	This section is collapsed by default. Click the triangle to open a description of the QoS policies that will be configured on the interfaces for the WAN Point to Point voice role.
Advanced	This section is collapsed by default. Click the triangle to open the Advanced section of the configuration step page, which provides the following two buttons: • Remove—Click this button to open a page in which you can remove network elements that were assigned for a voice role. This option lets you change your selection of network elements after they have been assigned to voice policy groups. The wizard removes the assignment of selected elements from the voice policy group. • Recommend—If QPM recommended rules are available for a specific voice role, clicking this button activates the wizard to accept the recommended selection of network elements for the current voice role. A list of the rules for the current voice role is displayed.
Selection Table	This section is expanded by default. It displays the table in which you select the network elements for QoS configuration. You can collapse this section, if required, by clicking the triangle.
Display Configuration Info.	Select this check box to view summary information about the assignments made in this configuration step of the wizard. Deselect this check box if you don't want to view the assignments summary at this configuration step of the wizard.
Name	Displays the interface name.
Type	Displays the interface type.
Description	Displays the interface description.
Card Type	Displays the type of card on which the interface resides.
Rate	Displays the interface rate.
Device Name	Displays the system name of the device.

Table B-81 IP Telephony Wizard - Select WAN Point to Point Connections Page (continued)

Field	Description
Voice Role	Displays the voice role associated with the voice policy groups to which the interface is currently assigned.
Peer Model	Displays the neighboring interface's device name.
Back button	Click to return to the previous step of the wizard.
Next button	Click to proceed to the next step. If you selected the Display Configuration Info. check box, the IP Telephony wizard—Assignment Summary page appears for this configuration step. If you deselected the Display Configuration Info. check box, the voice policy groups and the network element assignments for the current voice role will be saved to the deployment group, and the next configuration step of the wizard will appear.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- IP Telephony Wizard: Select Router WAN to Switch Connections Page, page B-114
- IP Telephony Wizard: Assignment Summary Page, page B-97
- IP Telephony Wizard: Remove Network Elements Page, page B-101
- IP Telephony Wizard: Select WAN Frame Relay Connections Page, page B-118
- Selecting WAN Serial Point-to-Point Connections, page 5-20

IP Telephony Wizard: Select WAN Frame Relay Connections Page

Use this page to select the interfaces on which to configure QoS for the Frame Relay WAN links in your network.

To open this page, do any of the following:

- In the Select WAN Point to Point Connections page of the IP Telephony wizard, click **Next**.
- In the Assignment Summary page of the WAN Point to Point configuration step, click **Next**.
- In the IP Telephony wizard navigation TOC, select **WAN Frame Relay**.

Table B-82 IP Telephony Wizard - Select WAN Frame Relay Connections Page

Field	Description
Description	This section is collapsed by default. Click the triangle to open a description of the QoS policies that will be configured on the interfaces for the WAN Frame Relay voice role.
Advanced	This section is collapsed by default. Click the triangle to open the Advanced section of the configuration step page, which provides the following two buttons: • Remove—Click this button to open a page in which you can remove network elements that were assigned for a voice role. This option lets you change your selection of network elements after they have been assigned to voice policy groups. The wizard removes the assignment of selected elements from the voice policy group. • Recommend—If QPM recommended rules are available for a specific voice role, clicking this button activates the wizard to accept the recommended selection of network elements for the current voice role. A list of the rules for the current voice role is displayed.
Selection Table	This section is expanded by default. It displays the table in which you select the network elements for QoS configuration. You can collapse this section, if required, by clicking the triangle.
Display Configuration Info.	Select this check box to view summary information about the assignments made in this configuration step of the wizard. Deselect this check box if you don't want to view the assignments summary at this configuration step of the wizard.
Name	Displays the interface name.

Table B-82 IP Telephony Wizard - Select WAN Frame Relay Connections Page (continued)

Field	Description
Type	Displays the interface type.
Description	Displays the interface description.
Card Type	Displays the type of card on which the interface resides.
Rate	Displays the interface rate.
Device Name	Displays the system name of the device.
Voice Role	Displays the voice role associated with the voice policy groups to which the interface is currently assigned.
Peer Model	Displays the neighboring interface's device name.
Back button	Click to return to the previous step of the wizard.
Next button	Click to proceed to the next step. If you selected the Display Configuration Info. check box, the IP Telephony wizard—Assignment Summary page appears for this configuration step. If you deselected the Display Configuration Info. check box, the voice policy groups and the network element assignments for the current voice role will be saved to the deployment group, and the next configuration step of the wizard will appear.
Finish button	Click to complete the wizard. The IP Telephony wizard—End page appears.

Related Topics

- IP Telephony Wizard: Select WAN Point to Point Connections Page, page B-116
- IP Telephony Wizard: Assignment Summary Page, page B-97
- IP Telephony Wizard: Remove Network Elements Page, page B-101
- IP Telephony Wizard: End Page, page B-121
- Selecting WAN Frame Relay Connections, page 5-22

IP Telephony Wizard: End Page

This page informs you that you have completed the IP Telephony wizard and that the QoS policies have been added and saved in your deployment group. Use this page to select whether to deploy the deployment group directly, or view a detailed summary of all the voice policy groups that were created by the wizard.

To open this page, do any of the following:

- In the Select WAN Frame Relay Connections page of the IP Telephony wizard, click **Next**.
- In the Assignment Summary page of the WAN Frame Relay configuration step, click **Next**.
- In the IP Telephony wizard navigation TOC, select **End**.
- Click **Finish** in any of the IP Telephony wizard configuration steps.

Table B-83 IP Telephony Wizard - End Page

Field	Description
Do you want to deploy your QoS policies now?	• Click the Yes radio button if you want to deploy your QoS policies directly. • Click the No radio button to go to the Policy Groups page to view the voice policy groups that were created by the wizard. From the Policy Groups page, you can modify the properties and policies configured in the voice policy groups, if required.
Back button	Click to go back through the wizard to change any of your selections.
Finish button	Click to close the wizard. The Policy Groups page or the Deployment Wizard appears, depending on your Yes/No selection.

Related Topics

- IP Telephony Wizard: Select WAN Frame Relay Connections Page, page B-118
- Policy Groups Page, page B-14
- Deployment Wizard - Deployment Group Selection Page, page C-2

Search

The following topics describe the fields in the pages that are accessed from the Search option to find policy groups and policies:

Policy/Properties Search Page

Use this page to define search criteria to find policy groups and policies.

To open this page, select **Configure > Search**.

Table B-84 Policy / Properties Search Page

Field	Description
Select Deployment Group	Select this radio button to search for policies or properties in deployment groups. • Select the deployment group in which to search. You can choose a single deployment group, or all deployment groups.
Templates	Select this radio button to search for policies or properties in policy group templates.
Policy Group Name (contains)	Enter all or part of the name of the policy group in which to search.
Policy	Select this radio button to search for policies that match the specified criteria: • Policy Name (contains)—Enter all or part of the name of the policies you want to find. • Policy Action—Select the action defined in the policies you want to find.

Table B-84 Policy / Properties Search Page (continued)

Field	Description
Properties	Select this radio button to search for policy groups that contain the specified properties: • Select a property from the list box.
Search button	Click to run the search. The corresponding Results page appears displaying the search results.

Related Topics

- Searching for QoS Properties and Policies, page 6-37
- Policy Search Results Page, page B-123
- Properties Search Results Page, page B-124
- Templates Policies Search Results Page, page B-125
- Templates Properties Search Results Page, page B-125

Policy Search Results Page

This page appears after you run a policy search in deployment groups, and displays the results of your search.

Table B-85 Policy Search Results Page

Field	Description
Deployment Group	Displays the names of the deployment groups to which the matching policies belong.
Policy Group	Displays the names of the policy groups to which the matching policies belong. Click a name to display the Policy Group General page to view and edit policy group information.
Policy Name	Displays the names of the policies that matched the search criteria. Click a name to display the Policy Summary page to view and edit policy information.
Policy Description	Displays the policy description.

Table B-85 Policy Search Results Page (continued)

Field	Description
Back to Search button	Click to return to the Policy/Properties Search page.

Related Topics

- General Page (Policy Group and Template), page B-17
- Policy Summary Page, page B-34
- Policy/Properties Search Page, page B-122

Properties Search Results Page

This page appears after you run a properties search in deployment groups, and displays the results of your search.

Table B-86 Properties Search Results Page

Field	Description
Deployment Group	Displays the names of the deployment groups to which the matching policy groups belong.
Policy Group	Displays the name of the policy group that matched a search criteria. Click a name to display the Policy Group General page to view and edit policy group information.
Property Type	Displays the name of each property type for which a matching policy group was found. Click a name to display the Policy Group QoS Properties page to view and edit QoS property information.
Back to Search button	Click to return to the Policy/Properties Search page.

Related Topics

- General Page (Policy Group and Template), page B-17
- Policy/Properties Search Page, page B-122
- QoS Properties Page, page B-20

Templates Policies Search Results Page

This page appears after you run a policy search in policy group templates, and displays the results of your search.

Table B-87 Templates Policies Search Results Page

Field	Description
Policy Group Template	Displays the names of the policy group templates to which the matching policies belong. Click a name to display the Policy Group Template General page to view and edit policy group template information.
Policy Name	Displays the names of the policies that matched the search criteria. Click a name to display the Policy Summary page to view and edit policy information.
Policy Description	Displays the policy description.
Back to Search button	Click to return to the Policy/Properties Search page.

Related Topics

- General Page (Policy Group and Template), page B-17
- Policy Summary Page, page B-34
- Policy/Properties Search Page, page B-122

Templates Properties Search Results Page

This page appears after you run a properties search in policy group templates, and displays the results of your search.

Table B-88 Templates Properties Search Results Page

Field	Description
Policy Group Template	Displays the name of the policy group template that matched a search criteria. Click a name to display the Policy Group Template General page to view and edit policy group template information.

Table B-88 Templates Properties Search Results Page (continued)

Field	Description
Property Type	Displays the name of each property type for which a matching policy group template was found. Click a name to display the Policy Group QoS Properties page to view and edit QoS property information.
Back to Search button	Click to return to the Policy/Properties Search page.

Related Topics

- General Page (Policy Group and Template), page B-17
- QoS Properties Page, page B-20
- Policy/Properties Search Page, page B-122

Deploy Tab Reference

The following topics describe the pages in the Deploy tab. Topics are organized according to the following Deploy tab options:

Deployment

The Deployment option contains the Deployment wizard that guides you through the process of creating a deployment job.

To open the Deployment wizard, select **Deploy > Deployment**.

The following pages are accessed from the Deployment option:

- Deployment Wizard - Job Details Page, page C-9
- Deployment Wizard - Summary Page, page C-10

Related Topics

- Using QPM Wizards, page 3-10

Deployment Wizard - Deployment Group Selection Page

Use this page to select the deployment group to be deployed.

To open this page, do any of the following:

- Select **Deploy > Deployment**.
- In the Deployment wizard navigation TOC, select **Deployment Group Selection**.

Table C-1 Deployment Wizard - Deployment Group Selection Page

Field	Description
Current version of a deployment group	Select this radio button to deploy the current version of a deployment group, and then choose the required deployment group from the list box. Click the View list link to open the Deployment Groups List page, displaying a detailed list of all the currently managed deployment groups.
Restore a previous version of a deployment group	Select this radio button to deploy a historical version of a deployment group, and then choose the required deployment group from the list box. Click the View list link to open the Job History List page, displaying all the historical deployment groups.
Next button	Click to proceed to the next step of the wizard.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Deployment Groups List Page, page C-3
- Job History List Page, page C-4
- Validate Historical Page, page C-5
- Step 1: Selecting a Deployment Group for Deployment, page 7-4

Deployment Groups List Page

Use this page to view the details (Owner, Creation Time) of all the current deployment groups, before making your deployment group selection. You can access this page from the Deployment wizard, the CLI Preview wizard, or the Device Configuration Verification wizard.

To open this page, do one of the following:

- Click the View list link alongside the current deployment group list box in the Deployment Group Selection page of the Deployment wizard.
- Click the View list link in the Deployment Group Selection page of the CLI Preview wizard.
- Click the View list link in the Deployment Group Selection page of the Device Configuration Verification wizard.

Table C-2 Deployment Groups List Page

Field	Description
Deployment Group	The deployment group name.
Owner	The person who last saved the deployment group.
Creation Time	The date and time the deployment group was created.
Select button	Click to confirm the deployment group selection. The selected deployment group name will be displayed in the current deployment group list box in the Deployment Group Selection page of the Deployment wizard, the CLI Preview wizard or the Device Configuration Verification wizard.

Related Topics

- Deployment Wizard - Deployment Group Selection Page, page C-2
- CLI Preview Wizard - Deployment Group Selection Page, page C-23
- Device Configuration Verification Wizard - Deployment Group Selection Page, page D-37

Job History List Page

Use this page to view the details of all the historical deployment groups before making your deployment group selection.

To open this page, click the View list link next to the historical deployment group list box in the Deployment Group Selection page of the Deployment wizard.

Table C-3 Job History List Page

Field	Description
Deployment Group	The deployment group name.
Version	The version number of the deployment job.
Job	The name of the deployment job.
Owner	The person who last saved the deployment group.
Creation Time	The date and time the deployment group was created.
Restore button	Click to confirm the historical deployment group selection. The selected deployment group name will be displayed in the historical deployment group list box in the Deployment Group Selection page.

Related Topics

- Deployment Wizard - Deployment Group Selection Page, page C-2
- Step 1: Selecting a Deployment Group for Deployment, page 7-4

Validate Historical Page

Use this page to access the validation report that results from the validation process of a historical deployment group.

To open this page, do any of the following:

- In the Deployment Group Selection page of the Deployment wizard, select a historical version of a deployment group and click **Next**.
- In the Deployment wizard navigation TOC, select **Validate Historical**.

Table C-4 Validate Historical Page

Field	Description
View Restore Validation Report	Click this button to open the Restore Validation Report window, that displays any validation violations that were discovered during the deployment group restore procedure.
Back button	Click to return to the previous step of the wizard.
Next button	Click to save the changed deployment group as a new version, and proceed to the next step of the wizard.
Finish button	Click to save the changed deployment group as a new version, and move to the last step of the wizard. The Summary page appears.

Related Topics

- Deployment Wizard - Deployment Group Selection Page, page C-2
- Restore Validation Report Window, page C-5
- Step 2: Validating the Historical Deployment Group, page 7-6

Restore Validation Report Window

Use this window to view a validation report that results from the validation checks that are done on a restored deployment group.

To open this window, click the View Restore Validation Report button in the Validate Historical page of the Deployment wizard.

Table C-5 Restore Validation Report Window

Field	Description
Missing Network Elements	Displays any invalid or missing network elements that were found in the restored deployment group. This validation procedure checks for the coordination of policies and managed devices. If the validation procedure detects network elements that are missing from the current device group, they will be displayed in this report. The assignments of policies to these network elements in the restored deployment group will be automatically removed.
Invalid Assignments	Displays any invalid assignments that were found in the restored deployment group. It displays all the network elements that no longer conform to the constraints of their policy group. The validation procedure checks for assigned network elements that no longer match the constraints of their policy groups. These network elements will be removed from the assignment.
Reusable Components Violations	Displays any reusable components violations that were found in the restored deployment group. This validation procedure checks for the coordination of policies and library components (IP aliases, application aliases and policy group templates). If the validation process detects some library components in the restored version that are different than the ones in the current libraries, this will be displayed in the report. The validation process overrides the current library components with the original ones and adds them locally to the deployment group. In this case, the dynamic link to the library components will no longer exist.
Constraints Violations	Displays any invalid policy groups that were found in the restored deployment group. This check validates the policy group device constraints against the predefined constraints limitations. These limitations may change from time to time causing some of the policy group constraints to be invalid. Invalid policy groups will be removed along with their assignments.

Related Topics

- Validate Historical Page, page C-5
- Step 2: Validating the Historical Deployment Group, page 7-6
- Restore Deployment Group Page, page C-16

Deployment Wizard - Device Selection and Preview Page

Use this page to preview your device configurations prior to deployment and select the devices you want to deploy.

To open this page, do any of the following:

- In the Deployment Group Selection page of the Deployment wizard, select a current version of a deployment group and click **Next**.
- In the Validate Historical page of the Deployment wizard, click **Next**.
- In the Deployment wizard navigation menu, select **Device Selection and Preview**.

Table C-6 Deployment Wizard - Device Selection and Preview Page

Field	Description
Device	Displays the device name or IP address. Devices whose configurations have changed since the last deployment will be displayed with the check boxes alongside them selected. You can accept the default selection, or you can make your own selection of devices to which you want to deploy your policies.
Device Folder	Displays the name of the device folder.

Table C-6 Deployment Wizard - Device Selection and Preview Page (continued)

Field	Description
Policy Configuration	Displays the current configuration for the device, as follows: • Modified—The device has not yet been configured with the latest configuration. • No Changes—The device was previously configured with the specified policies, and so does not require deployment. (You can override this by selecting/deselecting the check box of the device.) Click the policy configuration link to open a Device Configuration Preview window that displays the configuration details of the selected device.
Back button	Click to return to the previous step of the wizard.
Next button	Click to proceed to the next step of the wizard.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Deployment Wizard - Deployment Group Selection Page, page C-2
- Device Configuration Preview Window, page C-8
- Step 3: Selecting and Previewing the Devices for Deployment, page 7-7

Device Configuration Preview Window

Use this window to preview the configuration details of a device prior to deployment.

To open this window, do any of the following:

- Click a device's policy configuration link in the Device Selection and Preview page of the Deployment wizard.
- Click a device's policy configuration link in the Device Selection and Preview page of the CLI Preview wizard.
- Click a device's policy configuration link in the Device Selection and Preview page of the Device Configuration Verification wizard.

- Click the View CLI Commands button in a Job Details report.
- Click the View CLI Commands button in a CLI Preview Details page.
- Click the View CLI Commands button in a Job Verification Details page.

Table C-7 Device Configuration Preview Window

Field	Description
Backup button	Click to view the backup ShowRun configuration commands for the device.
Incremental Telnet button	Click to view the incremental Telnet script commands that will be written to the device, if deploying directly to network devices.
Close button	Click to close the Device Configuration Preview window.

Related Topics

- Deployment Wizard - Device Selection and Preview Page, page C-7
- Deployment Wizard - Job Details Page, page C-9
- Job Details Report Page, page C-17
- CLI Preview Wizard - Device Selection and Preview Page, page C-24
- CLI Preview Details Page, page C-25
- Job Verification Details Page, page D-35

Deployment Wizard - Job Details Page

Use this page to enter details about your deployment job and set the deployment options.

To open this page, do any of the following:

- In the Device Selection and Preview page of the Deployment wizard, click **Next**.
- In the Deployment wizard navigation TOC, select **Job Details**.

Table C-8 Deployment Wizard - Job Details Page

Field	Description
Job Name	The default deployment job name. You can change the default name by entering a name for your deployment job in this field.
Job Description	Optionally, you can enter a description for the deployment job in this field.
Deploy configuration to the devices using Telnet	Select this check box to deploy the deployment group directly to the devices. Deselect it if you don't want to deploy directly to the devices. By default, the check box is selected.
Back button	Click to return to the previous step of the wizard.
Next button	Click to proceed to the next step of the wizard.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Deployment Wizard - Device Selection and Preview Page, page C-7
- Job History Page, page C-14
- Step 4: Entering the Job Details for Deployment, page 7-9

Deployment Wizard - Summary Page

Use this page to view and verify all the data collected by the wizard for the current deployment job.

To open this page, do any of the following:

- In the Job Details page of the Deployment wizard, click **Next**.
- In the Deployment wizard navigation TOC, select **Summary**.

Table C-9 Deployment Wizard - Summary Page

Field	Description
Job Owner	The person who last saved the deployment job.
Job Name	The name of the deployment job.

Table C-9 Deployment Wizard - Summary Page (continued)

Field	Description
Job Description	A description of the deployment job, if available.
Deployment Group Name	The name of the deployment group.
Deployment Group Version	Current or History, depending on the deployment group version selected.
Number of devices to be deployed	The number of devices that will be deployed to.
Deploy configuration to the devices	Yes or No, depending on whether you selected to deploy directly to the devices in the Job Details page.
Back button	Click to return to the previous step of the wizard.
Deploy button	Click to deploy the deployment group to the network. The Active Jobs page appears.

Related Topics

- Deployment Wizard - Device Selection and Preview Page, page C-7
- Deployment Wizard - Job Details Page, page C-9
- Active Jobs Page, page C-12
- Step 5: Confirming the Wizard Information for Deployment, page 7-10

Jobs

The following topics describe the fields in the pages that are accessed from the Jobs option:

- Active Jobs Page, page C-12
- Job History Page, page C-14
- Restore Deployment Group Page, page C-16
- DNS Resolution Page, page C-17
- Job Details Report Page, page C-17
- Device Errors and Warnings Page, page C-19

- Deployment History Report Page, page C-19
- Managed Devices Page, page C-20

Active Jobs Page

The Active Jobs page provides a dynamic view of all the active deployments and their status. Use the Active Jobs page to:

- View the status of all the active deployment jobs.
- Redeploy a failed deployment.
- Pause and resume the deployment process.
- Terminate a deployment.
- Remove a deployment job from the table.
- View the details of a deployment job.

To open this page, do one of the following:

- Select **Deploy > Jobs > Active Jobs**.
- Click **Deploy** in the Summary page of the Deployment wizard.

Table C-10 Active Jobs Page

Field	Description
Job Name	The name of the deployment job. Click the Job Name link for a selected job to open the Job Details report for that job.
Owner	The person who last saved the deployment job.
Deployment Group	The name of the deployment group.
Start Time	The start time of deployment job configuration.
Job Status	Selected deployment job's status (Pending, In Progress, Paused, Aborted, Completed, or Failed).
Devices Pending	The number of devices that are waiting for deployment.
Devices In Progress	The number of devices whose deployment is in-progress.
Devices Completed	The number of devices whose deployment completed successfully.
Devices Failed	The number of devices whose deployment failed.

Table C-10 Active Jobs Page (continued)

Field	Description
Total	The total number of devices in the current deployment. (This number is the sum of the four previous status fields.)
Refresh	Click to force a manual update of the displayed data. The display is automatically refreshed every ten seconds.
Pause	Click to pause a job during deployment. Any devices that are being configured when the Pause command is issued will be finished. Devices for which deployment had not yet begun, will remain with the status “Pending”.
Resume	Click to resume the configuration of devices for a job that was paused.
Redeploy	Click to manually request that deployment be re-tried for a specific failed device or all failed devices in the selected job. Another deployment is created for the job.
Remove from Display	Click to remove a completed or failed deployment job from the table.
Abort	Click to terminate a deployment that is currently in progress or has been paused. Any devices that were not configured when the Abort command was issued will not be deployed. They will be set as Failed. A terminated deployment cannot be resumed.

Related Topics

- Deployment Wizard - Summary Page, page C-10
- Job Details Report Page, page C-17
- Viewing the Deployment Status, page 7-10
- Pausing and Resuming a Deployment Job, page 7-12
- Redeploying a Job, page 7-14
- Viewing the Job Details Report, page 7-20

Job History Page

Use this page to:

- View the results of a DNS host name resolution check for a deployment job.
- View the history details of deployment jobs.
- Restore a historical version for editing and deploying.
- View a historical version's policy groups.
- Delete deployment jobs.
- Lock and unlock jobs for deletion.
- Download the configuration files of a deployment job
- View a Job Details report for a deployment job.
- View a Deployment History report for a job.

To open this page, select **Deploy > Jobs > Job History**.

Table C-11 Job History Page

Field	Description
Job Name	The name of the deployment job. Click the Job Name link for a selected job to open the Job Details report for that job.
Owner	The person who last saved the deployment job.
Deployment Group	The name of the deployment group.
Deployment Time	The time the last deployment occurred for the job.
Deployments	The number of deployments that were made for the job. Click the Deployments link of a job whose deployment details you want to view to open a Deployment History report for the selected deployment.
Status	The selected job's deployment status—Pending, In Progress, Completed, Paused, Aborted, or Failed.
Lock Job	Lock or Unlock, depending on whether the job is locked to prevent deletion when the history cache becomes full.
Files	Click this link to download the zip file containing the individual configuration files for a device to your desktop.

Table C-11 Job History Page (continued)

Field	Description
Details	Click the Details icon for a job to open its Job Details report in which you can view the status of devices related to the deployment job.
DNS Resolution	Click to view the results of a DNS host name resolution check for a selected deployment job.
View Deployment Group	Click to verify the details of a selected historical version. The Policy Groups page appears in read-only mode, displaying the selected deployment group and its policy groups.
Restore	Click to restore a selected historical version for editing and deploying. The Restore Deployment Group page appears.
Delete	Click to delete a selected historical version from the Job History list. After deleted, you cannot restore it.
Lock Job	Click to prevent a selected historical version from being automatically deleted when the history cache is full.
Unlock Job	Click to unlock a historical version, making it available for deletion.

Related Topics

- Restore Validation Report Window, page C-5
- Restore Deployment Group Page, page C-16
- DNS Resolution Page, page C-17
- Job Details Report Page, page C-17
- Deployment History Report Page, page C-19
- Job Details Report Page, page C-17
- Viewing the DNS Resolution, page 7-23
- Restoring and Deploying a Historical Deployment Group, page 7-16
- Viewing a Historical Deployment Group, page 7-17
- Deleting a Historical Job, page 7-18
- Locking and Unlocking a Historical Job, page 7-19

- Viewing the Job Details Report, page 7-20
- Viewing the Deployment History Report, page 7-22

Restore Deployment Group Page

Use this page to view the validation report for a deployment group that is being restored, and to confirm or cancel the restore process.

This page opens automatically when you click Restore after selecting a historical deployment group in the Job History page.

Table C-12 Restore Deployment Group Page

Field	Description
Name	The name of the deployment group.
Version	The restored version number of the deployment group.
Show Restore Report	Click to open a Restore Validation Report window for the selected deployment group.
OK	Click to confirm the restoring of this version as the current deployment group for editing and deploying. The Policy Groups page appears.

Related Topics

- Job History Page, page C-14
- Restore Validation Report Window, page C-5
- Policy Groups Page, page B-14

DNS Resolution Page

Use this page to view the results of a DNS resolution check done by QPM on the host names that QPM resolved to IP addresses, for a selected deployment job.

To open this page, do one of the following:

- In the Job History page, select the required historical job and click **DNS Resolution**.
- In the CLI Preview page, select the preview job and click **DNS Resolution.**

Table C-13 DNS Resolution Page

Field	Description
Host Name	The name of the network host.
Resolved Address	The IP address to which the host name was resolved.
Policy	The policy associated with the host.
Policy Group	The policy group to which the policy belongs.

Related Topics

- Job History Page, page C-14
- Viewing the DNS Resolution, page 7-23

Job Details Report Page

Use this page to view:

- The final status of all the deployments of a selected job.
- The current deployment status of a job that is still in progress.
- A table of all the devices related to the deployment job.
- The CLI commands that were used to configure a device.

To open this page, do any of the following:

- In the Active Jobs page, click the Job Name link for a job.
- In the Job History page, click the Job Name link of the job whose details you want to view, or click the Details icon for the job.
- In the Managed Devices page, click the Job Name link for a device.

Table C-14 Job Details Report Page

Field	Description
Job Name	The name of the deployment job.
Deployment Group	The name of the deployment group.
Device Group	The device group that contains the deployment job.
Job Status	The deployment job's status (Pending, In Progress, Paused, Aborted, Completed, or Failed).
Owner	The person who last saved the deployment job.
Creation Time	The date and time the job was created.
Job Description	The description of the job, if any.
Note	If you selected *not* to deploy the deployment group directly to the devices, this field will display "Deployment to files only".
Device Name/IP	The name of the device or its IP address.
Status	The deployment status of the device.
Status Time	The time the device received its status.
Errors/Warnings	An error string, if available. In the case of a FAILED status, the CLI command that caused the error will also be displayed. If the error string for a Failed job displays "Internal error - unknown device state", some of the job's devices might be stuck in progress. In such a case, QPM will not be able to determine what was configured on these devices. You should contact Cisco technical support for help.
View CLI Commands	Click to view the CLI commands that were used to configure the device. A Device Configuration window opens.

Related Topics

- Device Configuration Preview Window, page C-8
- Active Jobs Page, page C-12
- Job History Page, page C-14
- Device Errors and Warnings Page, page C-19
- Managed Devices Page, page C-20
- Viewing the Job Details Report, page 7-20

Device Errors and Warnings Page

Use this page to view details about any errors or warnings that resulted from the deployment of a device.

To open this page, click the Errors/Warnings link for a device in the Job Details Report page.

Table C-15 Device Errors and Warnings Page

Field	Description
Type	Displays **Error** or **Warning**.
Message	Displays the reason for the error or warning message.
Message Time	Displays the time the error or warning occurred.

Related Topics

- Job Details Report Page, page C-17
- Viewing Device Deployment Errors and Warnings, page 7-22

Deployment History Report Page

Use this page to view the deployment history details of a selected deployment.

To open this page, in the Job History page, click the Deployments link of the job whose deployment details you want to view.

Table C-16 Deployment History Report Page

Field	Description
Job Name	The name of the deployment job.
Deployment Group	The name of the deployment group.
Device Group	The device group that contains the deployment job.
Owner ID	The person who last saved the deployment job.
Creation Time	The date and time the job was created.
Job Description	The description of the job, if any.
Note	If you selected *not* to deploy the deployment group directly to the devices, this field will display "Deployment to files only".
Deployment Type	The deployment type - Normal or Redeploy. Click this link to view the Job Details report of the selected deployment.
Start Time	The date and time the deployment started.
End Time	The date and time the deployment ended.

Related Topics

- Deployment Wizard - Job Details Page, page C-9
- Job History Page, page C-14
- Viewing the Job Details Report, page 7-20
- Viewing the Deployment History Report, page 7-22

Managed Devices Page

Use this page to view all the devices in the current device group that were configured (deployed to) by QPM, and their statuses. Devices that were never deployed to are not displayed.

To open this page, select **Deploy > Jobs > Managed Devices**.

Table C-17 Managed Devices Page

Field	Description
Device Name/IP	The name or IP address of the device.
Status	The deployment status of the device.
Status Time	The date and time of the device deployment.
Job Name	The deployment job responsible for the device. Click this link to view a Job Details report about the device's deployment job.

Related Topics

- Deployment Wizard - Job Details Page, page C-9
- Viewing the Status of Devices, page 7-24
- Viewing the Job Details Report, page 7-20

Previews

The following topics describe the fields in the pages that are accessed from the Previews option:

- CLI Preview Page, page C-21
- CLI Preview Wizard, page C-23
- CLI Preview Details Page, page C-25

CLI Preview Page

Use this page to view all the CLI Preview job requests that were created and those that are currently being executed.

To open this page, do any of the following:

- Select **Deploy > Previews**.
- Click **Preview** in the Summary page of the CLI Preview wizard.

Table C-18 CLI Preview Page

Field	Description
Owner	The person who last saved the deployment job.
Deployment Group	The current deployment group.
Deployment Time	The time the last deployment occurred for the CLI Preview job.
Status	The status of the CLI Preview job—Pending, In Progress, Completed, or Failed.
Details	Click the Details icon for a preview job to open its Job Details report, in which you can view the status of devices related to the job.
Refresh	Click to force a manual update of the displayed data.
DNS Resolution	Click to view the results of a DNS host name resolution check for a selected preview job.
New Preview	Click to open the CLI Preview wizard for creating a new CLI Preview job.
View Preview Details	Click to open the CLI Preview Details page for the selected job.
Delete	Click to delete a selected CLI Preview job from the list.

Related Topics

- CLI Preview Wizard - Summary Page, page C-25
- CLI Preview Wizard, page C-23
- CLI Preview Details Page, page C-25
- Viewing the DNS Resolution, page 7-23
- Creating a CLI Preview Job, page 7-25
- Step 3: Confirming the Wizard Information for a CLI Preview Job, page 7-28
- Viewing the CLI Preview Jobs, page 7-28

CLI Preview Wizard

The following topics describe the pages of the CLI Preview wizard that guides you through the steps required to create a new CLI Preview job, for the devices in a deployment group.

The CLI Preview wizard contains the following pages:

- CLI Preview Wizard - Deployment Group Selection Page, page C-23
- CLI Preview Wizard - Device Selection and Preview Page, page C-24
- CLI Preview Wizard - Summary Page, page C-25

Related Topics

- Using QPM Wizards, page 3-10

CLI Preview Wizard - Deployment Group Selection Page

Use this page to select the deployment group to be previewed.

To open this page, do any of the following:

- In the CLI Preview page, click **New Preview**.
- In the CLI Preview wizard navigation menu, select **Deployment Group Selection**.

Table C-19 CLI Preview Wizard - Deployment Group Selection Page

Field	Description
Deployment Group	Select the deployment group whose devices you want to preview. Click the View list link to view a detailed list of all the current deployment groups.
Next button	Click to proceed to the next step of the wizard.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Deployment Groups List Page, page C-3
- CLI Preview Page, page C-21
- Step 1: Selecting the Deployment Group for a CLI Preview Job, page 7-26

CLI Preview Wizard - Device Selection and Preview Page

Use this page to see previews of the CLI commands for all the devices in your deployment group. These CLI previews are determined by querying the devices for their existing configuration and then calculating the incremental changes.

To open this page, do any of the following:

- In the Deployment Group Selection page of the CLI Preview wizard, click **Next**.
- In the CLI Preview Wizard navigation menu, select **Device Selection and Preview**.

Table C-20 CLI Preview Wizard - Device Selection and Preview Page

Field	Description
Device	Displays the device name or IP address.
Device Folder	Displays the name of the device folder.
Policy Configuration	Displays the current configuration for the device (Modified, No Changes). Click to open a Device Configuration Preview window that displays the configuration details of the selected device.
Back button	Click to return to the previous step of the wizard.
Next button	Click to proceed to the next step of the wizard.
Finish button	Click to complete the wizard. The Summary page appears.

Related Topics

- Device Configuration Preview Window, page C-8
- CLI Preview Wizard - Deployment Group Selection Page, page C-23
- Step 2: Previewing and Selecting the Devices for a CLI Preview Job, page 7-27

CLI Preview Wizard - Summary Page

Use this page to view and verify all the data collected by the wizard for the current deployment job.

To open this page, do any of the following:

- In the Device Selection and Preview page of the CLI Preview wizard, click **Next** or **Finish**.
- In the CLI Preview Wizard navigation menu, select **Summary**.

Table C-21 CLI Preview Wizard - Summary Page

Field	Description
Deployment group name	The name of the deployment group.
Number of devices to be previewed	The number of devices that were selected for previewing.
Back button	Click to go back through the CLI Preview wizard to make any changes that are required.
Preview button	Click this button to activate the preview job. The CLI Preview page appears.

Related Topics

- CLI Preview Page, page C-21
- CLI Preview Wizard - Device Selection and Preview Page, page C-24
- Step 3: Confirming the Wizard Information for a CLI Preview Job, page 7-28

CLI Preview Details Page

Use this page to view a detailed report for a selected CLI Preview job, including device status information.

To open this page, do any of the following:

- In the CLI Preview page, select a CLI preview and click **View Preview Details**.
- In the CLI Preview page, select a CLI Preview and click its **Details** icon.

Table C-22 CLI Preview Details Page

Field	Description
Job Name	The name of the preview job.
Deployment Group	The name of the deployment group.
Device Group	The name of the device group.
Owner	The person who last saved the preview job.
Creation Time	The date and time the CLI Preview job was created.
Job Description	A description of the preview job, if available.
Device Name/IP	Displays the device name or IP address.
Status	Displays the deployment status of the device.
Status Time	The time the device received its status.
Errors/Warnings	An error string, if available. In the case of a FAILED status, the CLI command that caused the error will also be displayed.
View CLI Commands	Click to view the CLI commands that were used to configure the device. A Device Configuration Preview window opens.

Related Topics

- Device Configuration Preview Window, page C-8
- CLI Preview Page, page C-21
- Creating a CLI Preview Job, page 7-25

Reports Tab Reference

The following topics describe the pages in the Reports tab. Topics are organized according to the following Reports tab options:

IP Telephony

The following topic describes the fields in the page that is accessed from the IP Telephony option:

Voice Ready Report Page

Use this page to view a report showing the readiness of the network for voice configuration. The report displays all the configurable and nonconfigurable devices in the current device group and deployment group.

To open this page, select **Reports > IP Telephony**.

Table D-1 Voice Ready Report Page

Field	Description
Sys Name	Displays the system name of the device. Click the Sys Name link for a device in the table to view details about the device. The Device Properties page appears for the selected device.
Primary Name	Displays the main IP address of the device.
Model	Displays the device model.
OS	Displays the version of the operating system on the device.
Mapped OS	Displays the mapped OS version that QPM assigned to the device.
Voice Status	Displays a check mark if the device is configured for voice. If the device is not configurable for voice, the field will remain blank.
Reason	Displays an explanation of why the device is not configurable for voice.

Related Topics

- Viewing and Editing Device Properties, page 4-14
- Viewing the Voice Ready Report, page 5-25
- Using QPM Tables, page 3-8

Upload

The following topics describe the fields in the pages that are accessed from the Upload option:

- Upload Reports Page, page D-3
- Upload Report, page D-4

Upload Reports Page

Use this page to select a report displaying the status of the process of uploading QoS configurations to QPM.

To open this page, do any of the following:

- Select **Reports > Upload**.
- Click **View** in the dialog box that opens after the Upload process starts.

Table D-2 Upload Reports Page

Field	Description
Start Date	Displays the date and time the upload process started.
Complete Date	Displays the date and time the upload process completed.
User Name	Displays the name of the user who ran the upload task.
Status	Displays the status of the upload process: • In progress—Upload process is in progress. You cannot view the Upload report if the status is In progress. • Completed—The Upload process has completed. You can view the Upload report. • Failed—QPM could not complete the upload process. The upload report displays the error.
View button	Click to view the Upload report with details of the selected upload task. See Upload Report, page D-4 for details.

Table D-2 Upload Reports Page (continued)

Field	Description
Delete button	Click to delete the selected upload report.
Refresh Rate	Select the rate at which the page refreshes with updated information.

Related Topics

- Uploading Device QoS Configurations to Policy Groups, page 6-16

Upload Report

The Upload report displays general information for the report, and for each uploaded device, the following two tables:

- Errors and warnings—Displays details about the information, warning, and error messages generated by the upload process.
- Uploaded policies—Displays information about the policy groups created by the upload process.

To open the Upload report, in the Upload Reports page, select an upload task and click **View**, or click on the Start Date link of the required report.

Table D-3 Upload Report - General Information

Field	Description
User Name	Displays the name of the user who ran the upload task.
Start Date	Displays the date and time the upload process started. Click to open the report for the corresponding upload task.
Complete Date	Displays the date and time the upload process completed.
Report Type	Displays the type of report—Upload.
Report Description	Displays the description of the report.

Table D-4 Upload Report - Errors and Warnings

Field	Description
#	Displays the error number.
Network Element	Displays the type of network element to which the error applies, if relevant.
Severity	Displays the severity of the error or warning.
QoS Feature	Displays the QoS feature to which the error applies.
Message	Displays the error message.
CLI Configuration	Displays the CLI command to which the message applies, if relevant.

Table D-5 Upload Report - Uploaded Policies

Field	Description
#	Displays the line number in the report table.
Policy Group Name	Displays the name of the policy groups.
Network Elements	Displays the network elements assigned to each policy group.
QoS Properties	Displays the number of QoS properties defined for each policy group.
In Policies	Displays the number of inbound policies for each policy group.
Out Policies	Displays the number of outbound policies for each policy group.

Related Topics

- Upload Reports Page, page D-3

Analysis

The following topics describe the fields in the pages that are accessed from the Analysis option:

Historical Monitoring Tasks Page

Historical monitoring tasks collect data for historical monitoring reports.

Use this page to:

- View historical monitoring reports.
- View, create, edit, delete, and stop historical monitoring tasks.
- Export collected data from tasks.

To open this page, Select **Reports > Analysis**.

When the historical QoS analysis data collected by QPM reaches the configured disk space limit, the following happens:

- All running monitoring tasks are stopped automatically, and are set to the status `Stopped due to out of disk space`.
- The next time you open the Historical Monitoring Tasks page, a message notifies you that the disk space limit was reached and provides recover instructions.

Note This message only appears on the Historical Monitoring Tasks page. You will not receive notification that the disk space limit was reached until you open this page.

All data collected before the tasks were stopped is available for display in reports. To free the necessary disk space and continue monitoring, you must delete the stopped tasks and run the database rebuild utility. Then you can recreate the deleted tasks to resume running them.

For instructions for recovering from running out of analysis disk space, see Freeing Disk Space for QoS Analysis, page 9-16.

Table D-6 Historical Monitoring Tasks Page

Field	Description
Check box column	Select check box to select its row.
Name column	Displays the task name.
Description column	Displays the task description.
Status column	Displays the task status. The following are the possible statuses: • Running—Task is running correctly and collecting data. • Stopped—Task was stopped by user request. • Stopped due to disk space limit—The amount of collected data reached the configured disk space limit. • Finished—The task successfully finished. It will not collect any more data.
View report button	Click to view a report of the selected task. The Matching and Dropped Traffic for Policies page appears.
Create button	Click to create a new task. The Task Definition page appears.
Edit button	Click to edit a task that is in an error status. The Task Definition page appears. You can edit tasks in the following statuses: • In progress—QPM is processing the task. Refresh the page until the status changes. • Error
Delete button	Click to delete the selected task. A confirmation dialog box appears.
Stop button	Click to stop a running task.

Table D-6 Historical Monitoring Tasks Page (continued)

Field	Description
Export Data button	Click to export a task's collected monitoring data to a CSV file. The browser file download process starts.
Refresh Rate list box	Select a page refresh rate from the list. The refresh rate determines how often the page refreshes with updated information.

Historical Monitoring Task Wizard

Use the Historical Monitoring Task wizard to create and edit historical monitoring tasks.

The Historical Monitoring Task wizard contains the following pages:

- Monitoring Task Wizard - Task Definition Page, page D-8
- Monitoring Task Wizard - Select Devices Page, page D-9
- Monitoring Task Wizard - Select Interfaces Page, page D-10
- Monitoring Task Wizard - Select Policies Page, page D-11
- Monitoring Task Wizard - Summary Page, page D-11

Monitoring Task Wizard - Task Definition Page

Use this page to define basic properties of the historical monitoring task.

To open this page, select **Reports > Analysis**. The Historical Monitoring Tasks page appears. Then do one of the following:

- To create a new task, click **Create**.
- To edit a task that is in an error status, select the check box next to the task name, then click **Edit**.

Table D-7 Monitoring Task Wizard - Task Definition Page

Field	Description
Check box column	Select check box to select its row.
Name field	Enter a task name.

Table D-7 Monitoring Task Wizard - Task Definition Page (continued)

Field	Description
Polling Interval list box	Select a polling interval, which is the frequency at which the task will poll data, in minutes.
Start Time and End Time controls	Enter task start and end times using the date and time fields. Optionally, select the calendar tool to select a date. Enter dates in mm/dd/yyyy format. Enter times in 24-hour format (for example, 06:00 is 6:00 a.m.). Each task has a maximum running duration that is based on the polling interval you select. These duration limits are listed in Performing Historical QoS Analysis, page 9-6. You cannot configure an end time that exceeds the maximum running duration of the polling interval you have selected.
Enabled check box	Select to enable the job immediately after finishing the task definition. Deselect to disable the task. The task will not begin collecting data until the configured start time, regardless of the status of the Enabled check box. If the Enabled check box is not selected, the task will not begin collecting data, even if the configured start time passes.
Enter a comment or description field	Enter a description of the task or a comment about it.
Back button	Click to return to the previous step.
Next button	Click to proceed to the next step.
Cancel button	Click to cancel task creation and exit the wizard.

Monitoring Task Wizard - Select Devices Page

Use this page to select the devices that contain the interfaces that you want to monitor.

To open this page, do one of the following:

- Click **Next** in the Monitoring Task Wizard - Task Definition Page.
- Select **Select Interfaces** from the wizard Navigation list.

Table D-8 Monitoring Task Wizard - Select Devices Page

Field	Description
Check box column	Select check box to select its row.
Sys Name column	Displays device sys name.
IP Address column	Displays device IP address.
Model column	Displays device model.
OS Version column	Displays device OS version.
Mapped OS Version column	Displays the mapped OS version that QPM assigned to the device.
Back button	Click to return to the previous step.
Next button	Click to proceed to the next step.
Cancel button	Click to cancel task creation and exit the wizard.

Monitoring Task Wizard - Select Interfaces Page

Use this page to select the interfaces that you want to monitor.

To open this page, do one of the following:

- Click **Next** in the Monitoring Task Wizard - Select Devices Page.
- Select **Select Interfaces** from the wizard Navigation list.

Table D-9 Monitoring Task Wizard - Select Interfaces Page

Field	Description
Check box column	Select check box to select its row.
Name column	Displays interface name.
Type column	Displays interface type.
Description column	Displays interface description.
Back button	Click to return to the previous step.
Next button	Click to proceed to the next step.
Cancel button	Click to cancel task creation and exit the wizard.

Monitoring Task Wizard - Select Policies Page

Use this page to select the policies that you want to monitor.

To open this page, do one of the following:

- Click **Next** in the Monitoring Task Wizard - Select Interfaces Page.
- Select **Select Policies** from the wizard Navigation list.

Table D-10 Monitoring Task Wizard - Select Policies Page

Field	Description
Direction column	Displays the direction of the policy (in or out).
Name column	Displays the policy name.
Description column	Displays the policy description.
Back button	Click to return to the previous step.
Next button	Click to proceed to the next step.
Cancel button	Click to cancel task creation and exit the wizard.

Monitoring Task Wizard - Summary Page

Use this page to view a summary of the monitoring task and determine whether to edit, finish, or cancel it.

To open this page, do one of the following:

- Click **Next** in the Monitoring Task Wizard - Select Policies Page.
- Select **Summary** from the wizard Navigation list.

Table D-11 Monitoring Task Wizard - Summary Page

Field	Description
Name	Displays task name.
Polling Interval(min)	Displays the task polling interval in minutes.
Start Time	Displays the task start time.
End Time	Displays the task end time.
Enabled check box	Indicates whether the job is enabled.

Table D-11 Monitoring Task Wizard - Summary Page (continued)

Field	Description
Description	Displays the task description.
Back button	Click to return to the previous step.
Next button	Click to proceed to the next step.
Finish button	Click to finish the wizard and create the task.
Cancel button	Click to cancel task creation and exit the wizard.

Historical Reports Pages

The following pages are accessible by launching a historical monitoring report:

- Policies Graphs: Matching and Dropped Traffic for Policies Page, page D-12
- Filters Graphs: Matching Traffic for Filter Conditions Page, page D-15
- Actions Graphs: Policy Actions on Matching Traffic Page, page D-17

The historical policy analysis graphs do not show the effect of traffic dropping for reasons other than QoS policy actions, such as dropping because of full queues. Therefore, it is possible that the traffic volume shown for an interface will be greater than the capacity of the interface. In this case, if you set the vertical axis to percentage, the traffic volume for the interface will exceed 100% of the interface's capacity.

Policies Graphs: Matching and Dropped Traffic for Policies Page

Use this page to view data that shows how much traffic matched the policies and whether it was transmitted or dropped. You can customize the page with the customization controls.

To open this page, do any of the following:

- Click **View Report** in the Historical Monitoring Tasks Page.
- Click **Policies Graphs** in any historical monitoring report page

Table D-12 Policies Graphs - Matching and Dropped Traffic for Policies Page

Field	Description
Graph Type list box	Select the graph type to display: • **Line—**Presents data in a line chart format. • **Bar—**Presents data in a bar chart format.
Units list box	Select the units to display in the graphs: • **Packets/second—**Displays data flow rates in packets per second. • **Bits/second—**Displays data flow rates in bits per second.
Vertical Axis list box	Select the vertical scale for graphs: • **Linear—**Displays the vertical scale of charts in linear format (the distance between units remains constant). • **Logarithmic—**Displays the vertical scale of charts in logarithmic format (the distance between units gets smaller as the total gets higher). • **Percentage—**Displays the vertical scale of charts as a percentage of the total bandwidth available on the interface.
Group list box	Select how to group the objects (interfaces and policies) that are displayed in the graphs: • **Policy**—Organizes the report according to policy groups. • **Interface**—Organizes the report according to interfaces.
From Time and To Time controls	Select the period of time you want to view in the report: • Enter dates in the first From Time and To Time fields in the format *mm*/*dd*/*yyyy*, or click the calendar icons to select dates from the Calendar dialog box. • Enter times in the second From Time and To Time fields in 24-hour format.
Apply button	Click to view only data collected during the period defined by the From Time and To Time controls.
Reset button	Click to reset the time period displayed in the From Time and To time controls to the collection period defined for the analysis task.

Table D-12 Policies Graphs - Matching and Dropped Traffic for Policies Page (continued)

Field	Description
Policy/Interface selection table	Select which policies or interfaces (depending on the selection in the Group list box) to display in the report by selecting the check box next to the policies or interfaces you want to view in the right pane of the report, then click **Show Graphs.**
Show Graphs button	Click to update the graphs to display the policies and interfaces selected using the policy-interface selection table
Matching Traffic Per Class Prior to QoS Actions graphs	Displays the traffic that matched each policy group's filters, before any policy actions were performed. This data is obtained from the CBQosMatchPrePolicy MIB variable.
Matching Traffic Per Class After QoS Actions	Displays the traffic that matched each policy group's filters and was transmitted (not dropped) by the configured QoS policies. This data is obtained as follows: • The bits data is obtained from the CBQosCMPostPolicyBitRate MIB variable. • The packets data is obtained by subtracting the CBQosCMDrop MIB variable from the CBQoSMatchPrePolicy MIB variable.
Matching Traffic Per Class Discarded by QoS Drop Actions	Displays the traffic that matched each policy group's filters and was dropped (not transmitted) by QoS policy drop actions. This data is obtained from the CBQosCMDrop MIB variable.
Policies Graphs button	Click to open the Policies Graphs: Matching and Dropped Traffic for Policies Page.
Filters Graphs button	Click to open the Filters Graphs: Matching Traffic for Filter Conditions Page
Actions Graphs button	Click to open the Actions Graphs: Policy Actions on Matching Traffic Page
Back to Task List button	Click to open the Historical Monitoring Tasks Page.

Filters Graphs: Matching Traffic for Filter Conditions Page

Use this page to view data that shows how matching traffic was distributed among the policy filter conditions. You can customize the page with the customization controls.

To open this page, click **Filters Graphs** in any historical monitoring report page.

Table D-13 Filters Graphs - Matching Traffic for Filter Conditions Page

Field	Description
Graph Type list box	Select the graph type to display: • **Line—**Presents data in a line chart format. • **Bar—**Presents data in a bar chart format.
Units list box	Select the units to display in the graphs: • **Packets/second—**Displays data flow rates in packets per second. • **Bits/second—**Displays data flow rates in bits per second.
Vertical Axis list box	Select the vertical scale for graphs: • **Linear—**Displays the vertical scale of charts in linear format (the distance between units remains constant). • **Logarithmic—**Displays the vertical scale of charts in logarithmic format (the distance between units gets smaller as the total gets higher). • **Percentage—**Displays the vertical scale of charts as a percentage of the total bandwidth available on the interface.
Group list box	Select how to group the objects (interfaces and policies) that are displayed in the graphs: • **Policy**—Organizes the report according to policy groups. • **Interface**—Organizes the report according to interfaces.

Table D-13 Filters Graphs - Matching Traffic for Filter Conditions Page (continued)

Field	Description
From Time and To Time controls	Select the period of time you want to view in the report: • Enter dates in the first From Time and To Time fields in the format *mm/dd/yyyy*, or click the calendar icons to select dates from the Calendar dialog box. • Enter times in the second From Time and To Time fields in 24-hour format.
Apply button	Click to view only data collected during the period defined by the From Time and To Time controls.
Reset button	Click to reset the time period displayed in the From Time and To time controls to the collection period defined for the analysis task.
Filters graphs	Displays how much traffic in each class matched each of the class' filters. Each graph includes a legend that shows the time period represented by each point on the poll time (horizontal) axis. The correlation between the filters shown in this graph and the filter rules configured in the policy is not exact. Whenever possible, QPM translates the filter rules configured in QPM to modular CLI match statements, but there are cases in which only ACL translation can reflect the filter definition, resulting in multiple filter rules being combined into one match statement (rules combined by OR become separate match statements; rules combined by AND are combined into one match statement). This data is obtained from the CBQoSMatchPrePolicy MIB variable.
Policies Graphs button	Click to open the Policies Graphs: Matching and Dropped Traffic for Policies Page.
Filters Graphs button	Click to open the Filters Graphs: Matching Traffic for Filter Conditions Page
Actions Graphs button	Click to open the Actions Graphs: Policy Actions on Matching Traffic Page
Back to Task List button	Click to open the Historical Monitoring Tasks Page.

Actions Graphs: Policy Actions on Matching Traffic Page

Use this page to view data that shows the policy actions that were taken on matching traffic. You can customize the page with the customization controls.

To open this page, click **Actions Graphs** in any historical monitoring report page.

Table D-14 Actions Graphs - Policy Actions on Matching Traffic Page

Field	Description
Graph Type list box	Select the graph type to display: • **Line—**Presents data in a line chart format. • **Bar—**Presents data in a bar chart format.
Units list box	Select the units to display in the graphs: • **Packets/second—**Displays data flow rates in packets per second. • **Bits/second—**Displays data flow rates in bits per second.
Vertical Axis list box	Select the vertical scale for graphs: • **Linear—**Displays the vertical scale of charts in linear format (the distance between units remains constant). • **Logarithmic—**Displays the vertical scale of charts in logarithmic format (the distance between units gets smaller as the total gets higher). • **Percentage—**Displays the vertical scale of charts as a percentage of the total bandwidth available on the interface.
Group list box	Select how to group the objects (interfaces and policies) that are displayed in the graphs: • **Policy**—Organizes the report according to policy groups. • **Interface**—Organizes the report according to interfaces.

Table D-14 Actions Graphs - Policy Actions on Matching Traffic Page (continued)

Field	Description
From Time and To Time controls	Select the period of time you want to view in the report: • Enter dates in the first From Time and To Time fields in the format *mm/dd/yyyy*, or click the calendar icons to select dates from the Calendar dialog box. • Enter times in the second From Time and To Time fields in 24-hour format.
Apply button	Click to view only data collected during the period defined by the From Time and To Time controls.
Reset button	Click to reset the time period displayed in the From Time and To time controls to the collection period defined for the analysis task.
Policy Actions graphs	See Policy Actions Graphs, page D-18.
Policies Graphs button	Click to open the Policies Graphs: Matching and Dropped Traffic for Policies Page.
Filters Graphs button	Click to open the Filters Graphs: Matching Traffic for Filter Conditions Page
Actions Graphs button	Click to open the Actions Graphs: Policy Actions on Matching Traffic Page
Back to Task List button	Click to open the Historical Monitoring Tasks Page.

Policy Actions Graphs

Policy actions graphs display information about traffic that was dropped because of policy actions. Only actions that are configured in a policy will appear in this page. For example, if a policy has queuing and policing actions assigned, only actions graphs for queuing and policing will appear.

The following actions can appear in the graphs:

- Policing—Displays the following traffic amounts:
  - Conformed—Traffic conformed to rate limit.

    This data is obtained from the CBQoSPoliceConformed MIB variable.
  - Exceeded—Traffic exceeded rate limit.

    This data is obtained from the CBQoSPoliceExceeded MIB variable.

  - Violated—Traffic violated rate limit.

    This data is obtained from the CBQoSPolicyViolated MIB variable.

- Queuing—Displays the amount of traffic dropped due to queuing.

  This data is obtained from the CBQoSQueuingDiscard MIB variable.

- WRED—Displays counts of the following per precedence level:
  - Random drop—Traffic exceeded minimum but was less than maximum count.

    This data is obtained from the CBQoSREDRandomDrop MIB variable.
  - Tail drop—Traffic exceeded maximum count.

    This data is obtained from the CBQoSREDTailDrop MIB variable.
  - Transmit counter—Traffic was transmitted.
- Traffic Shaping—Displays counts of the following:
  - Delayed traffic.
  - Traffic drop due to traffic shaping.

    This data is obtained from the CBQoSTSStatsDrop MIB variable.
- CAR action (nonmodular QoS)—Displays counts of the following:
  - Bytes/packets that conformed to rate limit.
  - Packets/bytes that exceeded rate limit.

Real-Time Monitoring Tasks Page

Real-time tasks define the data to display in a real-time monitoring report.

Use this page to:

- View real-time monitoring reports.
- View, create, edit, and delete real-time monitoring tasks.

To open this page, select **Reports > Analysis**. The Historical Monitoring Tasks page appears. Then select **Real-Time** from the TOC.

Table D-15 Real-Time Monitoring Tasks Page

Field	Description
Check box column	Select check box to select its row.
Name column	Displays task name.
Description column	Displays task description.
Status column	Displays task status. The only status that will appear is Ready to run, which indicates that the task is ready to run.
Run button	Click to run the selected task's report. A QoS Policy Manager - Real-Time Report window appears. You can run multiple real-time monitoring reports at the same time. Each appears in a separate report window.
Create button	Click to create a new task. The Real Time Monitoring Wizard - Device Selection page appears.
Edit button	Click to edit the selected task. The Real Time Monitoring Wizard - Device Selection page appears.
Delete button	Click to delete the selected task. A confirmation dialog box appears.
Refresh Rate list box	Select a page refresh rate from the list. The refresh rate determines how often the page refreshes with updated information.

Real-Time Monitoring Wizard

Use the Real-Time Monitoring wizard to create and edit historical monitoring tasks.

The Real-Time Monitoring wizard contains the following pages:

- Real-Time Monitoring Wizard - Device Selection Page, page D-21
- Real-Time Monitoring Wizard - Interface Selection Page, page D-21

Real-Time Monitoring Wizard - Device Selection Page

Use this page to define basic properties of the real-time monitoring task and select the device that contains the interface to monitor.

To open this page, select **Reports > Analysis**. The Historical Monitoring Tasks page appears. Then select **Real-Time** from the TOC. The Real-Time Monitoring Tasks page appears. Then do one of the following:

- To create a new task, click **Create**.
- To edit a task, select the check box next to the task name, then click **Edit**.

Table D-16 Real-Time Monitoring Wizard - Device Selection Page

Field	Description
Name field	Enter a task name.
Polling Interval list box	Select a polling interval, which is the frequency at which the task will poll data, in minutes.
Radio button column	Select a radio button to select its row.
Sys Name column	Displays device sys name.
IP Address column	Displays device IP address.
Model column	Displays device model.
OS Version column	Displays device OS version.
Mapped OS Version column	Displays the mapped OS version that QPM assigned to the device.
Enter a comment or description field	Enter a description of the task or a comment about it.
Next button	Click to proceed to the next step.
Cancel button	Click to cancel task creation and exit the wizard.

Real-Time Monitoring Wizard - Interface Selection Page

Use this page to select the interface that the task will monitor.

To open this page, click **Next** in the Real-Time Monitoring Wizard - Device Selection Page.

Table D-17 Real-Time Monitoring Wizard - Interface Selection Page

Field	Description
Radio button column	Select a radio button to select its row.
Name column	Displays interface name.
Type column	Displays interface type.
Description column	Displays interface description.
Back button	Click to return to the previous step.
Finish button	Click to finish the wizard and create the task. The task's report appears in the QoS Policy Manager - Real Time Report window.
Cancel button	Click to cancel task creation and exit the wizard.

QoS Policy Manager - Real Time Report Window

Use this window to view a real-time monitoring report.

To open this window, click **Run** in the Real-Time Monitoring Tasks Page.

The real-time policy analysis graphs do not show the effect of traffic dropping for reasons other than QoS policy actions, such as dropping because of full queues. Therefore, it is possible that the traffic volume shown for an interface will be greater than the capacity of the interface. In this case, if you set the vertical axis to percentage, the traffic volume for the interface will exceed 100% of the interface's capacity.

Table D-18 QoS Policy Manager - Real Time Report Window

Field	Description
Graph Type list box	Select the graph type to display: • **Line—**Presents data in a line chart format. • **Bar—**Presents data in a bar chart format.
Units list box	Select the units to display in the graphs: • **Packets/second—**Displays data flow rates in packets per second. • **Bits/second—**Displays data flow rates in bits per second.
Vertical Axis list box	Select the vertical scale for graphs: • **Linear—**Displays the vertical scale of charts in linear format (the distance between units remains constant). • **Logarithmic—**Displays the vertical scale of charts in logarithmic format (the distance between units gets smaller as the total gets higher). • **Percentage—**Displays the vertical scale of charts as a percentage of the total bandwidth available on the interface.
Task Name field	Displays the name of the task.
Task Start Time field	Displays the start time of the task (when the report was run).
Device field	Displays the IP address of the device that is monitored in the report.
Interface field	Displays the interface name of the interface that is monitored in the report.
Actual Polling Interval field	Displays the polling interval at which the task polls for data. This interval might be different than the polling interval configured for the task. If QPM is not able to poll at the interval configured for the task (due to network congestion, for example), it will determine the shortest interval at which it can poll, which is displayed in this field.
Policy selection controls	To select which policies to display in the report, select the check box next to the policies you want to view in the right pane of the report, then click **Show Graphs**.

Table D-18 QoS Policy Manager - Real Time Report Window (continued)

Field	Description
Show Graphs button	Click to display only the policies selected in the policy selection controls.
Close Window button	Click to close report window.
Matching Traffic for Policies graph	Displays the traffic that matched each policy group's filters, before any policy actions were performed. This data is obtained from the CBQosMatchPrePolicy MIB variable.
Post Traffic for Policies graph	Displays the traffic that matched each policy group's filters and was transmitted (not dropped) by the configured QoS policies. This data is obtained as follows: • The bits data is obtained from the CBQosCMPostPolicyBitRate MIB variable. • The packets data is obtained by subtracting the CBQosCMDrop MIB variable from the CBQoSMatchPrePolicy MIB variable.
Dropped Traffic for Policies graph	Displays the traffic that matched each policy group's filters and was dropped (not transmitted) by QoS policy drop actions. This data is obtained from the CBQosCMDrop MIB variable.

Table D-18 QoS Policy Manager - Real Time Report Window (continued)

Field	Description
Filters graphs	Displays how much traffic in each class matched each of the class' filters. Each graph includes a legend that shows the time period represented by each point on the poll time (horizontal) axis. The correlation between the filters shown in this graph and the filter rules configured in the policy is not exact. Whenever possible, QPM translates the filter rules configured in QPM to modular CLI match statements, but there are cases in which only ACL translation can reflect the filter definition, resulting in multiple filter rules being combined into one match statement (rules combined by OR become separate match statements; rules combined by AND are combined into one match statement). This data is obtained from the CBQoSMatchPrePolicy MIB variable.
Actions graphs	See Policy Actions Graphs, page D-25.

Policy Actions Graphs

Policy actions graphs display information about the effect of policy actions. Only actions that are configured in a policy will appear in this page. For example, if a policy has queuing and policing actions assigned, only actions graphs for queuing and policing will appear.

The following actions can appear in the graphs:

- Policing—Displays the following traffic amounts:
  - Conformed—Traffic conformed to rate limit.

    This data is obtained from the CBQoSPoliceConformed MIB variable.
  - Exceeded—Traffic exceeded rate limit.

    This data is obtained from the CBQoSPoliceExceeded MIB variable.
  - Violated—Traffic violated rate limit.

    This data is obtained from the CBQoSPolicyViolated MIB variable.

- Queuing—Displays the amount of traffic dropped due to queuing.

  This data is obtained from the CBQoSQueuingDiscard MIB variable.
- WRED—Displays counts of the following per precedence level:
  - Random drop—Traffic exceeded minimum but was less than maximum count.

    This data is obtained from the CBQoSREDRandomDrop MIB variable.
  - Tail drop—Traffic exceeded maximum count.

    This data is obtained from the CBQoSREDTailDrop MIB variable.
  - Transmit counter—Traffic was transmitted.
- Traffic Shaping—Displays counts of the following:
  - Delayed traffic.
  - Traffic drop due to traffic shaping.

    This data is obtained from the CBQoSTSStatsDrop MIB variable.
- CAR action (non modular QoS)—Displays counts of the following:
  - Bytes/packets that conformed to rate limit.
  - Packets/bytes that exceeded rate limit.

Import Policy Groups

The following topics describe the fields in the pages that are accessed from the Import Policy Groups option:

- Import Policy Groups Reports Page, page D-27
- Import Report, page D-28

Import Policy Groups Reports Page

Use this page to select a report displaying the status of the process of importing policies from a QPM 2.1.x export file. The QPM 2.1.x export file contains policy database information in XML format. QoS configurations to QPM.

To open this page, do any of the following:

- Select **Reports > Import Policy Groups**.
- Click **View** in the dialog box that opens after the Import process starts.

Table D-19 Import Policy Groups Report Page

Field	Description
Start Date	Displays the date and time the import process started.
Complete Date	Displays the date and time the import process completed.
User Name	Displays the name of the user who ran the import task.
Status	Displays the status of the import process: • In progress—Import process is in progress. You cannot view the Import report if the status is In progress. • Completed—The import process has completed. You can view the Import report. • Failed—QPM could not complete the import process. The import report displays the error.
View button	Click to view the Import report with details of the selected import task. See Import Report, page D-28 for details.
Delete button	Click to delete the selected import report.
Refresh Rate	Select the rate at which the page refreshes with updated information.

Related Topics

- Importing Policies from QPM 2.1.x, page 10-11

Import Report

The Import report displays general information for the report, and the following two tables:

- Errors and warnings—Displays details about the information, warning, and error messages generated by the import process.
- Imported policies—Displays information about the policy groups created by the import process.

To open the Import report, in the Import Policy Groups Reports page, select an import task and click **View**, or click on the Start Date link of the required report.

Table D-20 Import Report - General Information

Field	Description
User Name	Displays the name of the user who ran the import task.
Start Date	Displays the date and time the import process started. Click to open the report for the corresponding import task.
Complete Date	Displays the date and time the import process completed.
Report Type	Displays the type of report—Import.
Report Description	Displays the description of the report.

Table D-21 Import Report - Errors and Warnings

Field	Description
#	Displays the error number.
Configured on (in QPM 2.1.x)	Displays the device, or network element, or QPM 2.1 device group, for the configuration to which the error applies.
Policy Name (in QPM 2.1.x)	Displays the name of the policy in QPM 2.1.x to which the error applies. If the error applies to the properties defined for the device, or interface, or QPM 2.1 device group, this field is empty.
Severity	Displays the severity of the error or warning.
QoS Feature	Displays the QoS feature to which the error applies, if relevant.
Message	Displays the error message.

Table D-22 Import Report - Imported Policies

Field	Description
#	Displays the line number in the report table.
Policy Group Name	Displays the name of the policy groups.
Network Elements	Displays the network elements assigned to each policy group.
QoS Properties	Displays the number of QoS properties defined for each policy group.
In Policies	Displays the number of inbound policies for each policy group.
Out Policies	Displays the number of outbound policies for each policy group.

Related Topics

- Import Policy Groups Reports Page, page D-27

Conflicts

The following topics describe the fields in the pages that are accessed from the Conflicts option:

- FRTS Conflicts - Subinterfaces Page, page D-30
- FRTS Conflicts - DLCIs Page, page D-31
- Assignment Conflicts Reports Page, page D-32
- Assignment Conflicts Report, page D-33
- Verify Device Configuration Page, page D-34

FRTS Conflicts - Subinterfaces Page

FRTS conflicts occur when subinterfaces are assigned to policy groups configured with Frame Relay Traffic Shaping (FRTS), but their parent interfaces have not been defined with FRTS.

Use the FRTS Conflicts - Subinterfaces page to generate a report that displays the assigned FRTS subinterfaces with FRTS conflicts in policy groups in the current deployment group.

Note To ensure that these subinterfaces will be configured on deployment, configure the parent interfaces with FRTS, or remove the subinterface from the FRTS policy group assignment.

To open the FRTS Conflicts - Interfaces page, and generate a report, select **Reports > Conflicts**, then select **FRTS Subinterfaces** in the TOC.

Table D-23 FRTS Conflicts - Subinterfaces Page

Field	Description
Sys Name	Displays the system name of the device to which the frame relay subinterface belongs.
Name	Displays the name of the subinterfaces for which there is an FRTS conflict.
Type	Displays the types of interface to which the subinterface belongs.
Description	Displays the interface description.
Card Type	Displays the type of card on which the interface resides.
Rate	Displays the interface rates.
Device Folder	Displays the name of the device folder to which the device belongs.

Related Topics

- FRTS Conflicts - DLCIs Page, page D-31
- Configuring FRTS Policies, page 6-56

FRTS Conflicts - DLCIs Page

FRTS conflicts occur when DLCIs are assigned to policy groups configured with Frame Relay Traffic Shaping (FRTS), but their parent interfaces have not been defined with FRTS.

Use the FRTS Conflicts - DLCIs page to generate a report that displays the assigned FRTS DLCIs with FRTS conflicts in policy groups in the current deployment group.

Note To ensure that these DLCIs will be configured on deployment, configure the parent interfaces with FRTS, or remove the DLCI from the FRTS policy group assignment.

To open the FRTS Conflicts - DLCIs page, and generate a report, select **Reports > Conflicts**, then select **FRTS DLCIs** in the TOC.

Table D-24 FRTS Conflicts - DLCIs Page

Field	Description
Sys Name	Displays the system name of the device to which the DLCI belongs.
Name	Displays the name of the DLCI for which there is an FRTS conflict.
Interface Name	Displays the name of the parent interface of the DLCI.
Device Folder	Displays the name of the device folder to which the device belongs.

Related Topics

- FRTS Conflicts - Subinterfaces Page, page D-30
- Configuring FRTS Policies, page 6-56

Assignment Conflicts Reports Page

Assignment conflict reports are generated in the following cases:

- Devices with policy group assignments are moved from one device group to another, as a result of synchronization of privileges. QPM removes the network element assignments of these devices.
- The IOS version on a device with policy group assignments is changed, either manually in the Device Properties page or by a rediscovery. If the policy groups to which the device is assigned contain QoS configurations that are no longer supported by the device IOS, QPM removes the network element assignments of the device.

Use the Assignment Conflicts Reports page to select a report showing the network element assignment conflicts.

To open the Assignment Conflicts Reports page, select **Reports > Conflicts**, then select **Assignments** in the TOC.

Table D-25 Assignment Conflicts Reports Page

Field	Description
Start Date	Displays the date and time the report was generated.
Complete Date	Displays the date and time the report was completed.
User Name	Displays the name of the user who generated the report.
Status	Displays the status of the assignment report: • In progress—The report is being generated. You cannot view a report in progress. • Completed—The report is complete. You can view the report.
Report Type	Displays the type of report.
View button	Click to view details of the selected report. See Assignment Conflicts Report, page D-33 for details.
Delete button	Click to delete a report from the list.
Refresh Rate list box	Select the rate at which the page refreshes to obtain updated information.

Assignment Conflicts Report

The Assignment Conflicts report displays the network element assignments that were removed when the mapped OS version of devices changed, or when devices were moved from their device group following a sync operation.

To open the Assignment Conflicts report, select a report in the Assignment Conflicts Reports page, and click **View**.

Table D-26 Conflict Assignments Report

Field	Description
User Name	Displays the name of the user who made the changes that caused the report to be generated.
Start Date	Displays the date and time the report was generated.
Complete Date	Displays the date and time the report was completed.
Report Type	Displays the type of report—Conflict Assignments.
Report SubTitle	Displays the cause of assignment conflicts in the report.
Report Description	Displays the description of the report.
#	Displays the serial number of the assignment conflict.
Deployment Group Name	Displays the name of the deployment group with the assignment conflict.
Policy Group Name	Displays the name of the policy group with the assignment conflict.
Device Name	Displays the name of the device containing the network element whose assignment was removed.
Network Element Name	Displays the name of the network element whose assignment was removed.

Related Topics

- Assignment Conflicts Reports Page, page D-32

Verify Device Configuration Page

Use this page to view all the device configuration verification requests that were created and those that are currently being executed.

To open this page, do any of the following:

- Select **Reports > Conflicts > Verify Device Configuration**.
- Click **Verify** in the Summary page of the Device Configuration Verification wizard.

Table D-27 Verify Device Configuration Page

Field	Description
Owner	The person who last saved the deployment job.
Deployment Group	The current deployment group.
Deployment Time	The date and time the last device verification was initiated for the job.
Status	The status of the device verification job—Pending, In Progress, Completed, or Failed.
Details	Click the Details icon for a device verification job to open its Job Details report, in which you can view the status of devices related to the job.
Refresh	Click to force a manual update of the displayed data.
New Verification	Click to open the Device Configuration Verification wizard for creating a new device configuration verification job.
View Verification Details	Click to view the details of a device configuration verification job. The Job Verification Details page appears for the selected device configuration verification job.
Delete	Click to delete a selected device configuration verification job from the list.

Related Topics

- Device Configuration Verification Wizard - Summary Page, page D-38
- Device Configuration Verification Wizard, page D-36
- Job Verification Details Page, page D-35

- Creating a Device Configuration Verification Job, page 7-31
- Step 3: Confirming the Wizard Information for a Verification Job, page 7-33
- Viewing the Device Configuration Verification Jobs, page 7-33

Job Verification Details Page

Use this page to view a detailed report for a selected device configuration verification job, including device status information.

To open this page, do any of the following:

- In the Verify Device Configuration page, select a device configuration verification job, and click **View Verification Details**.
- In the Verify Device Configuration page, select a device configuration verification job and click its **Details** icon.

Table D-28 Job Verification Details Page

Field	Description
Job Name	Displays the name of the device configuration verification job.
Deployment Group	Displays the name of the deployment group.
Device Group	Displays the name of the device group.
Job Status	Displays the status of the device verification job—Pending, In Progress, Completed, or Failed.
Owner	Displays the name of the person who last saved the device configuration verification job.
Creation Time	Displays the date and time the device configuration verification job was created.
Job Description	Displays a description of the device configuration verification job, if available.
Device Name/IP	Displays the device name or IP address.
Status	Displays the deployment status of the device.
Status Time	Displays the time the device received its status.
Errors/Warnings	Displays an error string, if available. In the case of a FAILED status, the CLI command that caused the error will also be displayed.

Table D-28 Job Verification Details Page (continued)

Field	Description
Match/Mismatch	Displays “Match” if the configuration assigned to the device in the current deployment group is the same as the configuration on the device. Displays “Mismatch” if CLI changes were made on a device after deployment, indicating a mismatch between the deployment group and the device configuration.
View CLI Commands	Click to view the CLI commands that were used to configure the device. A Device Configuration Preview window opens.

Related Topics

- Device Configuration Preview Window, page C-8
- Verify Device Configuration Page, page D-34
- Creating a Device Configuration Verification Job, page 7-31

Device Configuration Verification Wizard

The following topics describe the pages of the Device Configuration Verification wizard that guides you through the steps required to create a new device configuration verification job, for the devices in a deployment group.

The Device Configuration Verification wizard contains the following steps:

- Device Configuration Verification Wizard - Deployment Group Selection Page, page D-37
- Device Configuration Verification Wizard - Device Selection and Preview Page, page D-37
- Device Configuration Verification Wizard - Summary Page, page D-38

Related Topics

Using QPM Wizards, page 3-10

Device Configuration Verification Wizard - Deployment Group Selection Page

Use this page to select the deployment group that contains the devices whose configurations you want to verify.

To open this page, do any of the following:

- In the Verify Device Configuration page, click **New Verification**.
- In the Device Configuration Verification wizard navigation menu, select **Deployment Group Selection**.

Table D-29 Device Configuration Verification Wizard - Deployment Group Selection Page

Field	Description
Deployment Group	Select the deployment group whose devices you want to verify. Click the View list link to view a detailed list of all the current deployment groups.
Next button	Click to move to the next step of the wizard.
Finish button	Click to move to the last step of the wizard.

Related Topics

- Deployment Groups List Page, page C-3
- Verify Device Configuration Page, page D-34
- Step 1: Selecting the Deployment Group for a Verification Job, page 7-31

Device Configuration Verification Wizard - Device Selection and Preview Page

Use this page to select the devices whose configurations you want to verify, and preview their configurations. This page displays a list of all the devices that are part of the selected deployment group.

To open this page, do any of the following:

- In the Deployment Group Selection page of the Device Configuration Verification wizard, click **Next**.
- In the Device Configuration Verification wizard navigation menu, select **Device Selection and Preview**.

Table D-30 Device Configuration Verification Wizard - Device Selection and Preview Page

Field	Description
Device	Displays the device name or IP address.
Device Folder	Displays the name of the device folder.
Policy Configuration	Displays the current configuration for the device (Modified, Unchanged Policies). Click to open a Device Configuration Preview window that displays the configuration details of the selected device.
Back button	Click to move to the previous step of the wizard.
Next button	Click to move to the next step of the wizard.
Finish button	Click to move to the last step of the wizard.

Related Topics

- Device Configuration Preview Window, page C-8
- Device Configuration Verification Wizard - Deployment Group Selection Page, page D-37
- Step 2: Previewing and Selecting the Devices for a Verification Job, page 7-32

Device Configuration Verification Wizard - Summary Page

Use this page to verify the deployment group name and the number of devices selected for verification.

To open this page, do any of the following:

- In the Device Selection and Preview page of the Device Configuration Verification wizard, click **Next** or **Finish**.
- In the Device Configuration Verification wizard navigation menu, select **Summary**.

Table D-31 Device Configuration Verification Wizard - Summary Page

Field	Description
Deployment group name	The name of the deployment group.
Number of devices to be verified	The number of devices that were selected for verification.
Back button	Click to go back through the wizard to make any changes that are required.
Verify button	Click this button to activate the verify job. The Verify Device configuration page appears.

Related Topics

- Verify Device Configuration Page, page D-34
- Device Configuration Verification Wizard - Device Selection and Preview Page, page D-37
- Step 3: Confirming the Wizard Information for a Verification Job, page 7-33

Restore

The following topic describes the fields in the page that is accessed from the Restore option:

- Restore Reports Page, page D-39

Restore Reports Page

Use this page to view a report of all the deployment group restore operations for the current device group.

To open this page, select **Reports > Restore**.

Table D-32 Restore Reports Page

Field	Description
Start Date	Displays the date the restore process started.
Complete Date	Displays the date the restore process completed.
User Name	Displays the name of the user who ran the restore process.
Status	Displays the status of the restore process for the device.
View button	Click to view details of a selected restore report. The Restore Validation Report window opens.
Delete button	Click to delete a selected restore report from the list.
Refresh Rate list box	Select the rate at which the page refreshes to obtain updated information.

Related topics

- Restore Validation Report Window, page C-5
- Restoring and Deploying a Historical Deployment Group, page 7-16

Admin Tab Reference

The following topics describe the pages in the Admin tab. Topics are organized according to the following Admin tab options:

Backup / Retrieve Backup

The following topics describe the fields in the pages that are accessed from the Backup/Retrieve Backup option:

Create Backup Page

Use the Create Backup page to do the following:

- Make a full or incremental backup.
- Schedule incremental backups.

To open this page, select **Admin > Backup/Retrieve Backup**, or select **Create Backups** in the Backup/Retrieve Backup TOC.

Table E-1 Create Backup Page

Field	Description
Backup Now	Select this check box to make a backup immediately.
Full	Select this radio button to make a full backup: • Backup Directory Path—Enter the full path of the full backup directory. You can make the backup on the QPM server, or on another computer, using a mapped network drive.
Incremental	Select this radio button to make an incremental backup in a system-defined location on the QPM server.
Schedule Incremental Backup	Select this check box to create a schedule for incremental backups.
Date	Enter the date for the first backup in the schedule.
Time	Enter the time of the first backup in the schedule.
Frequency	Select the frequency of the incremental backups: • Once—Make a backup only once at the scheduled date and time. • Daily—Make a backup daily from the scheduled date, at the scheduled time. • Weekly—Make a backup weekly at the scheduled time, on the same day of the week as the scheduled date.
Submit button	Click to start the backup process, and save the incremental backup schedule.

Related Topics

- Retrieve Full Backup Page, page E-3
- Retrieve Incremental Backup Page, page E-4
- Scheduled Backups Page, page E-6
- Making and Scheduling Backups, page 10-3

Retrieve Full Backup Page

Use this page to:

- Retrieve a full backup.
- View details of previous full backups.
- Delete a full backup.

To open this page, select **Admin > Backup/Retrieve Backup**, then select **Retrieve Full Backup** in the Backup/Retrieve Backup TOC.

Table E-2 Full Backup History Page

Field	Description
Backup Date and Time	Displays the date and time of the full backups.
Login Name	Displays the login name of the user who made the full backup.
Backup Path	Displays the full path of the full backup.
Status	Displays the status of the full backup—whether the backup succeeded or failed.
Retrieve Backup button	Click to retrieve the selected full backup. The retrieved data overwrites current QPM data on the QPM server. The Retrieved Backup History page appears. **Note** You must restart the QPM server after retrieving a backup. **Caution** You should use the QPM Retrieve feature with care.
Delete button	Click to delete the full backup files.

Related Topics

- Create Backup Page, page E-2
- Retrieved Backup History Page, page E-5
- Viewing Backup History, page 10-4

Retrieve Incremental Backup Page

Use this page to:

- Retrieve incremental backups.
- View details of previous incremental backups.
- Delete all incremental backup.

To open this page, select **Admin > Backup/Retrieve Backup**, then select **Retrieve Incremental Backup** in the Backup/Retrieve Backup TOC.

Table E-3 Incremental Backup History Page

Field	Description
Backup Date and Time	Displays the date and time of the incremental backups.
Login Name	Displays the login name of the user who made the incremental backup.
Status	Displays the status of the incremental backup—whether the backup succeeded or failed.
Retrieve Backup button	Click to retrieve the selected incremental backup. QPM uses all the previous incremental backup files to recreate the database. The retrieved data overwrites current QPM data on the QPM server. The Retrieved Backup History page opens. **Note** You must restart the QPM server after retrieving a backup. **Caution** You should use the QPM Retrieve feature with care.
Delete All button	Click to delete all incremental backup files. You cannot delete an individual incremental file because all incremental files are required when retrieving an incremental backup.

Related Topics

- Create Backup Page, page E-2
- Retrieved Backup History Page, page E-5
- Viewing Backup History, page 10-4

Retrieved Backup History Page

Use this page to view retrieved full and incremental backups.

To open this page, select **Admin > Backup/Retrieve Backup**, then select **Retrieved Backup History** in the Backup/Retrieve Backup TOC.

Table E-4 Retrieve Backup History Page

Field	Description
Retrieve Date and Time	Displays the date and time of the retrieved backups.
Login Name	Displays the login name of the user who retrieved the backup.
Backup Type	Displays the type of backup—full or incremental.
Status	Displays the status of the retrieved backup—whether the retrieve operation succeeded or failed.
Info	• For full backups—Displays the path of the backup file. • For incremental backups—Displays the time the incremental backup was made.
Delete button	Click to delete the selected row in the table.

Related Topics

- Retrieve Full Backup Page, page E-3
- Retrieve Incremental Backup Page, page E-4
- Viewing Retrieved Backup History, page 10-7

Scheduled Backups Page

Use this page to:

- View the next scheduled backup for each incremental backup schedule.
- Delete an entire schedule.

To open this page, select **Admin > Backup/Retrieve Backup**, then select **Scheduled Backups** in the Backup/Retrieve Backup TOC.

Table E-5 Scheduled Backups Page

Field	Description
Next Backup	Displays the date and time of the next backup in each schedule.
Schedule Type	Displays the type of schedule—once only, daily, or weekly.
Delete Schedule	Click to delete the entire schedule to which the selected backup belongs.

Related Topics

- Create Backup Page, page E-2
- Viewing and Deleting Backup Schedules, page 10-9

Audit

The following topics describe the fields in the pages that are accessed from the Audit option:

- Audit Trail Policy Groups/Policies Page, page E-7
- Audit Trail Deployment Group Actions Page, page E-8
- Audit Trail Library Components Page, page E-9
- Audit Trail General Logs Page, page E-10
- Audit Calendar Dialog Box, page E-11

Audit Trail Policy Groups/Policies Page

Use this page to view changes made to policy groups and policies in a deployment group.

To open this page, do any of the following:

- Select **Admin > Audit**.
- Select **Policy Groups** in the Audit TOC.

Table E-6 Audit Trail Policy Groups/Policies Page

Field	Description
Deployment Group	Select the deployment group for which you want to view audit logs.
No.	Displays the audit log number.
Date	Displays the modification date.
Time	Displays the modification time.
Login Name	Displays the login name of the user that made the changes.
Message	Describes the modification that was made.
Item	Displays the type of item that was modified. Click the link to view a summary of the modified item.
Modification	Displays the type of modification that was made, for example whether a new item was created, or an existing item was modified or deleted.
Clear button	Click to clear old audit logs. A Calendar dialog box opens. See Audit Calendar Dialog Box, page E-11.

Related Topics

- General Page (Policy Group and Template), page B-17
- Policy Summary Page, page B-34
- Audit Trail Deployment Group Actions Page, page E-8
- Audit Trail Library Components Page, page E-9
- Audit Trail General Logs Page, page E-10

Audit Trail Deployment Group Actions Page

Use this page to view actions performed on a deployment group. These actions include uploading policy groups, importing policy groups, deployment, saving and restoring historical versions, and so on.

To open this page, select **Deployment Groups** in the Audit TOC.

Table E-7 Audit Trail Deployment Group Actions Page

Field	Description
Deployment Group	Select the deployment group for which you want to view audit logs.
No.	Displays the audit log number.
Date	Displays the modification date.
Time	Displays the modification time.
Login Name	Displays the login name of the user that made the changes.
Message	Describes the modification that was made.
Action	Displays the action that was performed. Click the action to open the corresponding Reports page.
Clear button	Click to clear old audit logs. A Calendar dialog box opens. See Audit Calendar Dialog Box, page E-11.

Related Topics

- Import Policy Groups Reports Page, page D-27
- Upload Reports Page, page D-3
- Job Details Report Page, page C-17
- Audit Trail Policy Groups/Policies Page, page E-7
- Audit Trail Library Components Page, page E-9
- Audit Trail General Logs Page, page E-10

Audit Trail Library Components Page

Use this page to view changes made to global library items—IP aliases, application aliases, and policy group templates.

Note System-created templates do not appear in the Audit logs.

To open this page, select **Libraries** in the Audit TOC.

Table E-8 Audit Trail Library Components Page

Field	Description
No.	Displays the audit log number.
Date	Displays the modification date.
Time	Displays the modification time.
Login Name	Displays the login name of the user that made the changes.
Message	Describes the modification that was made.
Item	Displays the type of item that was modified. For policy group templates, click the link to view a summary of the modified item.
Modification	Displays the type of modification that was made, for example whether a new item was created, or an existing item was modified or deleted.
Clear button	Click to clear old audit logs. A Calendar dialog box opens. See Audit Calendar Dialog Box, page E-11.

Related Topics

- General Page (Policy Group and Template), page B-17
- Audit Trail Policy Groups/Policies Page, page E-7
- Audit Trail Deployment Group Actions Page, page E-8
- Audit Trail General Logs Page, page E-10

Audit Trail General Logs Page

Use this page to view actions on device inventory items, for example, rediscovery.

To open this page, select **General** in the Audit TOC.

Table E-9 Audit Trail General Logs Page

Field	Description
No.	Displays the audit log number.
Date	Displays the modification date.
Time	Displays the modification time.
Login Name	Displays the login name of the user that made the changes.
Message	Describes the modification that was made.
Item	Displays the type of item that was modified.
Clear button	Click to clear old audit logs. A Calendar dialog box opens. See Audit Calendar Dialog Box, page E-11.

Related Topics

- Audit Trail Policy Groups/Policies Page, page E-7
- Audit Trail Deployment Group Actions Page, page E-8
- Audit Trail Library Components Page, page E-9

Audit Calendar Dialog Box

Use the Calendar dialog box to specify the date up to which you want to delete Audit logs.

The Calendar dialog box opens after you click **Clear** in an Audit page.

Table E-10 Audit Calendar Dialog Box

Field	Description
Date Navigation	Use the navigation arrows above the calendar table to navigate through the calendar.
Calendar Table	In the calendar table, choose the date to which you want to delete logs. The audit logs before and including the selected date are deleted.

Related Topics

- Audit Trail Policy Groups/Policies Page, page E-7
- Audit Trail Deployment Group Actions Page, page E-8
- Audit Trail Library Components Page, page E-9
- Audit Trail General Logs Page, page E-10

Import Policy Groups

The following topics describe the fields in the pages that are accessed from the Import Policy Groups option:

- Import Policy Groups From 2.1 Page, page E-12
- Import Policy Groups - Device Selection Page, page E-13
- Import Dialog Box, page E-14

Import Policy Groups From 2.1 Page

Use this page to import policies from a QPM 2.1.x database that was previously exported to XML format. The policies are imported into policy groups, according to the network elements on which they were configured.

Note To import devices from a QPM 2.1.x database, use the Import devices from 2.1.x option. See Import Devices Wizard, page A-22.

To open this page, select **Admin > Import Policy Groups**.

Table E-11 Import Policy Groups From 2.1 Page

Field	Description
Select Deployment Group	Select the deployment group into which to import the policy groups.
Import file path (xml)	Enter the full path of the XML file to import, or click the Browse button and select the XML file.
OK button	Click OK to continue the Import process. The Import Policy Groups - Device Selection page appears.

Related Topics

- Import Policy Groups - Device Selection Page, page E-13
- Importing Policies from QPM 2.1.x, page 10-11

Import Policy Groups - Device Selection Page

Use this page to select the devices you want to assign to imported policy groups.

This page appears when you complete the Import Policy Groups From 2.1 page and click **OK**.

Table E-12 Import Policy Groups - Device Selection Page

Field	Description
Sys Name	System name of device.
Primary Device Name	The main IP address or hostname of the device.
Model	Device model.
OS Version	Version of the operating system on the device.
Mapped OS Version	OS version that QPM uses to determine QoS capabilities that can be configured.
Status	Status of the device.
Device Folder	Device folder to which the device belongs.
Import Policies button	Click to start the import operation. A dialog box opens informing you that the import operation has started. See Import Dialog Box, page E-14.

Related Topics

- Import Policy Groups From 2.1 Page, page E-12
- Importing Policies from QPM 2.1.x, page 10-11

Import Dialog Box

Use this dialog box to go to the Import Policy Groups Reports page, or continue editing policies, after the import operation has started.

Table E-13 Import Dialog Box

Field	Description
View button	Click to display the Import Policy Groups Reports page.
Continue button	Click to display the Policy Groups page to continue editing policy groups and policies.

Related Topics

- Import Policy Groups - Device Selection Page, page E-13
- Importing Policies from QPM 2.1.x, page 10-11
- Import Policy Groups Reports Page, page D-27
- Policy Groups Page, page B-14

SNMP Parameter/Properties Page

Use this page to change the default SNMP settings for devices in the QPM inventory.

To open this page, select **Admin > SNMP**.

Table E-14 SNMP Parameter/Properties Page

Field	Description
Timeout	The amount of time the system should wait for a device to respond before trying to access it again.
Retries	The number of times the system tries to access devices.
Min Thread Number	The minimum number of SNMP requests that can processed concurrently.

Table E-14 SNMP Parameter/Properties Page (continued)

Field	Description
Max Thread Number	The maximum number of SNMP requests that can processed concurrently.
Save button	Click to save the displayed SNMP settings.

CLI Command Reference for QPM Actions

QPM uses device commands to configure your QoS policies and configurations on the devices. These are the same commands you can use on the device's command line interface (CLI), and they are described in the device's documentation.

This section shows the command sequences used to configure each type of abstract policy action that you can create using QPM. You can use this information to help you understand how QPM configures your devices. See the device's documentation for complete information on the commands and their parameters. (See More Information About Quality of Service, page 2-30 for a partial list of product documentation.)

These sections show the full command translation, including optional parameters. If you do not configure an optional setting, the associated command or parameter is not included in the command sequence QPM uses to configure the device.

Note The notation in the translation is **bold** for the device's key words, *italic* for variables. Some of the variables are parameters you enter into QPM. Other variables are managed by QPM, for example, the ACL number.

These sections describe QPM abstract actions:

Access List Configuration

When you create filters for non class-based policies, QPM translates the filter definitions to ACLs using this command sequence:

- **access-list** *acl-index* {**deny | permit**} *protocol source source-wildcard* [{**eq** *src-port* | **range** *src-port-from src-port-to*}] *destination destination-wildcard* [{**eq** *dest-port* | **range** *dest-port-from dest-port-to*}] [**precedence** *precedence*] [**dscp** *dscp*]

Named ACL

When you create filters for class-based policies, QPM uses this command sequence to configure ACLs on the device, if it supports filter names:

1. **ip access-list extended** *name*
2. **deny | permit** *protocol source source-wildcard* [{**eq** *src-port* | **range** *src-port-from src-port-to*}] *destination destination-wildcard* [{**eq** *dest-port* | **range** *dest-port-from dest-port-to*}] [**precedence** *precedence*] [**dscp** *dscp*]

Class-Based QoS Configuration

When you select Class Based QoS as a QoS property, and create class-based queuing policies on the interface, QPM uses this command sequence to configure the device:

1. **access-list** *ACLNum filter*
2. **class-map [match all | match any]** *classname*
   a. **match [not] access-group** *ACLNum*
   b. **match [not] ip dscp** *dscp*
   c. **match [not] ip precedence** *precedence*
   d. **match [not] cos** *cos*
   e. **match [not] ip rtp** *low_port range*
   f. **match [not] protocol** *protocol* [*parametername* [*value*]]
   g. **match [not] class-map** *classname*
   h. **match [not] mpls experimental** *value*
3. **policy-map** *policy-map-name*
   a. **class** {*classname* | **class-default**}

      set ip precedence *precedence*

      set ip dscp *dscp*

      set cos *cos-value*

      set fr-de

      set mpls experimental *value*

      police *police-rate* [*police-bc*] [**pir** *pir*] [**be** *police-be*] **conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]

      where *action* is:

      {**transmit** | **continue** | **set-prec-transmit** *precedence* | **set-dscp-transmit** *dscp* | **set-prec-continue** *precedence* | **set-dscp-continue** *dscp* | **drop**}

      shape average *shape-rate* [*shape-bc shape-be*]

      shape peak *shape-rate* [*shape-bc shape-be*]

shape adaptive *shape-adaptive-rate*

shape fecn-adapt

bandwidth *bandwidth*

bandwidth percent *percent*

priority *bandwidth* [*burst*]

priority percent *percent* [*burst*]

fair queue *number-of queues*

fair queue queue-limit *individual-queue-limit*

queue-limit *queue-limit*

random-detect (see WRED Configuration, page F-11 for the random-detect commands)

4. **interface** *interfacename*
   a. **service-policy** *direction policy-map-name*

Note Some commands are for class-based QoS on a device that supports NBAR or IPRTP.

On ATM VCs, this command sequence is used:

1. **interface** *interfacename*
2. **pvc** *pvc-name*
   a. **service-policy** *direction policy-map-name*

On frame-relay interfaces, this command sequence is used:

1. **map-class frame-relay** *classname*
   a. **service-policy [input | output]** *policyname*
2. **interface** *interfacename*
   a. **frame-relay class** *classname*

Class-Based QoS Marking

When you select Class Based QoS as a QoS property, and create marking policies on the interface, QPM uses this command sequence to configure the device:

1. **policy-map** *policy-map-name*
   a. **class** *classname*

      set ip precedence *precedence*

      set ip dscp *dscp*

      set cos *cos-value*

      set fr-de

      set mpls experimental *value*

Class-Based QoS Policing

When you select Class Based QoS as a QoS property, and create policing policies on the interface, QPM uses this command sequence to configure the device:

1. **policy-map** *policy-map-name*
   a. **class** *classname*

      police *police-rate* [*police-bc*] [**pir** *pir*] [**be** *police-be*] **conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]

      where *action* is:

      {**transmit** | **continue** | **set-prec-transmit** *precedence* | **set-dscp-transmit** *dscp* | **set-prec-continue** *precedence* | **set-dscp-continue** *dscp* | **drop**}

Class-Based QoS Shaping

When you select Class Based QoS as a QoS property, and create shaping policies on the interface, QPM uses this command sequence to configure the device:

1. **policy-map** *policy-map-name*
   a. **class** *classname*

      shape average *shape-rate* [*shape-bc shape-be*]

      shape peak *shape-rate* [*shape-bc shape-be*]

      shape adaptive *shape-adaptive-rate*

      shape fecn-adapt

Modular Shaping

When you select modular shaping as a QoS property, and create shaping policies, QPM uses this command sequence to configure the device:

1. **policy-map** *out_policies*

   CLI out_policies configuration
2. **policy-map** *policy-map-name*

   class class-default
   a. **shape** {**average | peak**} *shape-rate* [*shape-bc shape-be*]

      shape adaptive *shape-adaptive-rate*

      shape fecn-adapt
   b. **service-policy** *out_policies*
3. **interface** *interfacename*

   service-policy output *policy-map-name*

FIFO Queuing Configuration

When you select FIFO as a QoS property, QPM uses this command sequence to configure the device:

1. **interface** *interfacename*
2. **no fair-queue**

WFQ Configuration

When you select WFQ as a QoS property, QPM uses this command sequence to configure the device:

1. **interface** *interfacename*
2. **fair-queue**

WFQ on VIP Cards (DWFQ with QoS Group) Configuration

When you select WFQ or FQ as a QoS property, and that interface is on a VIP card, QPM uses this command sequence to configure the device:

1. **access-list** *ACLNum condition*
2. **rate-limit input access-group** *ACLNum rate bc be* **conform-action set-qos-transmit** *qos-group-num* **exceed-action set-qos-transmit** *qos-group-num*
3. **interface** *interfacename*
4. **fair-queue qos-group**
5. **fair-queue qos-group** *qos-group* **weight** *weight*
6. **fair-queue qos-group** *qos-group* **limit** *limit*
7. **fair-queue aggregate-limit** *aggregate-packet*
8. **fair-queue individual-limit** *individual-packet*

FRTS Configuration

When you enable Frame Relay traffic shaping (FRTS) on an interface, QPM uses this command sequence to configure the device:

1. **map-class frame-relay** *classname*
2. **frame-relay cir** *cir*
3. **frame-relay mincir** min*cir*
4. **frame-relay bc** *bc*
5. **frame-relay be** *be*
6. **frame-relay adaptive-shaping** {**becn | foresight**}
7. **frame-relay ip rtp priority** *low range bandwidth*
8. **no frame-relay adaptive shaping**
9. **no frame-relay** {**adaptive-shaping becn | adaptive-shaping foresight**}
10. **interface** *interfacename*
    a. **frame-relay traffic-shaping**
    b. **frame-relay class** *classname*
    c. **frame-relay ip rtp header-compression [passive]**

Note If you are using FRTS with different queuing types, additional commands are available. See the relevant queuing commands for information about these commands.

If you are using FRTS on DLCI, the following commands are used:

- **interface** *interfacename*
  - **frame-relay traffic-shaping**
  - **frame-relay interface-dlci** *dlci-name*
  - **class** *classname*

WFQ with FRTS Configuration

When you select WFQ as a QoS property, and you enable Frame Relay traffic shaping (FRTS) on an interface, QPM uses this command sequence to configure the device:

1. **map-class frame-relay** *classname*
2. **frame-relay fair-queue** *congestive-discard-threshold number-dynamic-conversation-queues number-reservable-conversation-queues max-buffer-size-for-fair-queues*
3. **interface** *interfacename*
4. **frame-relay traffic-shaping**
5. **frame-relay class** *classname*

FRTS with FRF.12 (Voice Configuration) Configuration

When you enable Frame Relay traffic shaping (FRTS) on an interface, and configure the voice fields, QPM uses this command sequence to configure the device:

1. **map-class frame-relay** *classname*
2. **frame-relay fragment** *fragment-size*
3. **frame-relay voice bandwidth** *bps-reserved*
4. **interface** *interfacename*
5. **frame-relay traffic-shaping**
6. **frame-relay class** *classname*

WRED Configuration

When you select WRED as a QoS property, or select WRED for the drop mechanism for a class-based policy or interface QoS property, QPM uses this command sequence to configure the device:

1. **interface** *interfacename*
2. **random-detect** *weight*

When you use advanced WRED the following commands are also available:

- **random-detect**
- **random-detect exponential-weighting-constant** *weight*
- **random-detect precedence** {*precedence* | **rsvp**} *min-threshold max-threshold probability-denominator*

Priority Queuing Configuration

When you select Priority Queuing as a QoS property, and create priority queuing policies on the interface, QPM uses this command sequence to configure the device (except for Frame Relay interfaces on which you have enabled FRTS):

1. **access-list** *ACLNum filter*
2. **priority-list** *priorityNum* **protocol ip** *level* **list** *ACLNum*
3. **priority-list** *priorityNum* **default** *level*
4. **priority-lis**t *priorityNum* **queue-limit** *high-limit medium-limit normal-limit low-limit*
5. **interface** *interfacename*
6. **priority-group** *priorityNum*

If the interface is Frame Relay using FRTS, QPM uses this command sequence to configure the device:

1. **map-class frame-relay** *classname*
2. **frame-relay priority-group** *priorityNum*
3. **interface** *interfacename*
4. **frame-relay class** *classname*

Custom Queuing Configuration

When you select Custom Queuing as a QoS property, and create custom queuing policies on the interface, QPM uses this command sequence to configure the device (except for Frame Relay interfaces on which you have enabled FRTS):

1. **access-list** *ACLNum filter*
2. **queue-list** *qListNum* **protocol ip** *qNum* **list** *ACLNum*
3. **queue-list** *qListNum* **queue** *qNum* **byte-count** *bytes* [**limit** *limit*]
4. **queue-list** *qListNum* **default** *qNum*
5. **interface** *interfacename*
6. **custom-queue-list** *qListNum*

If the interface is Frame Relay using FRTS, QPM uses this command sequence to configure the device:

1. **map-class frame-relay** *classname*
2. **frame-relay custom-queue-list** *qListNum*
3. **interface** *interfacename*
4. **frame-relay class** *classname*

Weighted Round-Robin (WRR) Policies

When you create queue weight policies for a layer 3 switch, QPM uses this command sequence to configure the device:

1. **qos switching**
2. **qos mapping** [**source** *Fastethernet name*] [**destination** *Fastethernet name*] **precedence** *precedence* **wrr-weight** *weight*

NBAR Port Map Configuration

When you enable NBAR port mapping, QPM uses this command sequence to configure the device:

- **ip nbar port-map** *protocol* {**tcp | udp**} *portnumbers*

RSVP Configuration

When you enable resource reservation protocol (RSVP), QPM uses this command sequence to configure the device:

1. **ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*]]
2. **ip rsvp udp-multicast**

IP RTP Priority Configuration

When you enable IP RTP priority, QPM uses this command sequence to configure the device:

- **ip rtp priority** *start-port port-range bandwidth*

CRTP Configuration

When you enable CRTP (RTP header compression), QPM uses this command sequence to configure the device:

1. **interface** *interfacename*
2. **ip rtp header-compression [passive]**

If the interface is Frame Relay, QPM uses this command sequence to configure the device:

- **frame-relay ip rtp header-compression [passive]**

LFI Configuration

When you enable LFI, QPM uses this command sequence to configure the device:

1. **interface** *interfacename*
2. **ppp multilink interleave**
3. **ppp multilink fragment-delay** *delay*

TX-Ring Configuration

When you enable a TX-ring limit on a PVC, QPM uses this command sequence to configure the device:

1. **interface** *interfacename*
2. **pvc** *pvc-name*
3. **tx-ring-limit** *ring-limit*

Inline Power

When you enable inline power, QPM uses this command sequence to configure the device:

- **set port inlinepower** *ports-list* auto

Access Control Policies

When you create access control policies, QPM uses this command sequence to configure the device:

1. **access-list** *ACLNum filter*
2. **interface** *interfacename*
3. **ip access-group** *ACLNum direction*

Router Marking Policies (PBR)

When you create marking policies, QPM uses this command sequence to configure the device:

1. **access-list** *ACLNum filter*
2. **route-map** *tag* **permit** [*sequence*]
3. **match ip address** *ACLNum*
4. **set ip precedence** *precedence*
5. **interface** *interfacename*
6. **ip policy route-map** *tag*

Policing Policies (CAR)

When you create policing policies, QPM uses this command sequence to configure the device:

1. **access-list** *ACLNum filter*
2. **interface** *interfacename*
3. **rate-limit** {**input** | **output**} **access-group** *ACLNum rate bc be* **conform-action** {**transmit** | **continue** | **set-prec-transmit** *precedence* | **set-dscp-transmit** *dscp* | **set-prec-continue** *precedence* | **set-dscp-continue** *dscp* | **drop**} **exceed-action** {**transmit** | **continue** | **set-prec-transmit** *precedence* | **set-dscp-transmit** *dscp* | **set-prec-continue** *precedence* | **set-dscp-continue** *dscp* | **drop**}

Shaping Policies (GTS)

When you create shaping policies, QPM uses this command sequence to configure the device:

1. **access-list** *ACLNum filter*
2. **interface** *interfacename*
3. **traffic-shape group** *ACLNum rate [bc be]*

Catalyst 5000 Marking Policies

When you create marking policies for a Catalyst 5000 family switch, QPM uses this command sequence to configure the device:

1. **set qos enable**
2. **set qos ip-filter** *precedence protocol source source-port destination destination-port*

Catalyst 6000 2Q2T and 1P2Q2T Queuing Configuration

When you configure 2Q2T and 1P2Q2T queuing for a Catalyst 6000 family switch, QPM uses this command sequence to configure the device:

1. **set qos enable**
2. **set qos map 1p2q2t | 2q2t tx** *queue-number threshold-number* **cos** *cos-list*
3. **set qos drop-threshold 2q2t tx queue** *queue-number threshold-1 threshold-2*
4. **set qos wrr 1p2q2t | 2q2t** *queue-weight-1 queue-weight-2*
5. **set qos txq-ratio 1p2q2t | 2q2t** *queue-ratio-1 queue-ratio-2 [queue-ratio-3]*
6. **set qos wred 1p2q2t tx queue** *queue-number threshold-1 threshold-2*

Catalyst 6000 CoS, Precedence, DSCP, and DSCP Markdown Mapping

When you configure these mapping settings for a Catalyst 6000, QPM uses this command sequence to configure the device:

1. **set qos cos-dscp-map** *dscp dscp dscp dscp dscp dscp dscp dscp*
2. **set qos dscp-cos-map** *dscp, dscp, dscp, dscp, dscp, dscp, dscp, dscp:cos*
3. **set qos ipprec-dscp-map** *dscp dscp dscp dscp dscp dscp dscp dscp*

4. **set qos policed-dscp-map** *dscp, dscp, dscp, dscp, dscp, dscp, dscp, dscp:dscp*
5. **set qos policed-dscp-map excess-rate** *dscp, dscp, dscp, dscp, dscp, dscp, dscp, dscp:dscp*

Catalyst 6000 Port Configuration

When you configure the trust state for a Catalyst 6000 family switch port, QPM uses this command sequence to configure the device:

1. **set port qos** *module/port* **trust** {**trust-cos | trust-ipprec | trust-dscp**}
2. **set port qos** *module/port* **trust-ext** {**trust-cos | untrusted**}
3. **set port qos** *module/port* {**port-based | vlan-based**}

Catalyst 6000 Marking Policies

When you create marking policies for a Catalyst 6000 family switch, QPM uses this command sequence to configure the device:

1. **set qos acl ip** *acl-name* **dscp** {*dscp* | **trust-cos | trust-ipprec | trust-dscp**} *protocol source* [{**eq** *port* | **range** *port port*}] *destination* [{**eq** *port* | **range** *port port*}] [{**precedence** *precedence* | **dscp-field** *dscp*}]
2. **commit qos acl** *acl-name*
3. **set qos acl map** *acl-name* {*module/port* | *vlan*}

Catalyst 6000 Policing Policies

When you create policing policies for a Catalyst 6000 family switch, QPM uses this command sequence to configure the device:

1. **set qos policer** {**aggregate | microflow**} *policer-name* **rate** *rate* [**policed-dscp erate** *rate* {**policed-dscp | drop**}] **burst** *burst* [{**policed-dscp | drop**}]

2. **set qos acl [default-action] ip** *acl-name* **dscp** {*dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} {**aggregate** | **microflow**} *policer-name* [*protocol source* [{**eq** *port* | **range** *port port*}] *destination* [{**eq** *port* | **range** *port port*}]]
3. **commit qos acl** *acl-name*
4. **set qos acl map** *acl-name* {*module/port* | *vlan*}

Configuration on Catalyst Switches with Supervisor IOS

Port Configuration on Catalyst Switches with Supervisor IOS

When you configure the trust state for Catalyst 6000 switches with Supervisor IOS, QPM uses this command sequence to configure the device:

1. **mls qos**
2. **interface** *interfacename*
3. **mls qos**
4. **mls qos trust** {**cos** | **ip-precedence** | **dscp**}
5. **mls qos vlan-based**

When you configure the trust state for Catalyst 2950 switches with Supervisor IOS, QPM uses this command sequence to configure the device:

1. **mls qos**
2. **interface** *interfacename*
3. **mls qos**

4. **mls qos trust** {**cos** | **dscp**}

When you configure the trust state for Catalyst 3550 switches with Supervisor IOS (no VLAN-based QoS), QPM uses this command sequence to configure the device:

1. **mls qos**
2. **interface** *interfacename*
3. **mls qos**
4. **mls qos trust** {**cos** | **ip-precedence** | **dscp**}

Marking Policies on Catalyst Switches with Supervisor IOS

When you configure marking policies for a Catalyst 6000 with Supervisor IOS, QPM uses this command sequence to configure the device:

1. **class-map [match all | match any]** *classname*
   a. **match [not] access-group** *ACLNum*
2. **policy-map** *policy-map-name*

   class *classname*

   trust {**cos** | **ip-precedence** | **dscp**}

When you configure marking policies for a class-default filter for a Catalyst 2950 with Supervisor IOS, or Catalyst 3550 with Supervisor IOS, QPM uses this command sequence to configure the device:

1. **Switchport priority extend trust**
2. **Switchport priority extend cos** *cos*

When you configure marking policies for a user-defined filter for a Catalyst 2950 with Supervisor IOS, QPM uses this command sequence to configure the device:

1. **class-map [match all | match any]** *classname*
   a. **match [not] access-group** *ACLNum*
2. **policy-map** *policy-map-name*
3. **class** *classname*
4. **set ip dscp** *dscp*

When you configure marking (policing) policies for a user-defined filter for a Catalyst 3550 with Supervisor IOS, QPM uses this command sequence to configure the device:

1. **class-map [match all | match any]** *classname*
   a. **match [not] access-group** *ACLNum*
2. **policy-map** *policy-map-name*
3. **class** *classname*
4. **set ip dscp** *dscp*
5. **set ip precedence** *precedence*
6. **trust** {**cos | ip-precedence | dscp**}

Policing Policies on Catalyst Switches with Supervisor IOS

When you configure policing policies for a Catalyst 6000 with Supervisor IOS or Catalyst 3550 with Supervisor IOS, QPM uses this command sequence to configure the device:

1. **policy-map** *policy-map-name*

   class *classname*

   a. **police [flow]** *rate bc be* [**pir** *pir*] **conform-action** {**set-prec-transmit | set-dscp-transmit | drop**} **exceed-action** {**transmit | policed-dscp-transmit | drop**} **[violate-action** {**transmit | policed-dscp-transmit | drop**}**]**
   b. **police** *aggregate policer-name*

If you define an aggregate policing policy, the following command is used:

- **mls qos aggregate-policer** *policer-name rate bc be* [**pir** *pir*] **conform-action** {**set-prec-transmit | set-dscp-transmit | drop**} **exceed-action** {**transmit | policed-dscp-transmit | drop**} **[violate-action** {**transmit | policed-dscp-transmit | drop**}**]**

When you configure policing policies for a Catalyst 2950 with Supervisor IOS, QPM uses this command sequence to configure the device:

1. **policy-map** *policy-map-name*

   class *classname*

   a. **police** *rate bc* **[exceed-action** {**dscp** *dscp* **| drop**}**]**

   b. **police** *aggregate policer-name*

If you define an aggregate policing policy, the following command is used:

- **mls qos aggregate-policer** *policer-name rate bc be* [**pir** *pir*] **conform-action** {**set-prec-transmit | set-dscp-transmit | drop**} **exceed-action** {**transmit | policed-dscp-transmit | drop**} **[violate-action** {**transmit | policed-dscp-transmit | drop**}**]**

Queuing on Catalyst Switches with Supervisor IOS

When you configure 2Q2T or 1P2Q2T queuing for Catalyst 6000 switches with Supervisor IOS, QPM uses the following command sequence:

1. **mls qos**
2. **interface** *interfacename*
3. **mls qos**
4. **wrr-queue cos-map** *queue-number threshold-number cos-list*
5. **priority-queue cos-map** *queue-id cos-list*
6. **wrr-queue queue-limit** *queue-ratio-1 queue-ratio-2*
7. **wrr-queue bandwidth** *queue-weight-1 queue-weight-2*
8. **wrr-queue threshold** *queue-number threshold-1 threshold-2*
9. **wrr-queue random-detect max-threshold** *queue-number threshold-1 threshold-2*

When you configure 4Q2T queuing for Catalyst 3550 switches with Supervisor IOS, QPM uses the following command sequence:

1. **wrr-queue cos-map** *queue-number cos-list*
2. **priority-queue out**
3. **wrr-queue dscp-map** *threshold-id dscp-list*

4. **wrr-queue queue-limit** *queue-ratio-1 queue-ratio-2 queue-ratio-3 queue-ratio-4*
5. **wrr-queue bandwidth** *queue-weight-1 queue-weight-2 queue-weight-3 queue-weight-4*
6. **wrr-queue threshold** *queue-number threshold-1 threshold-2*
7. **wrr-queue random-detect max-threshold** *queue-number threshold-1 threshold-2*

When you configure 4Q1T queuing for Catalyst 2950 switches with Supervisor IOS, QPM uses the following command sequence:

1. **wrr-queue bandwidth** *queue-weight-1 queue-weight-2 queue-weight-3 queue-weight-4*
2. **wrr-queue cos-map** *queue-number cos-list*

CoS, Precedence, DSCP, and DSCP Markdown Mapping on Catalyst Switches with Supervisor IOS

When you configure these mapping settings for a Catalyst 6000 with Supervisor IOS or Catalyst 3550 with Supervisor IOS, QPM uses this command sequence to configure the device:

1. **mls qos map cos-dscp** *dscp dscp dscp dscp dscp dscp dscp dscp*
2. **mls qos map dscp-cos** *dscp dscp dscp dscp dscp dscp dscp dscp* **to** *cos*
3. **mls qos map ip-prec-dscp** *dscp dscp dscp dscp dscp dscp dscp dscp*
4. **mls qos map policed-dscp [**{**normal-burst | max-burst**}**]** *dscp dscp dscp dscp dscp dscp dscp dscp* **to** *dscp*

When you configure these mapping settings for a Catalyst 2950 with Supervisor IOS, QPM uses this command sequence to configure the device:

1. **mls qos map cos-dscp** *dscp dscp dscp dscp dscp dscp dscp dscp*
2. **mls qos map dscp-cos** *dscp dscp dscp dscp dscp dscp dscp dscp* **to** *cos*

Catalyst 2900XL and Catalyst 3500XL Marking Policies

When you configure Catalyst 2900XL and Catalyst 3500XL marking policies, QPM uses this command sequence to configure the device:

1. **interface** *interfacename*
2. **Switchport priority default cos** *cos*
3. **Switchport priority extend** {**none | trust**}
4. **Switchport priority extend cos** *cos*

Layer 3 Policing Policies

When you configure Layer 3 policing policies, QPM uses this command sequence to configure the device:

1. **interface** *interfacename*
2. **rate-limit** {**input | output**} *rate* [*burst*]

Layer 3 Shaping Policies

When you configure Layer 3 shaping policies, QPM uses this command sequence to configure the device:

1. **interface** *interfacename*
2. **traffic-shape rate** *rate* [*burst*]

Catalyst 4000 Queuing Policies

When you configure 2Q1T queuing policies for Catalyst 4000 switches, QPM uses this command sequence to configure the device:

- **set qos map** *queue-type qid threshold* **cos** *cos-value*

Catalyst 4000 Marking Policies

When you configure marking policies for Catalyst 4000 switches, QPM uses this command sequence to configure the device:

- **set qos defaultcos** *cos*

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W