CiscoWorks
QoS Policy Manager (QPM) v3.0

Management of Quality of Service (QoS) Policies for Integrated Networks

This page left intentionally blank.

The products and specifications, configurations, and other technical information regarding the products in this manual are subject to change without notice. All statements, technical information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. You must take full responsibility for their application of any products specified in this manual.

LICENSE

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THE MANUAL, DOCUMENTATION, AND/OR SOFTWARE ("MATERIALS"). BY USING THE MATERIALS YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT AGREE WITH THE TERMS OF THIS LICENSE, PROMPTLY RETURN THE UNUSED MATERIALS (WITH PROOF OF PAYMENT) TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Cisco Systems, Inc. ("Cisco") and its suppliers grant to you ("You") a nonexclusive and nontransferable license to use the Cisco Materials solely for Your own personal use. If the Materials include Cisco software ("Software"), Cisco grants to You a nonexclusive and nontransferable license to use the Software in object code form solely on a single central processing unit owned or leased by You or otherwise embedded in equipment provided by Cisco. You may make one (1) archival copy of the Software provided You affix to such copy all copyright, confidentiality, and proprietary notices that appear on the original. EXCEPT AS EXPRESSLY AUTHORIZED ABOVE, YOU SHALL NOT: COPY, IN WHOLE OR IN PART, MATERIALS; MODIFY THE SOFTWARE; REVERSE COMPILE OR REVERSE ASSEMBLE ALL OR ANY PORTION OF THE SOFTWARE; OR RENT, LEASE, DISTRIBUTE, SELL, OR CREATE DERIVATIVE WORKS OF THE MATERIALS.

You agree that aspects of the licensed Materials, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Cisco. You agree not to disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Cisco. You agree to implement reasonable security measures to protect such trade secrets and copyrighted Material. Title to the Materials shall remain solely with Cisco.

This License is effective until terminated. You may terminate this License at any time by destroying all copies of the Materials. This License will terminate immediately without notice from Cisco if You fail to comply with any provision of this License. Upon termination, You must destroy all copies of the Materials.

Software, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. You agree to comply strictly with all such regulations and acknowledge that it has the responsibility to obtain licenses to export, re-export, or import Software.

This License shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this License shall remain in full force and effect. This License constitutes the entire License between the parties with respect to the use of the Materials

Restricted Rights - Cisco's software is provided to non-DOD agencies with RESTRICTED RIGHTS and its supporting documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the U.S. Government is subject to the restrictions as set forth in subparagraph "C" of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19. In the event the sale is to a DOD agency, the U.S. Government's rights in software, supporting documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and DFARS 227.7202.

DISCLAIMER OF WARRANTY. ALL MATERIALS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

In no event shall Cisco's or its suppliers' liability to You, whether in contract, tort (including negligence), or otherwise, exceed the price paid by You. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

Turn the television or radio antenna until the interference stops.

Move the equipment to one side or the other of the television or radio.

Move the equipment farther away from the television or radio.

Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The following third-party software may be included with your product and will be subject to the software license agreement:

CiscoWorks software and documentation are based in part on HP OpenView under license from the Hewlett-Packard Company. HP OpenView is a trademark of the Hewlett-Packard Company. Copyright © 1992, 1993 Hewlett-Packard Company.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Network Time Protocol (NTP). Copyright © 1992, David L. Mills. The University of Delaware makes no representations about the suitability of this software for any purpose.

Point-to-Point Protocol. Copyright © 1989, Carnegie-Mellon University. All rights reserved. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

The Cisco implementation of TN3270 is an adaptation of the TN3270, curses, and termcap programs developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981-1988, Regents of the University of California.

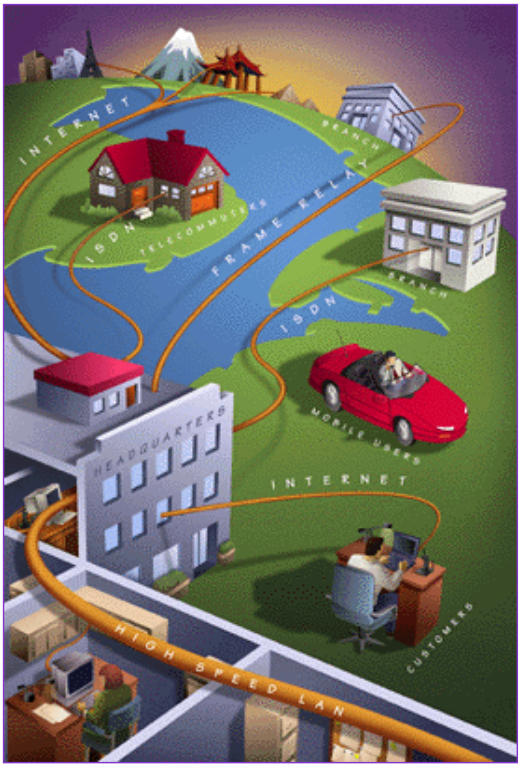
Cisco incorporates Fastmac and TrueView software and the RingRunner chip in some Token Ring products. Fastmac software is licensed to Cisco by Madge Networks Limited, and the RingRunner chip is licensed to Cisco by Madge NV. Fastmac, RingRunner, and TrueView are trademarks and in some jurisdictions registered trademarks of Madge Networks Limited. Copyright © 1995, Madge Networks Limited. All rights reserved.

The X Window System is a trademark of the X Consortium, Cambridge, Massachusetts. All rights reserved.

Cisco Secure, ACS, ACS, VMS, DFM, QoS Policy Manager, QPM, URT, IPM, SAA, CiscoWorks, RME, Resource Manager Essentials, AutoConnect, AutoRoute, AXIS, BPX, Catalyst, CD-PAC, CiscoAdvantage, CiscoFusion, Cisco IOS, the Cisco IOS logo, CiscoLink, CiscoPro, the CiscoPro logo, CiscoRemote, theCiscoRemote logo, CiscoSecure, Cisco Systems, CiscoView, CiscoVision, CiscoWorks, CiscoWorks 2000, ClickStart, ControlStream, CWSI, EdgeConnect, EtherChannel, FairShare, FastCell, FastForward, FastManager, FastMate, FastPADlmp, FastPADmicro, FastPADmp, FragmentFree, FrameClass, Fulcrum INS, IGX, Impact, InternetJunction, JumpStart, LAN2LAN Enterprise, LAN2LAN Remote Office, LightSwitch, MICA, NetBeyond, NetFlow, Newport Systems Solutions, Packet, PIX, Point and Click Internetworking, RouteStream, Secure/IP, SMARTnet, StrataSphere, StrataSphere BILLder, StrataSphere Connection Manager, StrataSphere Modeler, StrataSphere Optimizer, Stratm, StrataView Plus, StreamView, SwitchProbe, SwitchVision, SwitchWare, SynchroniCD, The Cell, The FastPacket Company, TokenSwitch, TrafficDirector, Virtual EtherSwitch, VirtualStream, VlanDirector, Web Clusters, WNIC, Workgroup Director, Workgroup Stack, and XCI are trademarks; Access by Cisco, Bringing the Power of InternetworkingtoEveryone, Enter the Net with MultiNet, and The Network Works. No Excuses. are service marks; and Cisco, theCisco Systems logo, CollisionFree, Combinet, EtherSwitch, FastHub, FastLink, FastNIC, FastPacket, FastPAD, FastSwitch, ForeSight, Grand, GrandJunction, GrandJunction Networks, the Grand Junction Networks logo, HSSI, IGRP, IPX, Kalpana, theKalpana logo, LightStream, MultiNet, MultiWare, OptiClass, Personal Ethernet, Phase/IP, RPS, StrataCom, TGV, the TGV logo, and UniverCD are registered trademarks of Cisco Systems, Inc. All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners.

About This Tutorial

Cisco.com



- **Identify the need for QoS management**
- **Describe the industry standards and the Cisco implementation of QoS management**
- **Illustrate QoS scenarios**
- **Provide helpful guidelines for installation and system administration of QPM**
- **Provide links to helpful documentation and white papers**

About This Tutorial

This tutorial provides self-paced training on using the CiscoWorks Quality of Service (QoS) Policy Manager or QPM v3.0 application. QPM lets the user 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 network managers to create and manage end-to-end differentiated services in their network, thus making more efficient and economical use of their existing network resources.

This tutorial is structured as a series of individual modules made up of chapters that conclude with self-administered exercises. The tutorial explores the architecture, product features, implementation scenarios, installation, and system administration of the QPM product. A separate chapter provides a useful reference section containing links to product documentation and technical white papers on QoS concepts and terminology. The material is presented through text, illustrations, hypertext links, and typical usage scenarios.

Who Should Use This Tutorial

This tutorial was written as a technical resource for network administrators responsible for deploying or managing QoS policies in their network and assumes that readers will have an understanding of networking principles, QoS terminology, and network management concepts.

Prerequisites

Before using the QPM application, you should have first satisfied the following prerequisites:

- A basic understanding of network management
- A basic understanding of TCP/IP networking
- A basic understanding of the operation and configuration of their network, including the topology, device inventory, and security requirements
- A basic understanding of Cisco IOS, Cisco CatOS, and Cisco AVVID (Architecture for Voice, Video and Integrated Data) products
- A basic understanding of queuing mechanisms and QoS (Quality of Service) concepts

Estimated Completion Time

24 hours

How the Tutorial is Organized

Cisco.com

- **Chapter 1: Introduction**
- **Chapter 2: QPM Product Features**
- **Chapter 3: QoS Scenarios**
- **Chapter 4: Installation & System Administration**
- **Chapter 5: Reference Material**

How This Tutorial Is Organized

The tutorial is divided into five chapters. Each chapter begins with the learning objectives specific to the chapter and concludes with a series of self-assessment exercises based on the chapter's objectives. Multiple-choice exercises are provided at the end of the chapter to enable the reader to assess their understanding of the material presented. A summary of each chapter is listed below.

Chapter 1 - Introduction

This chapter introduces the need for quality of service mechanisms and tools to help manage QoS policies. An overview of Cisco's solution for performing QoS management is presented by introducing CiscoWorks QPM before learning about the features and capabilities of QPM in Chapter 2 and using QPM in common scenarios in Chapter 3.

Chapter 2 – QPM Product Features

What is Quality of Service (QoS) and why is it so important? This chapter first provides a QoS primer by reviewing important QoS terminology and concepts.

Secondly, this chapter provides details on how to use the features of QPM to implement and deploy QoS mechanisms on Cisco devices. A typical workflow on how to use QPM is provided. The workflow provides an outline for the remaining chapter. The workflow is broken down into sub-chapters which focus on planning for QoS, adding devices to the QPM inventory, creating deployment groups, QoS policy groups, and policies, deploying QoS policies and monitoring the results of the policies deployed.

Chapter 3 - QoS Scenarios

This chapter presents some scenarios in which to provide a hands-on look at using QPM. These scenarios will help you to understand how to use QPM to define various QoS policies in both data and voice networks. These scenarios will help to reinforce the information learned in Chapter 2.

Chapter 4 - Installation and System Administration

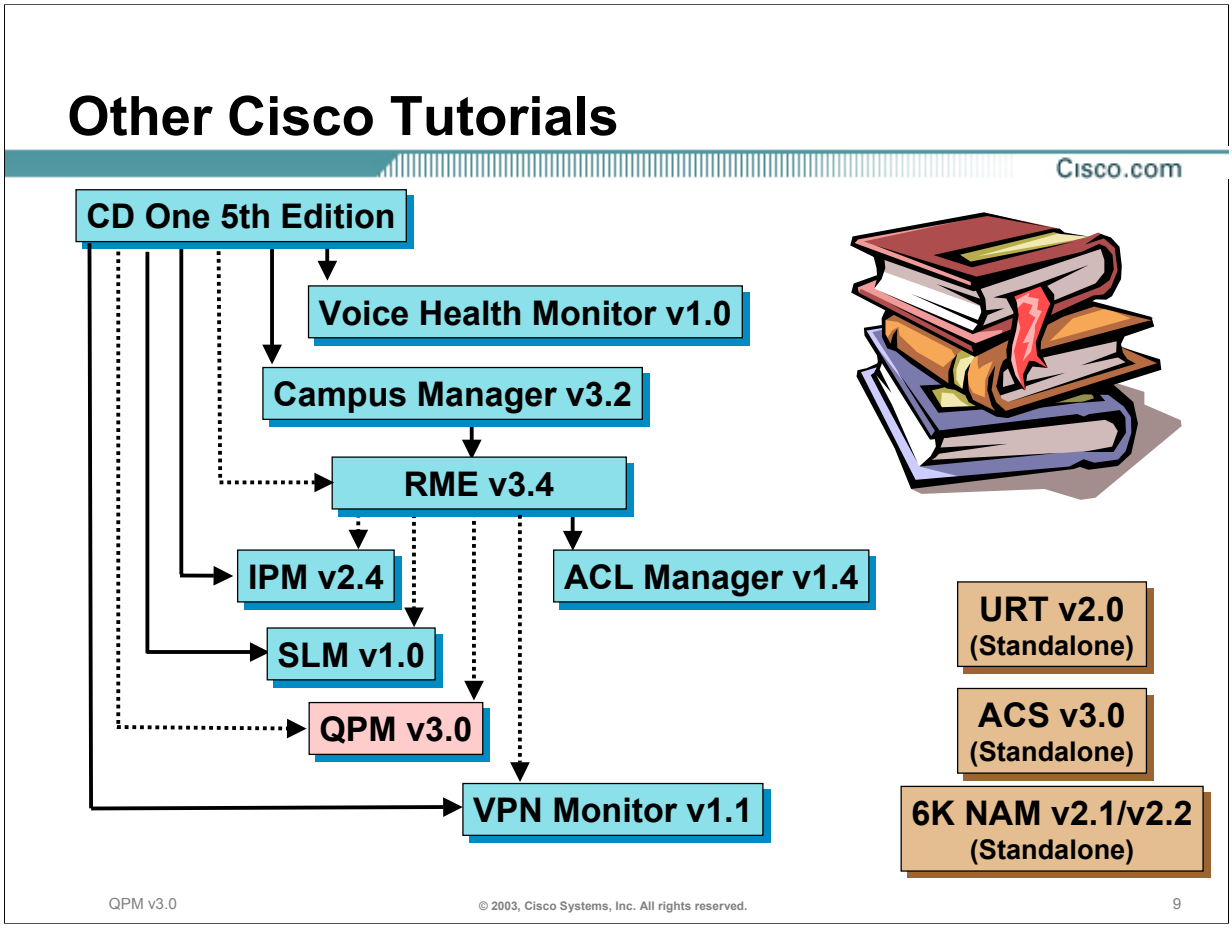
This chapter provides information about product requirements, hardware installation guidelines, device configuration, and tips for system administrators. For more detailed instructions on installing CiscoWorks QPM v3.0, please refer to the Installation Guide. A link to the Installation Guide can be found in the reference section (Chapter 5).

Chapter 5 - References

This chapter contains a comprehensive list of additional product information, such as links to white papers and documentation.

Chapter Questions and Answers

This section contains the answers to the questions that conclude each chapter.



Other Cisco Tutorials

This tutorial provides a comprehensive study of the CiscoWorks QPM v3.0 application. Other tutorials for many of the CiscoWorks management products also exist. QPM can be installed on top of the CiscoWorks CD One software and import devices from Resource Manager Essential (RME). Therefore, the reader is encouraged to read the CD One and RME tutorials for more information on the CiscoWorks server, user account management, and RME inventory management features.

The interested reader may wish to review other CiscoWorks product tutorials to learn about how to manage their networks using a comprehensive set of applications. Since many of the CiscoWorks products rely or benefit on other products, we recommend that you read the tutorials in the depicted order. Here are some additional notes on the reading order dependency.

- Review the CD One tutorial first to obtain a quick understanding of the CiscoWorks server and its functionality, the Integration Utility, and CiscoView.
- If you have purchased the LAN Management Solution (LMS) bundle, review sections in Campus Manager (Topology Services) prior to reading the RME tutorial. The importing of devices into Essentials is greatly enhanced by Campus Manager's Network Services auto-discovery of devices.
- If you have purchased the Routed WAN (RWAN) Management Solution bundle, review sections within the RME tutorial on Inventory and Configuration Management. ACL Manager requires the devices being managed in the Inventory and the Configuration Archive containing up-to-date device configuration files.
- If you have purchased the RWAN Management Solution bundle, review sections within the RME tutorial on Inventory Management. IPM (Internetwork Performance Manager) can import the devices being managed in the CiscoWorks2000 Inventory.
- VPN Monitor requires that devices be imported from the RME Inventory and can generate RME Syslog reports pertaining to VPN devices and problems. Other functions within RME are also useful in overall VPN management.
- URT is a stand-alone product; however, by understanding the RME inventory, one can import devices into URT from the RME inventory.

This page left intentionally blank.

Chapter 1

Introduction

QoS Policy Manager (QPM) v3.0

Chapter 1 Objectives

Cisco.com

Upon completion of this chapter, you will be able to:

- **Identify the Growing Need for Policy Networking**
  - **Increasing Demand for Network Services**
  - **Differentiation of Network Services**
- **Realize the Benefits of Policy Networking**
- **Identify the Challenges**
  - **Defining Service-Level Policies**
  - **Configuring Service-Level Policies**
  - **Monitoring Service-Level Policies**
- **Describe the Cisco Solution**
  - **CiscoWorks QoS Policy Manager**

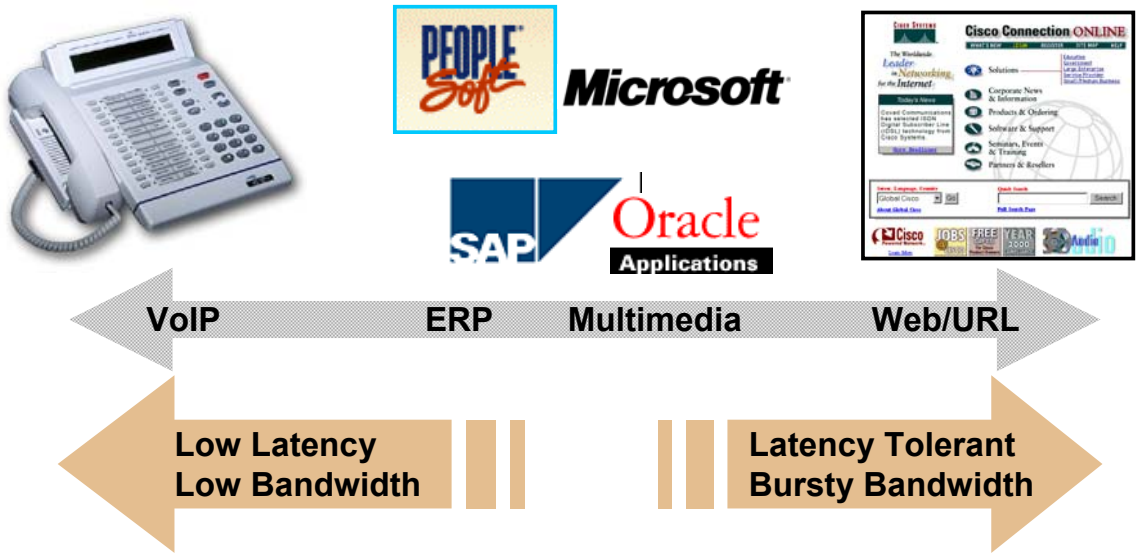
Chapter 1 Objectives

Welcome to the first step to improving your ability to automate the process for configuring and deploying Quality of Service (QoS) policies throughout the enterprise network. This chapter highlights the growing need for policy networking, the challenges faced by network designers and administrators, and products available from Cisco Systems that can greatly simplify the task of configuring, deploying, and monitoring QoS policies throughout the enterprise network.

The Growing Need for Policy Networking

Proliferation of Network Services

Cisco.com



QoS Trade-Offs by Application Type

The Growing Need for Policy Based Networking

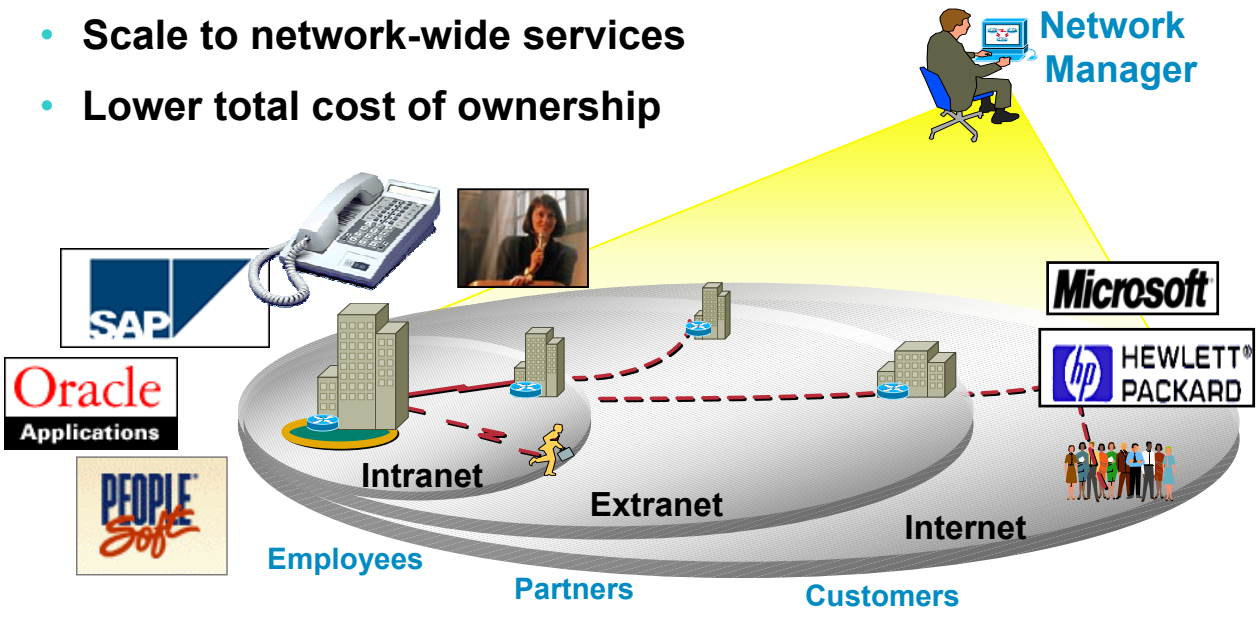
Over the last five years, there has been a fundamental shift in the way companies utilize their network. Almost everything a business does is now offered as a network service. Not only are the number of networked applications increasing, but the amount of bandwidth consumed by an application is increasing. As the convergence of data, voice, and video applications move forward, each application varies in their amount of bandwidth consumed and tolerance for increased network latency or delay. For example, web-based application traffic, which is often bursty in terms of the amount of bandwidth consumed, can tolerant moderate network latency. On the other hand, voice and video application traffic, which consists of small packet sizes, can not tolerant network delays. Voice packet delays can cause either voice quality degradation (voice clipping and skips) due to the end-to-end voice latency or packet loss if the delay is variable.

As a result, it has become increasing important to classify network traffic and prioritize the mission-critical and time sensitive application in order to improve and guarantee network service levels.

Benefits of Policy Based Networking

Cisco.com

- Converge voice and data networks
- Ensure application performance
- Scale to network-wide services
- Lower total cost of ownership



QPM v3.0

Introduction 1-4

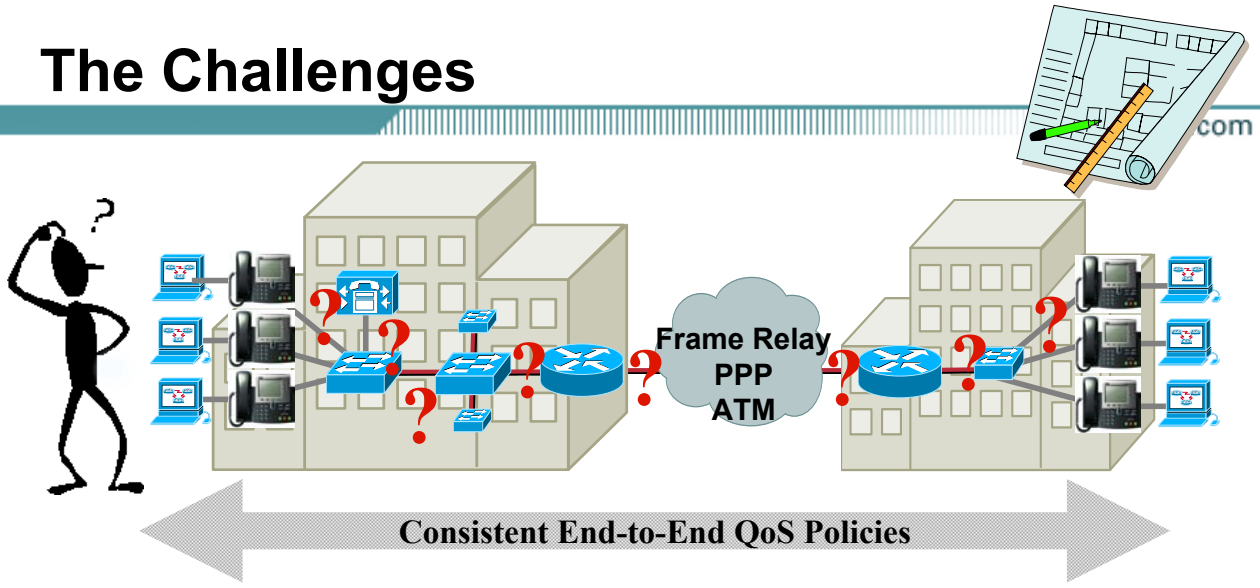
Benefits of Policy Based Networking

For the reasons just discussed, network administrators are looking towards policy based networking. By implementing QoS policies throughout the enterprise network, the network administrators can ensure end-to-end application performance. This includes all applications such as client-server, Enterprise Resource Planning (ERP), multimedia, web-based applications, and of course Voice over IP (VoIP).

Quality of Service (QoS) for applications and users can be guaranteed when proper network design is combined with the new Cisco Catalyst products and the latest Cisco IOS releases. When building a Cisco AVVID (Architecture for Voice, Video and Integrated Data) network, the customer should adhere to network design principles defined in the IP Telephony/VoIP Design and Implementation Design Guide. (Refer to Chapter 5 for the URL to obtain access to this design guide.)

By realizing these benefits of implementing QoS policies, and that buffering, not bandwidth, is the issue in maintaining quality of service, corporations can lower the total cost of ownership in the network.

The Challenges



Knowing the Catalysts® OS and Cisco IOS® Device Commands

```
cat6k-access> (enable) set port qos 5/1-48 trust-ext untrusted
cat6k-access> (enable) set port qos 5/1-48 trust trust-cos
cat6k-access> (enable) set qos acl ip ACL_IP-PHONES trust-cos ip any any
cat6k-access> (enable) set port qos 5/1-48 vlan-based
cat6k-access> (enable) commit qos acl all
cat6k-access> (enable) set qos acl map ACL_IP-PHONES 110
```


The Challenge

So why are QoS policies not implemented in every network? While the need for managing the network applications for quality of service (QoS) is obvious, the configuration and deployment of QoS policies is not obvious.

The first challenge is determining where QoS policies get deployed in the network; at the edge, the access layer, the distribution layer, the core, and/or at the remote branch offices? For successful deployment of QoS policies, the network designer must ensure end-to-end network quality at each layer.

The second challenge may be that policies are difficult to configure. Utilizing the QoS features within intelligent network devices can be a complex exercise for network managers. We all know that there is a great deal of configuration complexity in configuring an end-to-end QoS environment or configuring an end-to-end security environment. So, for that reason, automated tools are required to be able to deploy these kinds of end-to-end intelligent services. And, of course, without automated policy configuration tools, it's highly likely that a user that tries to apply policies from end to end across a complex network will end up with inconsistencies.

Another issue is inconsistency in policies. In today's networks, users generally limit their deployment of intelligent tools in switches and routers based on their fear of having inconsistent policies or on the complexity and cost of implementing those policies in networks through things like Cisco IOS-based ACLs, Access Control Lists. Therefore, the solution is to have centralized policy control to manage the deployment of policies.

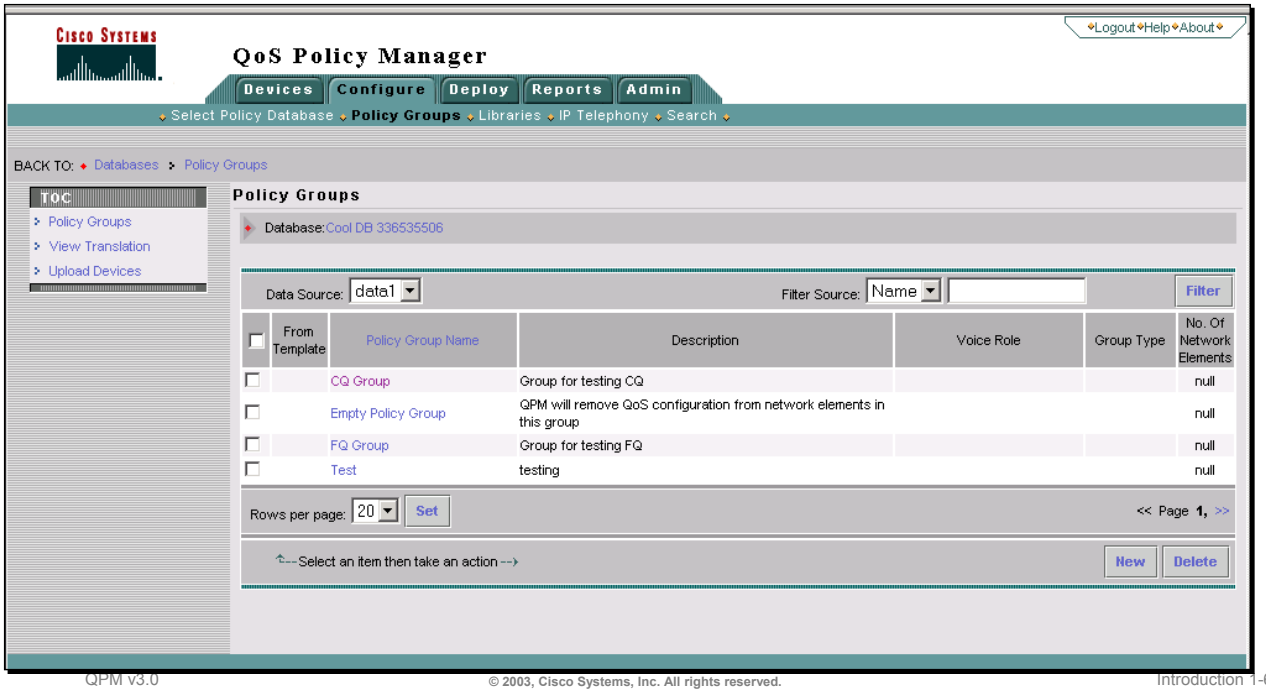
And finally, what we want to be able to apply in policy networking is an end-to-end model for controlling application traffic. The application traffic needs to be something that can be profiled. Intelligent network devices need to be able to profile traffic based on the application type, so that it can apply highly granular policies using the application recognition capabilities of the network.

The upcoming pages will address these issues. Now let's look a little more closely at the Cisco solution, QPM – QoS Policy Manager.

The Cisco Solution
CiscoWorks QoS Policy Manager

Cisco.com

- *Centralized, Multi-Device QoS Policy Management for Voice and Data Networks*
- *Secure HTML-based user interface; Common CiscoWorks framework*



The Cisco Product Solution – CiscoWorks QPM

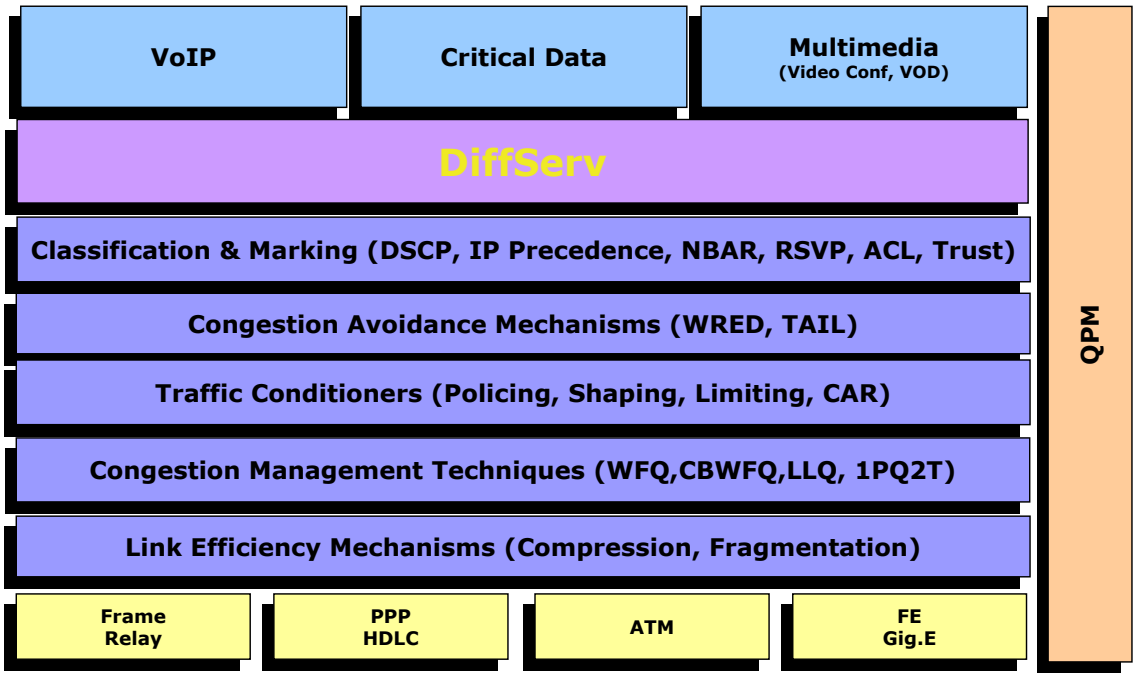
Cisco realizes that to effectively manage data and converged IP telephony networks, network managers need tools that can simplify the configuration, deployment, management, and monitoring of QoS policies. In response to these management concerns, Cisco has developed CiscoWorks QoS Policy Manager (QPM) to address these complex tasks.

QPM, the focus of this tutorial, lets the user define QoS policies at a more abstract level than can be defined using individual Cisco IOS/CatOS device commands. Using QPM, the user does not need to know the exact device commands to configure the QoS policy. QPM has an embedded knowledge base of the command line syntax. In addition, with QPM the user can define policies for groups of devices rather than one device at a time. Policies can be created using simple layman type constructs that apply to multiple applications or groups of hosts much more easily than can be defined using device commands.

By giving the user a high level view of their policies, QPM makes it easier to define, modify, and deploy QoS policies. By simplifying QoS policy definition and deployment, QPM makes it easier to create and manage differentiated services in the network, thus making more efficient and economical use of existing network resources. For example, the user can deploy policies that ensure that their mission-critical applications always get the bandwidth required to run their business.

The Cisco Solution
CiscoWorks QoS Policy Manager Features

Cisco.com



QPM v3.0 Introduction 1-7

The Cisco Product Solution – CiscoWorks QPM Features

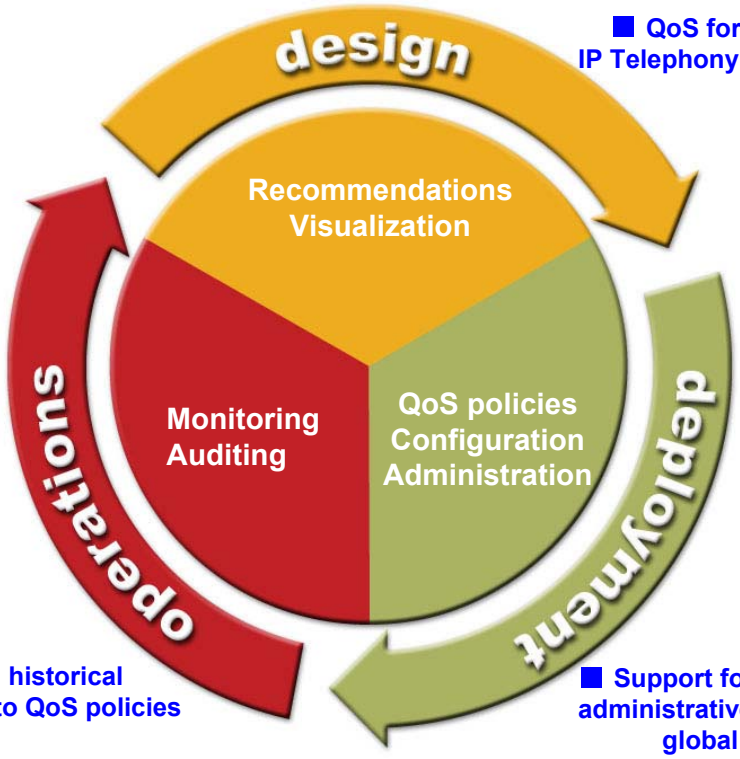
The latest version of QPM is capable of configuring, deploying, and monitoring a large gamut of QoS mechanisms for not only critical data, but also for voice over IP (VoIP) and multimedia applications such as video conferences and video on demand (VOD) for media-rich e-learning solutions.

It does not matter if the critical application data is traversing the Campus over Ethernet or the WAN using ATM, PPP, HDLC or Frame Relay. QPM detects the physical interface types and can configure and deploy the assigned QoS mechanisms.

In Chapter 2 of this tutorial, an entire section is dedicated to explaining the various mechanisms and techniques for managing quality of service. This figure above illustrates the QoS features supported by QPM. Chapter 2 will describe how to use QPM to configure these QoS mechanisms.

The Cisco Solution
QPM Features - Complete Lifecycle Coverage

Cisco.com



- QoS for voice guidance with IP Telephony wizard, updated templates
- Real time and historical feedback related to QoS policies
- Support for large networks using administrative + deployment domains, global policies + libraries

QPM v3.0

Introduction 1-8

The Cisco Product Solution – CiscoWorks QPM Features

In order to effectively manage a voice and telephony enabled network, administrators need tools that can simplify the configuration, deployment, management, and monitoring of QoS policies. Managing QoS in this environment is not a do-one-time-and-forget task; effective management is an ongoing process.

QoS management entails:

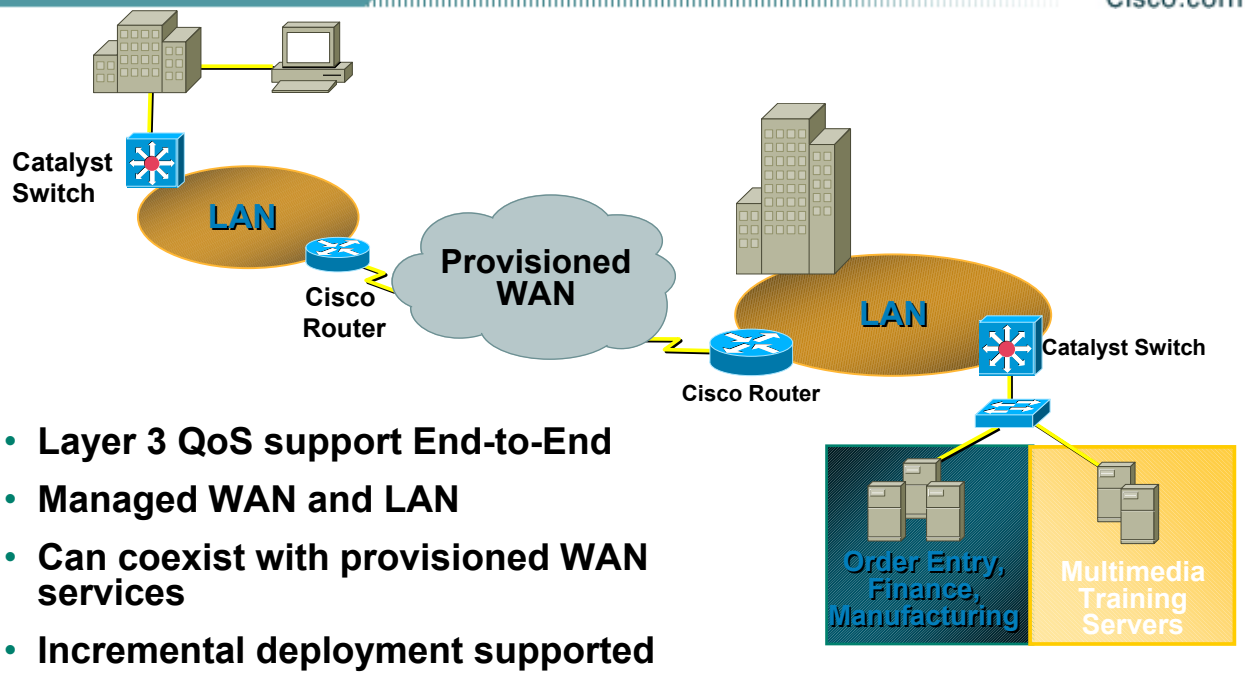
- Baseline monitor critical traffic flows to figure out what policies are needed
- Classify applications into service classes
- Provision QoS with network-wide enforcement
- Validate QoS settings and results

QoS management is a continuous cycle involving monitoring to gain visibility into network operations, configuring or adjusting policies critical to application performance, and automating multiple service-levels across any network topology. The management tool must be able to deliver centralized QoS analysis and policy control for voice/video/data networks, enable network-wide, content-based differentiated services, and campus-to-WAN automated QoS configuration and deployment.

In the design of QoS policies, QPM provides a library of predefined QoS policies for IP Telephony networks based on Cisco specified design guidelines. An IP Telephony wizard walks the user through the various network points that may requires QoS configuration for voice traffic at the global device or interface level.

And finally, the deployment of QoS configurations is simplified with QPM by the use of administrative and deployment domains.

QPM Policy Deployment



- Layer 3 QoS support End-to-End
- Managed WAN and LAN
- Can coexist with provisioned WAN services
- Incremental deployment supported
- Optional User/Device authorization with ACS

QPM Policy Deployment

The latest version of QPM is extremely beneficial for the convergence of IP networks with voice, video, and data. Along with the embedded knowledge base of device commands, QPM has IP Telephony templates that can be used to configure and deploy QoS policies for devices located at the network edge, access layer, distribution layer, and core backbone. As you will see in the upcoming chapters, QPM is also suitable for data-only networks that support mission critical client-server, web-based, and custom applications.

QPM is suitable for large-scale enterprise deployments consisting of hundreds or thousands of devices, such as IP Telephony deployments. QPM is scalable and facilitates management of large networks by allowing you to create multiple QoS deployment groups, each of which manages a subset of the network devices and policies. In this way, you can effectively partition the network (typically by region and/or types of devices) and implement phased deployment of QoS policies across the network. The number of devices managed in a single deployment group will vary according to your needs and preferences.

And finally, QPM can be used with Cisco Secure Access Control Server (ACS) and the device groups within ACS for user/device authorization.

This page intentionally left blank.

Thank You!

Chapter 1 provided you with a quick overview of the need for QoS policy management and Cisco's solution – CiscoWorks QPM. Continue on to Chapter 2 to discover how to use QPM to define and deploy QoS policies in your network.

Chapter 2

Product Features

QoS Policy Manager (QPM) v3.0

Chapter 2 Objectives

Cisco.com

Upon completion of this chapter, you will be able to:

- **Describe QoS Terminology and Concepts**
- **Identify QPM Product Features**
- **Use the QPM Product to Implement Cisco QoS Mechanisms**

Chapter 2 Objectives

In the previous chapter, you learned about the need for, and benefits of, policy-based networking. Cisco has addressed these needs through its Architecture for Voice, Video and Integrated Data (AVVID) strategy.

A part of the AVVID strategy, is the CiscoWorks QPM product or QoS Policy Manager. This chapter provides the user with an overview of QoS terminology, and discusses the features of QPM and how to use them to achieve the benefits of policy based networking.

After the overview of QoS terminology and QPM, the chapter is divided into the sections highlighting a typical workflow or roadmap for using QPM.

- First, learn how to add devices to QPM for policy management
- Learn how to create a deployment group that contains QoS policies within a policy group and assign the policies to network elements.
- Once the policies have been defined, explore how to use QPM to deploy the QoS policies to the devices
- And finally, learn how to analyze the effects of the QoS policies by monitoring, analyzing, and creating QPM reports

Part 1

Terminology Review

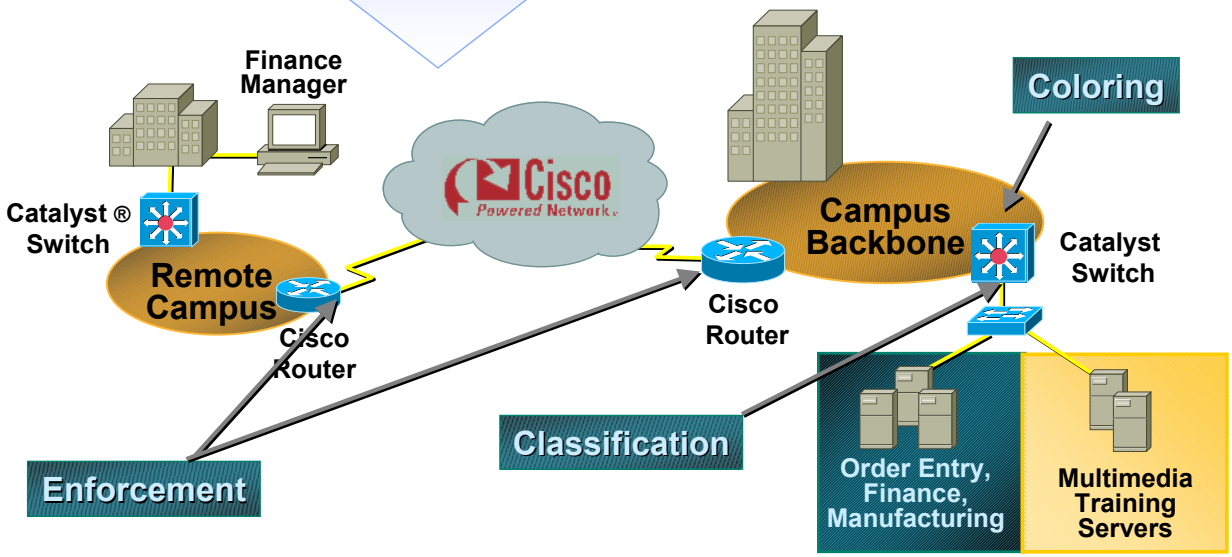
The Quality of Service (QoS) concepts and terminology reviewed in this section are key elements in the understanding of the parameters and features of QPM. By beginning the chapter with a review of what these terms are, and why they are used, will better illuminate the architecture, configuration, and implementation discussions that follow.

What Is QoS?

Quality of Service

Cisco.com

"A set of capabilities that allow you to create differentiated and guaranteed services for network traffic, thereby providing better service for selected applications and users."

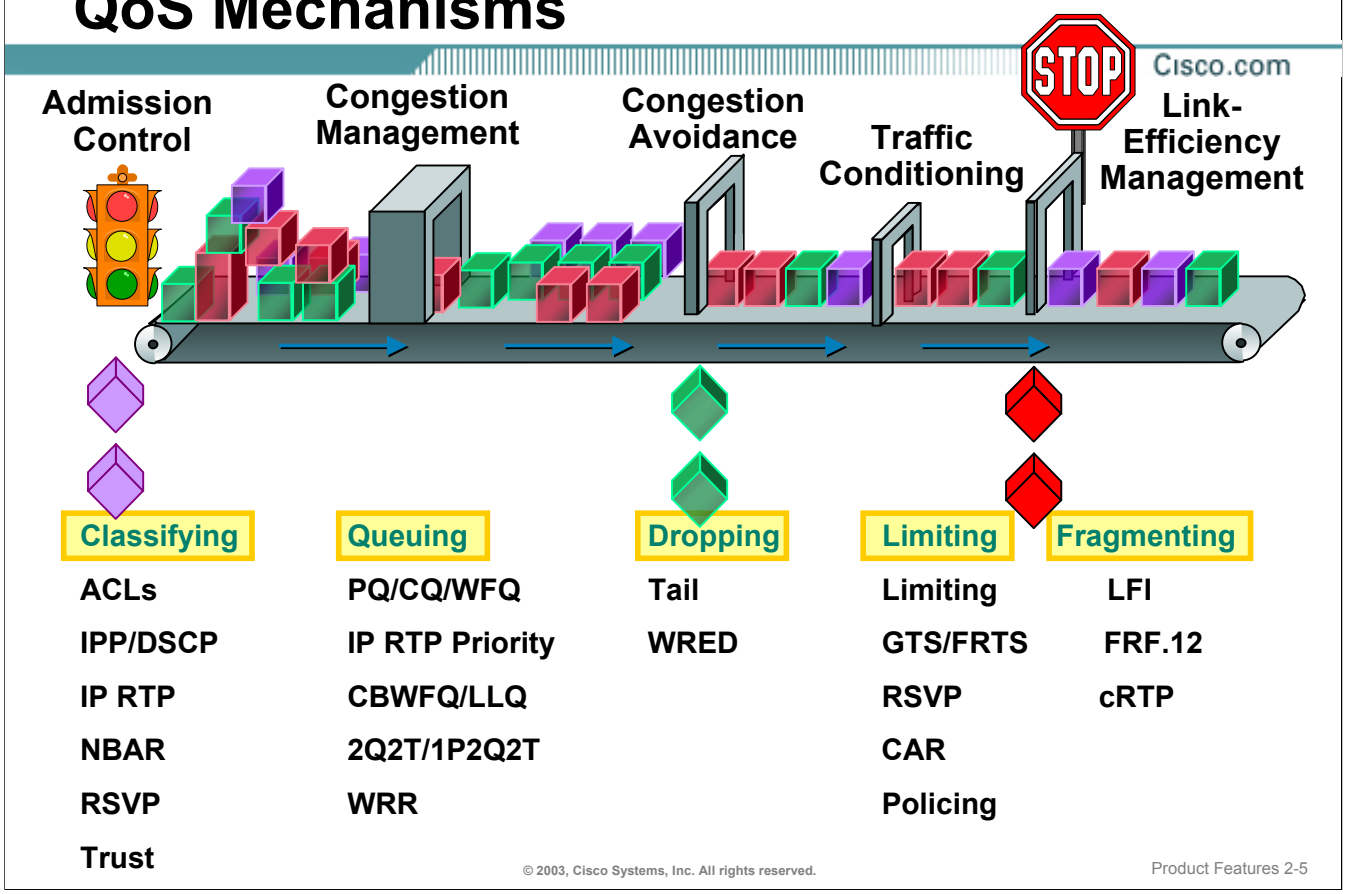


The Definition

Quality of Service (QoS) is a set of capabilities that allows network administrators to create differentiated services for network traffic, thereby providing better service for selected network traffic.

For example, with QoS, you can increase bandwidth for critical traffic, limit bandwidth for non-critical traffic, and provide consistent network response, among other things. This allows you to use expensive network connections more efficiently, and to establish service level agreements with customers of the network. In addition, QoS services can provide various levels of security for protecting your data through encryption. Briefly, the QoS mechanisms deployed throughout the enterprise network must first classify the traffic at the network edge by marking or coloring the traffic. The "marked" packets are later used as identification in the various policies and some of the queuing algorithms for determining forwarding order. Strict queuing and limiting policies must be enforced throughout the packet's journey to its destination.

As identified on the next page, there are various tools or mechanisms for providing these services.



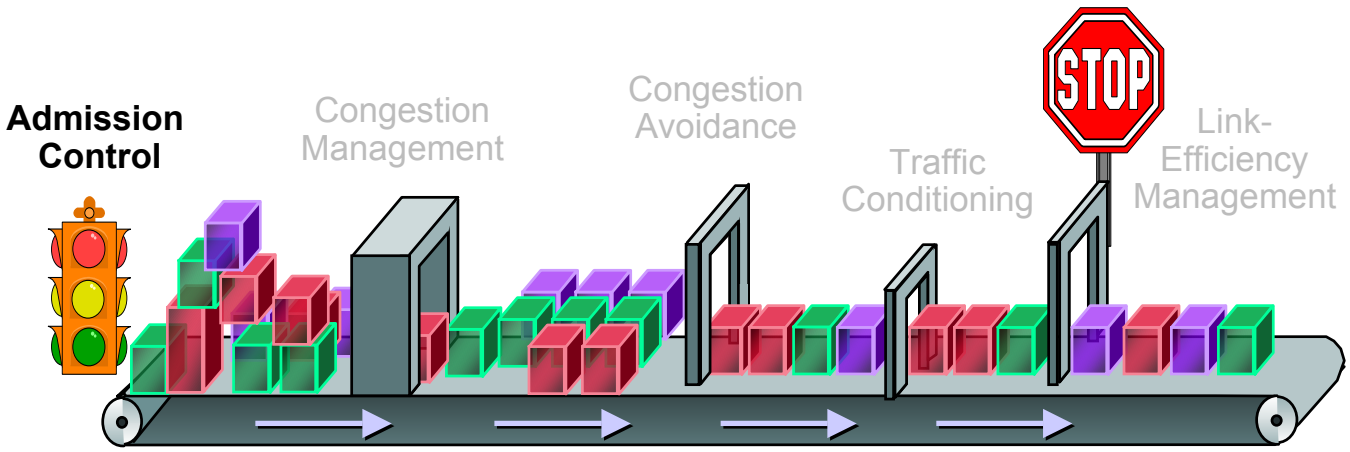
Quality of Service Mechanisms

Understanding the behavior of all the different QoS mechanisms is difficult to learn and to present in a meaningful way. Therefore, we have categorized these mechanisms into five areas:

- Admission Control - These mechanisms filter application traffic based on the characteristics of the traffic. The traffic can then be marked or colored to help identify it along the network path.
- Congestion Management - These mechanisms provide various ways to queue traffic at the interface. By identifying the type of traffic first, the application traffic can be placed in different queues and serviced according to the queue type.
- Congestion Avoidance - At times the interface queue can become full. These mechanisms determine which packets should be dropped. By dropping packets in a TCP environment, congestion avoidance attempts to throttle back TCP flows before the interface becomes congested.
- Traffic Conditioning - Application traffic is often bursty in nature. These mechanisms help to smooth traffic by either limiting the traffic to a specified rate or shaping the traffic using queuing techniques.
- Link Efficiency Management - Fragmenting large packets or using packet header compression can often help make the link more efficient.

Each of these QoS mechanisms will be reviewed in the upcoming pages.

This page intentionally left blank.



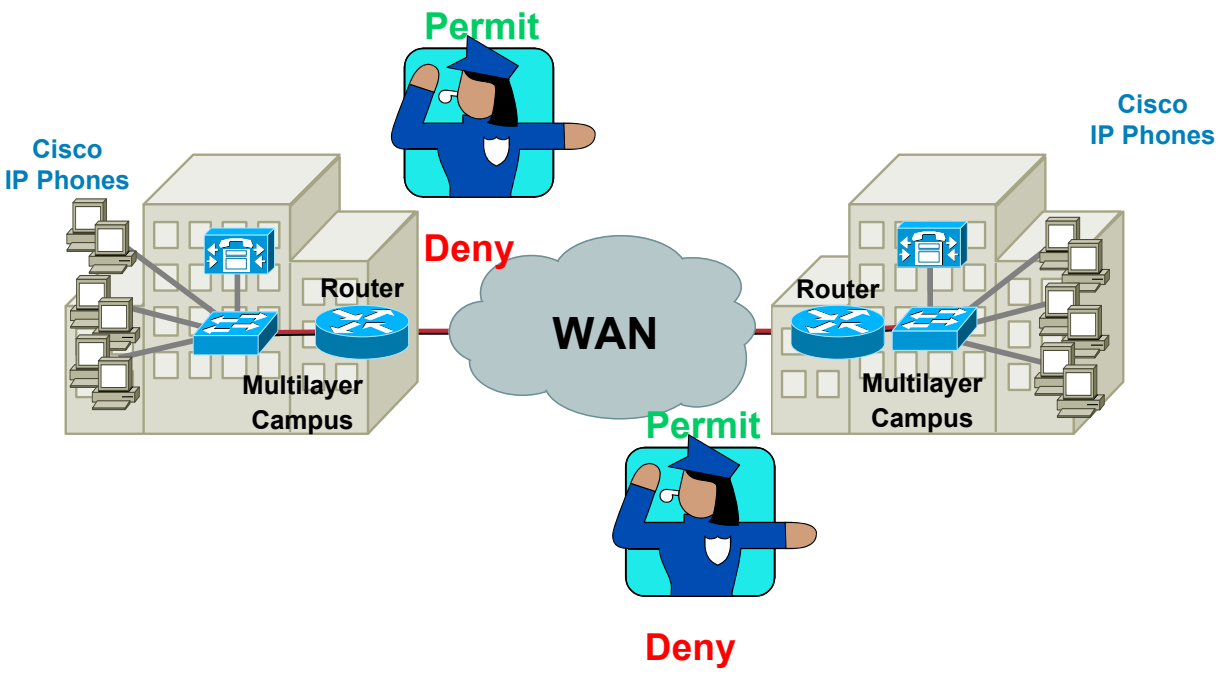
Terminology Review

Classifying Traffic

- ACLs
- CoS / IP Precedence / DSCP
- IP RTP
- NBAR
- RSVP
- Trust

Classifying Traffic
Access Control Lists

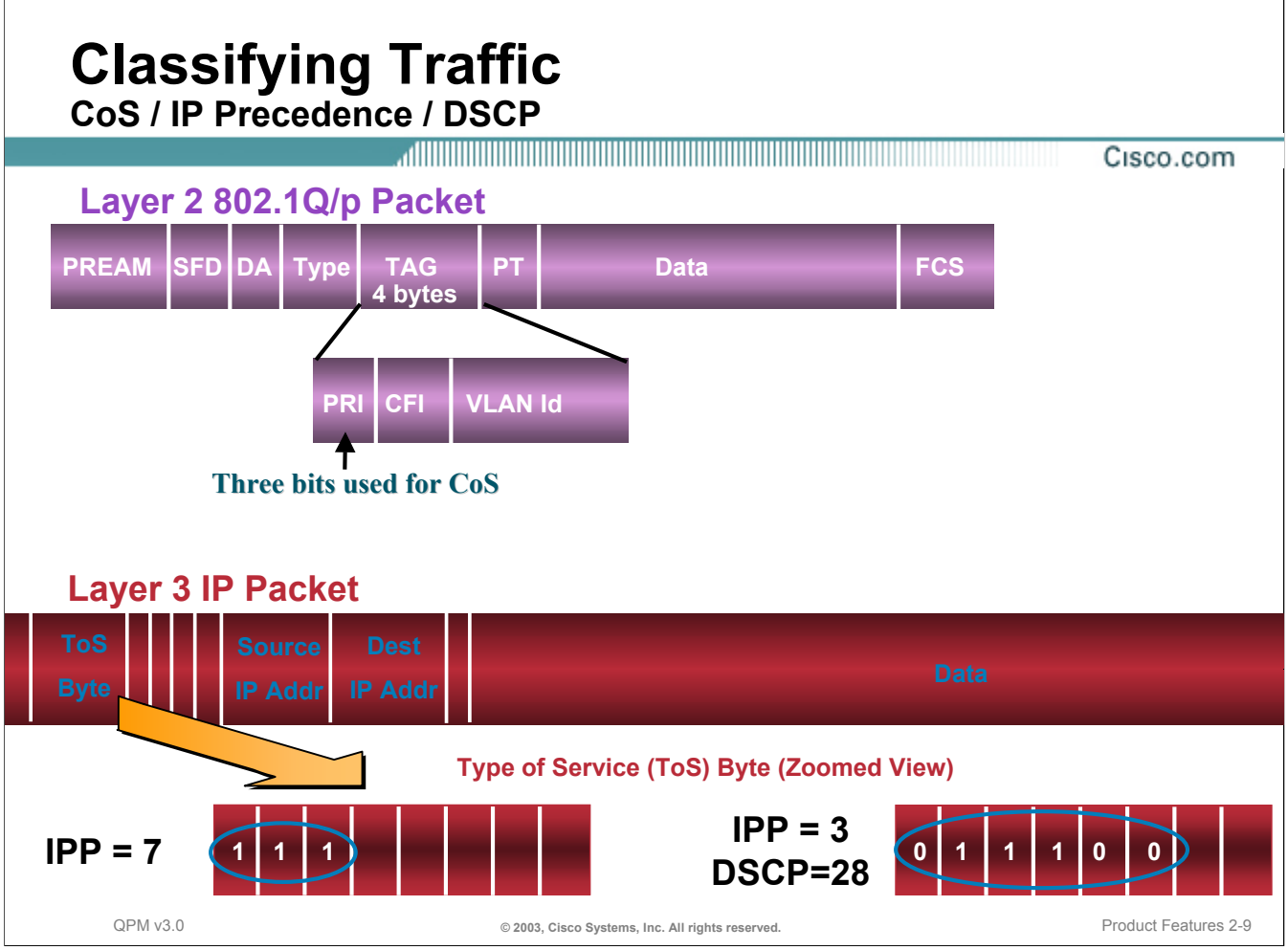
Cisco.com



Classifying Traffic - Access Control Lists

An access control list (ACL) consists of one or more access control entries (ACEs) that collectively define a network traffic profile. This profile can then be referenced by Cisco IOS® features such as traffic filtering, priority or custom queuing, dynamic access control, encryption, Telnet access, and so on. Each ACE includes an action element ("permit" or "deny") and a filter element based upon criteria such as source address, destination address, protocol, protocol-specific parameters, and so on.

Traffic in the network can be controlled or filtered by using ACLs. ACLs permit or deny the transport of packets into or out of interfaces. In addition to using ACLs for implementing a QoS policy, ACLs are commonly used to provide network security.



Classifying Traffic - CoS / IP Precedence / DSCP

In order to implement end-to-end quality of service, packets traversing the network must first be classified or colored in some way. The packet is generally colored at the first inbound interface it encounters into the network. The color is typically carried with the packet throughout its journey and used by various QoS mechanisms to determine how the packet is serviced for forwarding. Packets can be colored by the end-user application, by Policy Based Routing, or by Committed Access Rate (CAR) in the routers.

Packets can be marked as important by “coloring” the packet using layer 2 Class of Service (CoS) settings in the User Priority bits of the 802.1p portion of the 802.1Q header, or by setting various bits in the IP header. The IP header can be colored in one of two ways. Setting the IP Precedence (IPP) value, the first three bits in the ToS (Type of Service) field located in the IP packet header, allow for eight (0 – 7) different levels of coloring. The newer DSCP (differentiated services code point) value, the first six bits in the ToS (Type of Service) field located in the IP packet header, allow for 64 (0 - 63) different levels of coloring. As illustrated, the bits used by both mechanisms overlap, so one would generally utilize either ToS or DSCP values in the network, but not both.

Changing the packet’s color at the “edge” of the network can affect how the packet is handle on its entire path through the core of the network. Interfaces which use WFQ, WRED, and WWR policy properties, automatically recognize and use the packets color when queuing packets. Other QoS properties such as priority queuing and custom queuing, as well as shaping and limiting policies do not automatically use the packet’s color, therefore an additional policy on the outbound interface that recognizes the packets color as its matching criteria can be used for these services.

Classifying Traffic
CoS / IP Precedence / DSCP

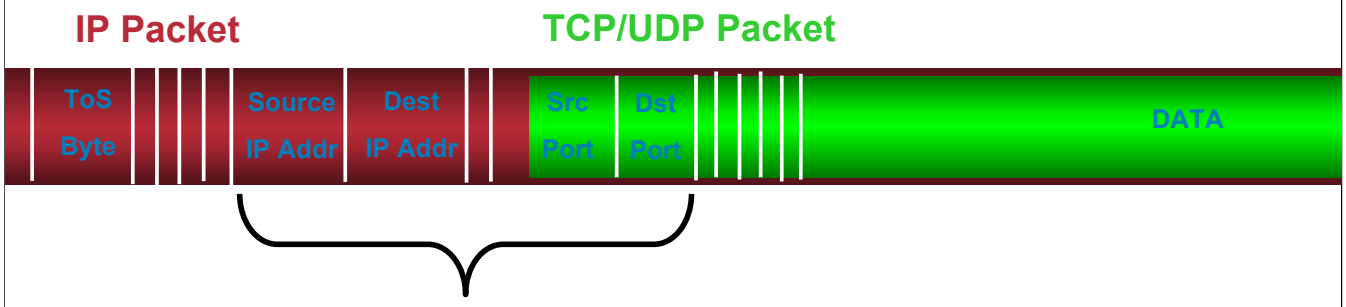
Layer 2 Class of Service	IP Precedence	DSCP
CoS 0	Routine (IP precedence 0)	0-7
CoS 1	Priority (IP precedence 1)	8-15
CoS 2	Immediate (IP precedence 2)	16-23
CoS 3	Flash (IP precedence 3)	24-31
CoS 4	Flash-override (IP precedence 4)	32-39
CoS 5	Critical (IP precedence 5)	40-47
CoS 6	Internet (IP precedence 6)	48-55
CoS 7	Network (IP precedence 7)	56-63

Classifying Traffic - CoS / IP Precedence / DSCP

This illustration provides a reference for mapping layer 2 CoS and layer 3 IP Precedence (IPP) and DSCP. For example, all IP phone RTP packets should be tagged with values of CoS=5 for the Layer 2 802.1p settings and IP Precedence=5 for Layer 3 settings. Additionally, all voice control packets should be tagged with a Layer 2 CoS value of 3 and a Layer 3 ToS of 3. If using Differentiated Service Code Points (DSCP), a wider range of values can be assigned to identify a larger range of traffic profiles.

Classifying Traffic
Source / Destination Address or Port

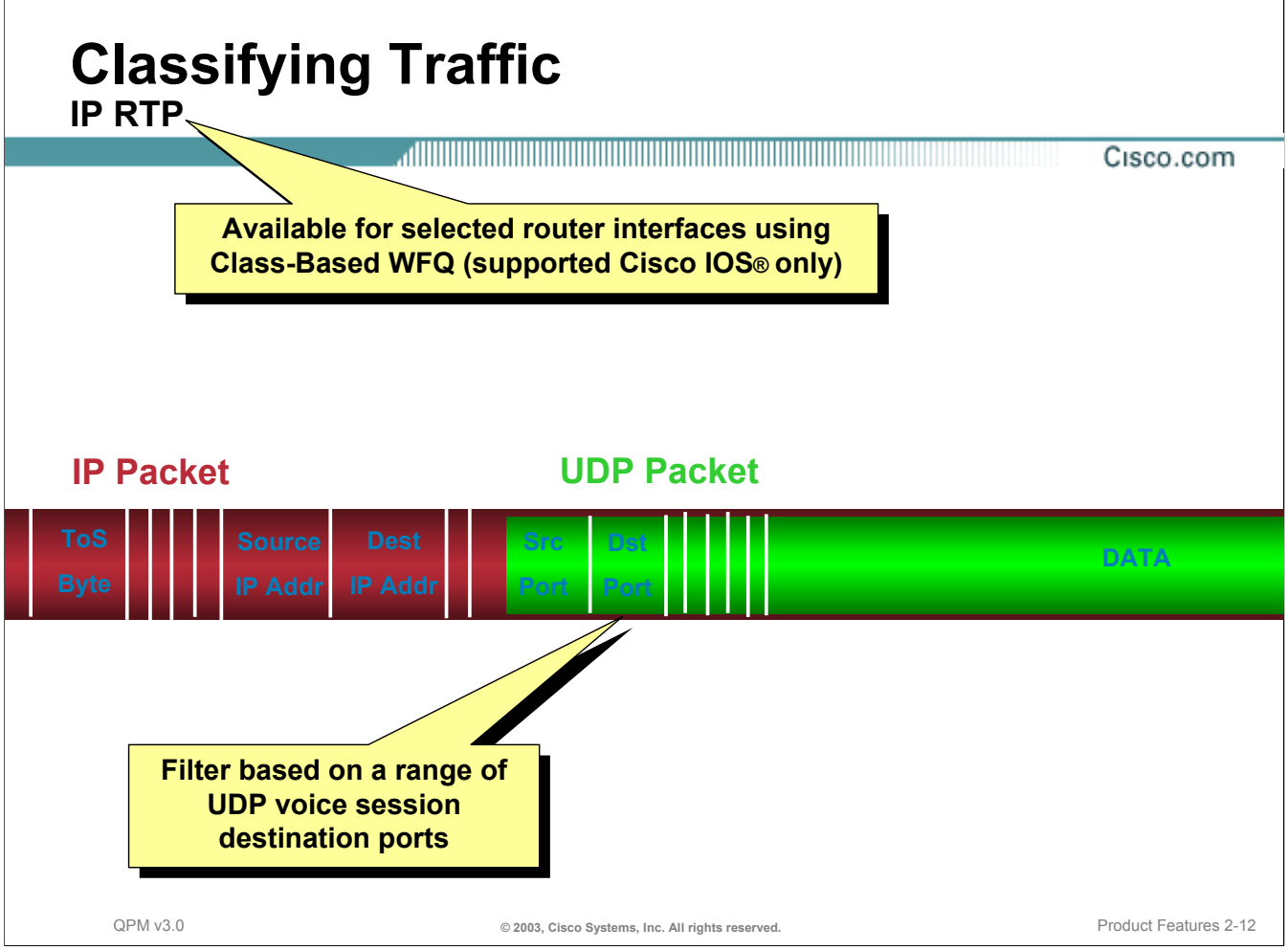
Cisco.com



Filter based on IP address (source /or destination)
Filter based on UDP or TCP application port (source /or destination)

Classifying Traffic - Source Destination Address or Port

A simple, yet effective way to classify or filter traffic on the network, is to simply evaluate where the traffic is coming from or where is it going. This information is available in the layer 3 IP packet header. Packets can be filtered by the IP addresses or the TCP or UDP application port in either direction. This technique can be used to prioritize traffic to or from a specific node or application.



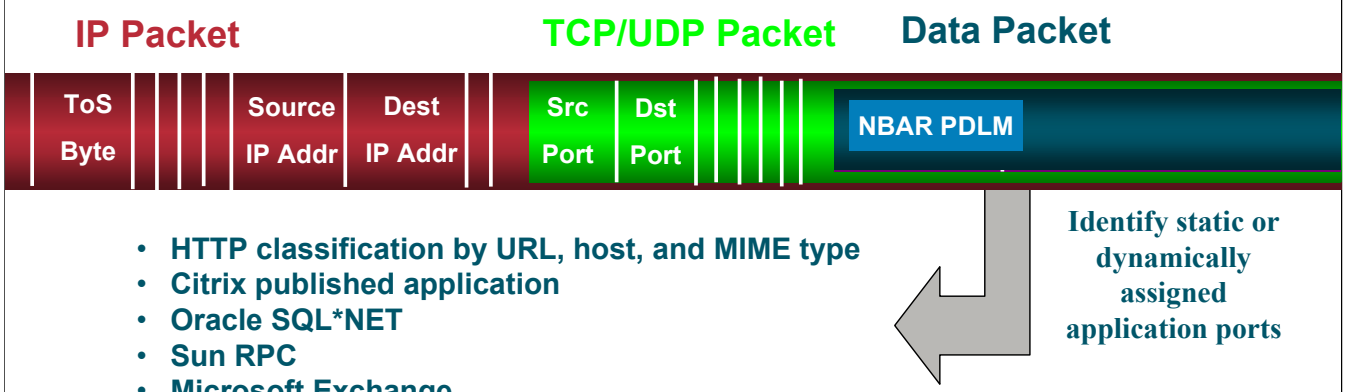
Classifying Traffic - IP RTP

For selected router interfaces that are utilizing Class Based Weighted Fair Queuing (CBWFQ), Voice over IP (VoIP) traffic sessions can be filtered by evaluating the UDP destination ports. As indicated, it is important to correctly classify and transport VoIP traffic to ensure quality of service in an IP Telephony network. The entire voice port range is UDP ports 16384 to 32767.

Note that the software version of the router must support IP RTP Priority with CBWFQ. Refer to Chapter 5 for a complete list of supported devices and QoS techniques supported by software release versions.

Classifying Traffic
Network-Based Application Recognition (NBAR)

Cisco.com



- HTTP classification by URL, host, and MIME type
- Citrix published application
- Oracle SQL*NET
- Sun RPC
- Microsoft Exchange
- UNIX r commands
- VDOLive
- RealAudio
- Microsoft Netshow
- File Transfer Protocol (FTP)
- StreamWorks
- Trivial File Transfer Protocol (TFTP)

Classifying Traffic - NBAR

Classifying applications sounds like a simple task, but it is often a hard undertaking. The difficulty is that today's Internet-based and client-server applications make it difficult for the network to identify and provide the proper level of control you need.

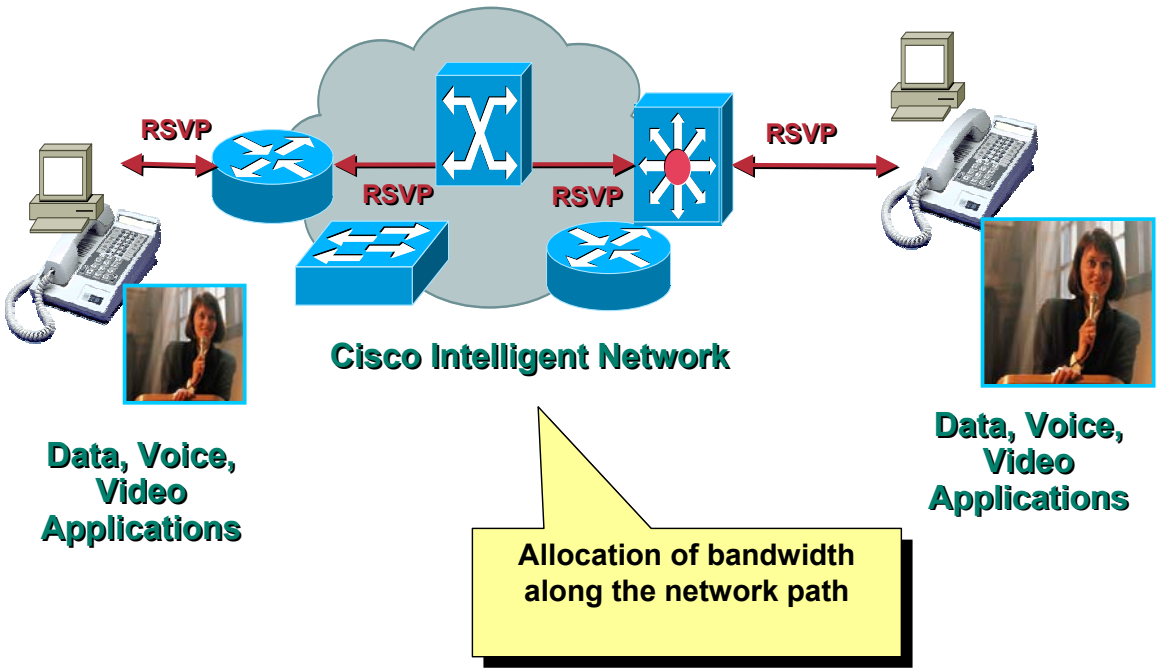
Network Based Application Recognition (NBAR) solves this problem by adding intelligent network classification to your infrastructure. NBAR is a new classification engine that can recognize a wide variety of applications, including web-based and client/server applications that dynamically assign TCP or UDP port numbers. Once the application is recognized, the network can invoke specific services for that particular application. NBAR currently works with QoS features to ensure that the network bandwidth is best used to fulfill your objectives. These features include the ability to guarantee bandwidth to critical applications, limit bandwidth to other applications, drop selective packets to avoid congestion, and color packets appropriately so that your network and the service provider's network can provide the proper QoS from end to end.

NBAR supports a wide range of network protocols, including the common protocols that were once difficult to classify. (Refer to figure above.)

NBAR can also classify static-port protocols such as those currently classifiable with access control lists (ACLs).

Classifying Traffic
Resource Reservation Protocol (RSVP)

Cisco.com



Classifying Traffic - RSVP

A more sophisticated form of filtering 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. Once 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 unacceptable jitter, delay, and packet drop can be avoided.

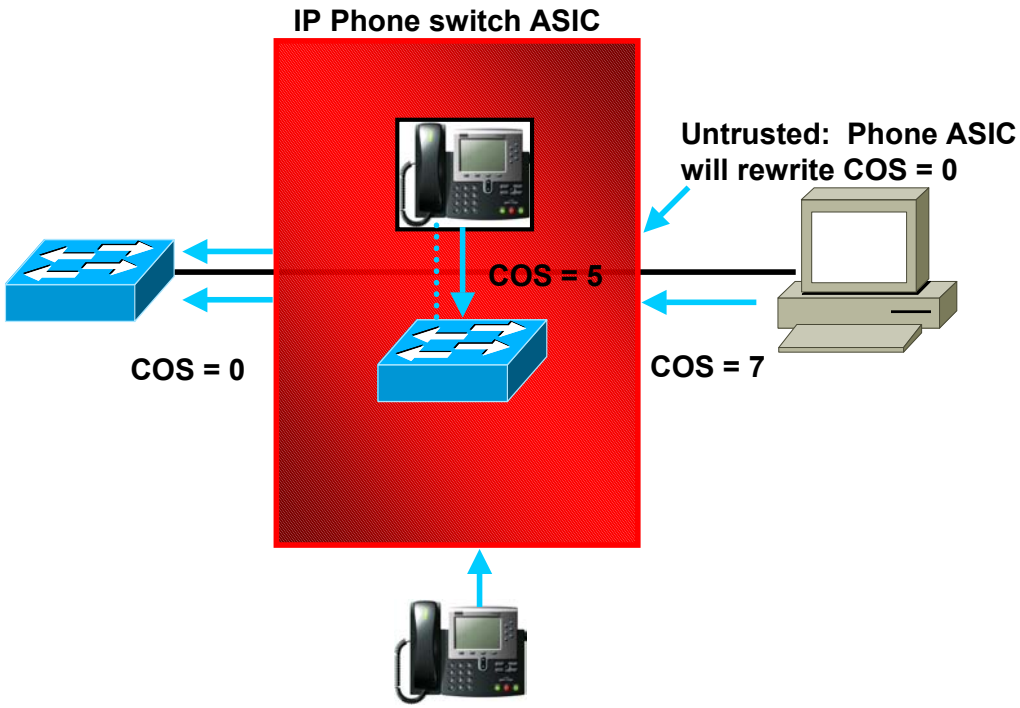
RSVP is typically used by multicast applications. With multicasting, an application sends a stream of traffic to several destinations. For example, the Cisco IP/TV application can provide several audio-video programs to users. If a user accesses one of the provided programs, IP/TV sends a stream of video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

Network devices consolidate multicast traffic to reduce bandwidth usage. Thus, if there are 10 users for a traffic flow behind a router, the router sees one traffic flow, not 10. In unicast traffic, the router sees 10 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 RSVP unicast applications. In other words, RSVP 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.

Classifying Traffic
Trust Boundaries - Catalyst® 6000

Cisco.com



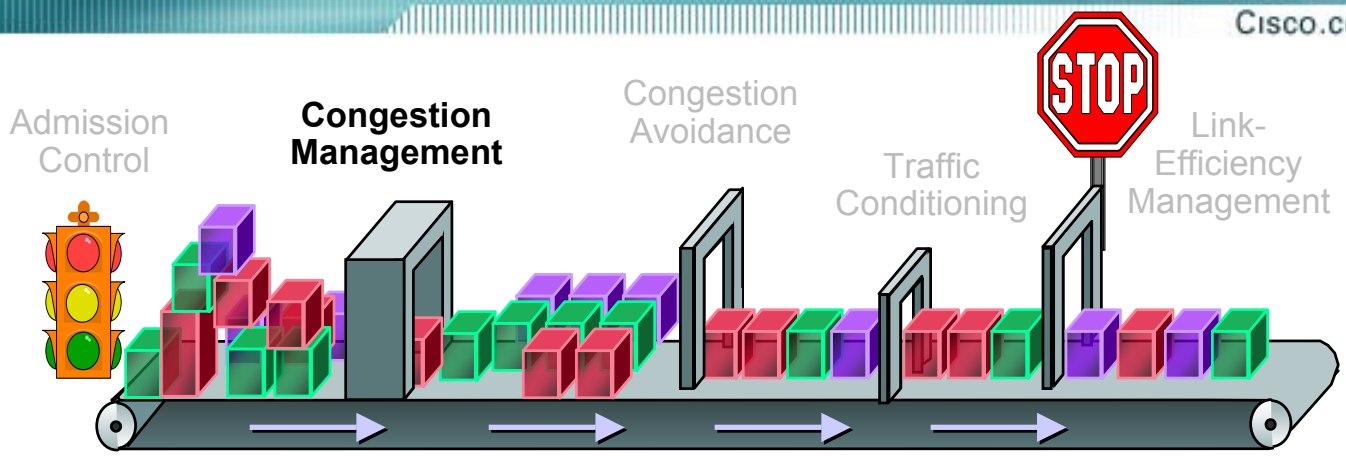
QPM v3.0

Classifying Traffic - Trust Boundaries

Coloring a packet or flow with a specific priority establishes a trust boundary that must be enforced. The concept of trust is integral to implementing QoS on Catalyst 6000 switches. Once end devices have a set class of service (CoS) or type of service (ToS), the switch port has the option of trusting them or not. If the port trusts the settings, it does not need to do any reclassification; if it does not trust the settings, then it must perform reclassification for appropriate QoS. QPM allows ports to be configured as trusted or untrusted, on both the individual port level and the device group level. On trusted ports, the received CoS/ToS values are used. On untrusted ports, the received CoS/ToS values are replaced with the port CoS/ToS value.

Catalyst 6000 switches (but not Catalyst 6000 switches with Supervisor IOS) provide the additional capability to extend the trust boundary. For example, this is particularly useful for a VoIP network where you have a PC-IP phone-Catalyst 6000 setup. You can ensure that voice packets retain their high precedence settings by extending the trust boundary to the IP phone and setting it to "untrusted" so that the precedence of all packets received from the PC is negated.

This page intentionally left blank.



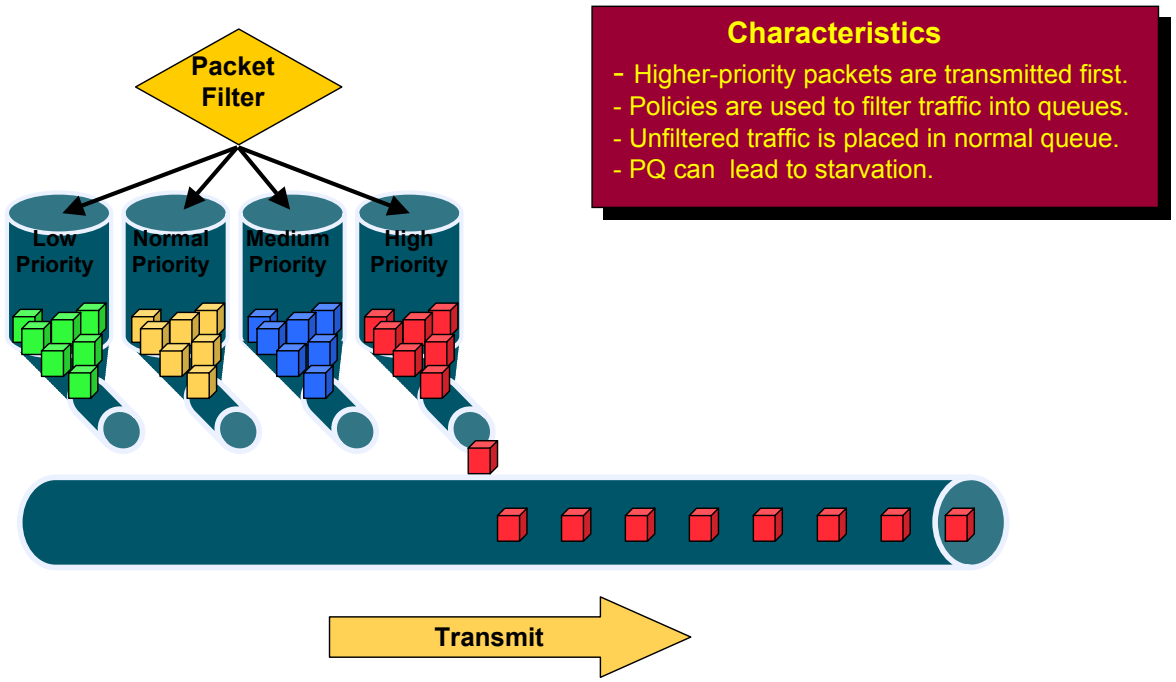
Terminology Review

Queuing Traffic - Congestion Management

- Priority Queuing (PQ)
- Custom Queuing (CQ)
- Weighted Fair Queuing (WFQ)
- Class Based WFQ (CBWFQ)
- IP RTP Priority
- Low Latency Queuing (LLQ)
- 2Q2T/1P2Q2T (Catalyst 6000)
- Weighted Round Robin (WRR)

Queuing Traffic
Priority Queuing (PQ)

Cisco.com



Characteristics

- Higher-priority packets are transmitted first.
- Policies are used to filter traffic into queues.
- Unfiltered traffic is placed in normal queue.
- PQ can lead to starvation.

Priority Queuing

One type of Policy Action which may utilize coloring is Priority Queuing (PQ). Coloring for PQ is not an automatic policy action and must be defined in the QoS policy. PQ ensures that important traffic gets the fastest handling at each point where it is used. It was designed to give strict priority to important traffic. Priority queuing can prioritize packets according to network protocol (IP, IPX, or AppleTalk), incoming interface, packet size, source/destination address, and so on.

In PQ, each packet is placed in one of four queues: High, Medium, Normal, or Low based on its classification. Packets that are not classified by this priority-list mechanism fall into the Normal queue.

During transmission, the algorithm gives higher-priority queues absolute preferential treatment over low-priority queues. All packets in the High Priority queue are serviced prior to transmitting packets in the Medium Priority queue. And the packets in the Low Priority queue are not transmitted until all High, Medium, and Normal packets are serviced.

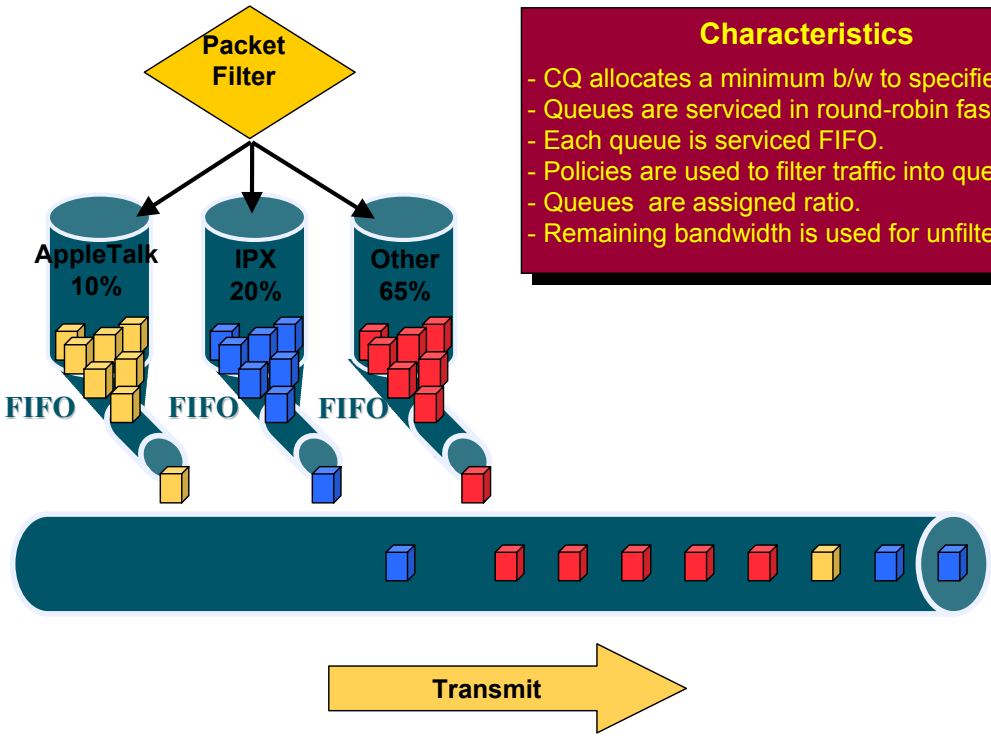
PQ is useful for making sure that mission-critical traffic traversing various WAN links gets priority treatment. For example, Cisco uses PQ to ensure that important Oracle-based sales reporting data gets to its destination ahead of other less critical traffic. PQ currently uses static configuration and thus does not automatically adapt to changing network requirements.

Although PQ provides a simple and intuitive approach to scheduling, it can cause starvation on the lower priority traffic, PQ can cause queuing delays that could have effected higher priority traffic to be randomly transferred to lower priority traffic. Depending on the bandwidth used by higher-priority packets, this could result in lower priority traffic never being transmitted.

To avoid inflicting these conditions on lower priority traffic, you can use traffic shaping or Committed Access Rate (CAR) to rate-limit the higher priority traffic. (These techniques are discussed next.) Priority queuing introduces extra overhead that is acceptable for slow interfaces, but may not be acceptable for higher-speed interfaces such as Ethernet. With priority queuing enabled, the system takes longer to switch packets because the processor card needs to classify the packets.

Queuing Traffic
Custom Queuing (CQ)

Cisco.com



Characteristics

- CQ allocates a minimum b/w to specified traffic.
- Queues are serviced in round-robin fashion.
- Each queue is serviced FIFO.
- Policies are used to filter traffic into queues.
- Queues are assigned ratio.
- Remaining bandwidth is used for unfiltered traffic.

Custom Queuing

Another type of QoS policy action which may utilize coloring is Custom Queuing (CQ). Coloring for CQ is not automatic and must be defined in the policy. For networks that need to provide a guaranteed level of service for all traffic, Cisco offers custom queuing. CQ allows a customer to reserve a percentage of bandwidth for specified protocols. Customers can define up to 16 output queues for normal data and an additional queue for system messages such as LAN keep-alive messages (routing packets are not assigned to the system queue). Cisco routers service each queue sequentially, transmitting a configurable percentage of traffic on each queue before moving on to the next one. CQ guarantees that mission-critical data is always assigned a certain percentage of the bandwidth, but also assures predictable throughput for other traffic.

To provide this feature, Cisco routers determine how many bytes should be transmitted from each queue, based on the interface speed and the configured percentage. When the calculated byte count from a given queue has been transmitted, the router completes transmission of the current packet and moves on to the next queue, servicing each queue in a round-robin fashion.

Independent tests of Cisco routers have shown that when a line is saturated with traffic from multiple protocols, traffic carried on the line maintains allocated bandwidth percentages to within a few percentage points of what was specified in the configuration.

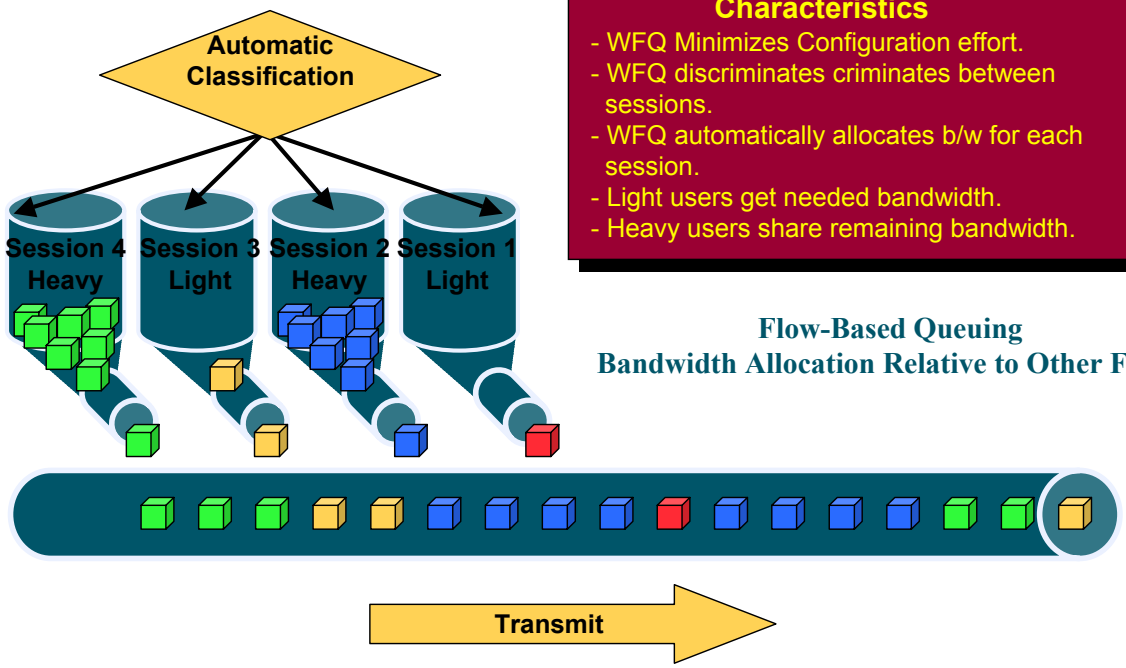
A key advantage of Cisco's "bandwidth reservation" technique is that unused bandwidth can be dynamically allocated to any protocol that requires it. For example, if SNA is allocated 50 percent of the bandwidth but uses only 30 percent, the next protocol in the queue can take up the extra 20 percent until SNA requires it.

Additionally, CQ maintains the predictable throughput of dedicated lines by efficiently using packet-switching technologies such as Frame Relay.

The bandwidth reservation must be in increments of 5% 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.

Queuing Traffic
Weighted Fair Queuing (WFQ)

Cisco.com



Characteristics
- WFQ Minimizes Configuration effort.
- WFQ discriminates criminates between sessions.
- WFQ automatically allocates b/w for each session.
- Light users get needed bandwidth.
- Heavy users share remaining bandwidth.

Flow-Based Queuing
Bandwidth Allocation Relative to Other Flows

Weighted Fair Queuing

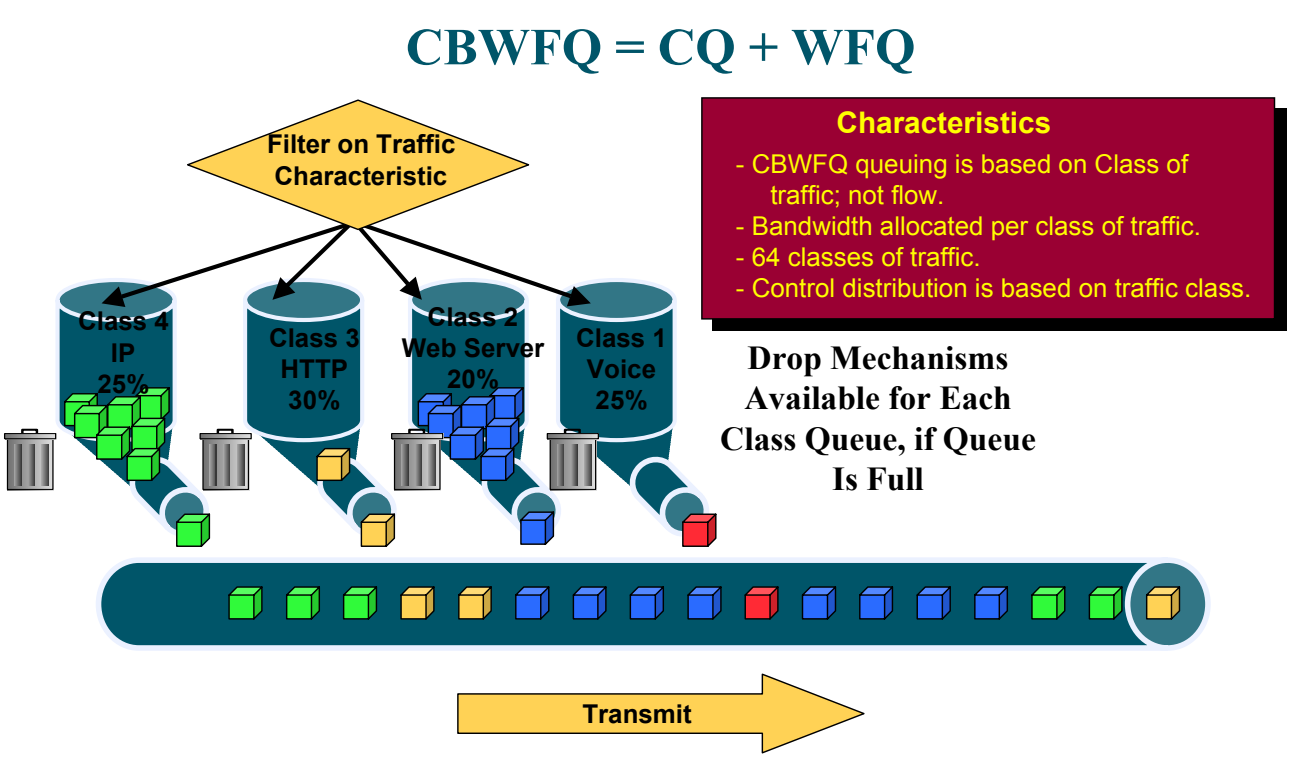
Weighted Fair Queuing (WFQ) is an intelligent traffic prioritization scheme. It provides consistent response time to heavy and light users alike without excessive configuration. WFQ is a flow based queuing algorithm that does two things simultaneously: it schedules interactive traffic to the front of the queue to reduce response time, and it fairly shares the remaining bandwidth between high bandwidth flows. All of this is done automatically without classification policies!

WFQ automatically determines packet priority based on the color of the packet. This highlights the need for proper coloring of packets at the edge of the network. Because WFQ is flow base, it automatically adapts to changing network traffic conditions. WFQ efficiently uses available bandwidth by transmitting all low priority packets waiting if no high priority packets are queued, no bandwidth is wasted if packets are waiting.

WFQ makes response time consistent by recognizing sessions and dividing up bandwidth accordingly. Sessions are prioritized and assigned bandwidth based on the color of the packet. A packet with IP precedence 7 is of higher priority than a packet with IP precedence of 3, and will be serviced first. To divide up the bandwidth, each sessions precedence value + 1, are added together to get the divisor of the ratio. The numerator is the precedence value + 1. For example 4 sessions have precedence value 4, two have 7, and one each for 0, 1, and 2. The divisor equals 5+5+5+5+8+8+1+2+3 = 42. So each session with IP precedence of 4 gets 5/42 of bandwidth, etc.

Queuing Traffic
Class-Based WFQ (CBWFQ)

Cisco.com



Class Based Weighted Fair Queuing

An effective use of Class-based weighted fair queuing (CBWFQ) would be to guarantee bandwidth to a few critical applications to ensure reliable application performance.

CBWFQ combines the best characteristics of weighted fair queuing and custom queuing. CBWFQ uses WFQ processing to give higher weight to high priority traffic, but derives that weight from classes that you create on the interface. 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.

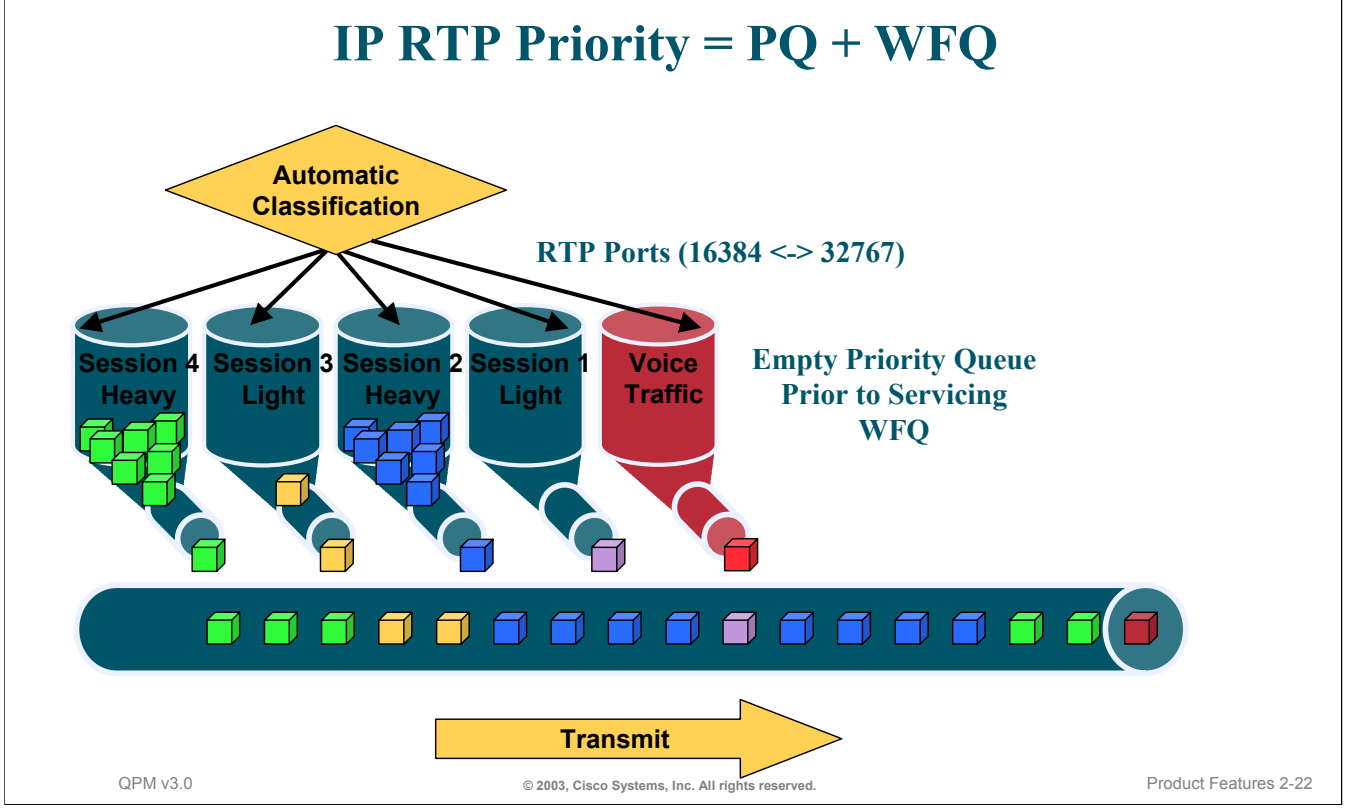
With CBWFQ, you can create up to 64 classes on an interface. (Unlike WFQ, queues are not automatically based on IP precedence or DSCP value.) CBWFQ also lets you control the drop mechanism used when congestion occurs on the interface. You can use WRED for the drop mechanism, and configure the WRED queues, 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 IP precedence is not equal.

The disadvantage of CBWFQ is that, like custom queuing, you must create policy statements on the interface to place the traffic in the classes.

If CBWFQ is available on an interface, it is recommended that you use CBWFQ instead of custom queuing.

Queuing Traffic
IP RTP Priority

Cisco.com



IP RTP Priority Queuing

The IP RTP (Real-Time Transport Protocol) Priority feature provides a strict priority queuing scheme for delay-sensitive data such as voice. Voice traffic can be identified by its RTP port numbers and classified into a priority queue. The result is that voice is serviced as strict priority in preference to other nonvoice traffic. IP RTP Priority is especially useful on slow-speed links whose speed is less than 1.544 Mbps.

The IP RTP Priority feature allows the user to specify a range of User Datagram Protocol (UDP)/RTP ports whose traffic is guaranteed strict priority service over any other queues or classes using the same output interface. Strict priority means that if packets exist in the priority queue, they are dequeued and sent first—that is, before packets in other queues are dequeued.

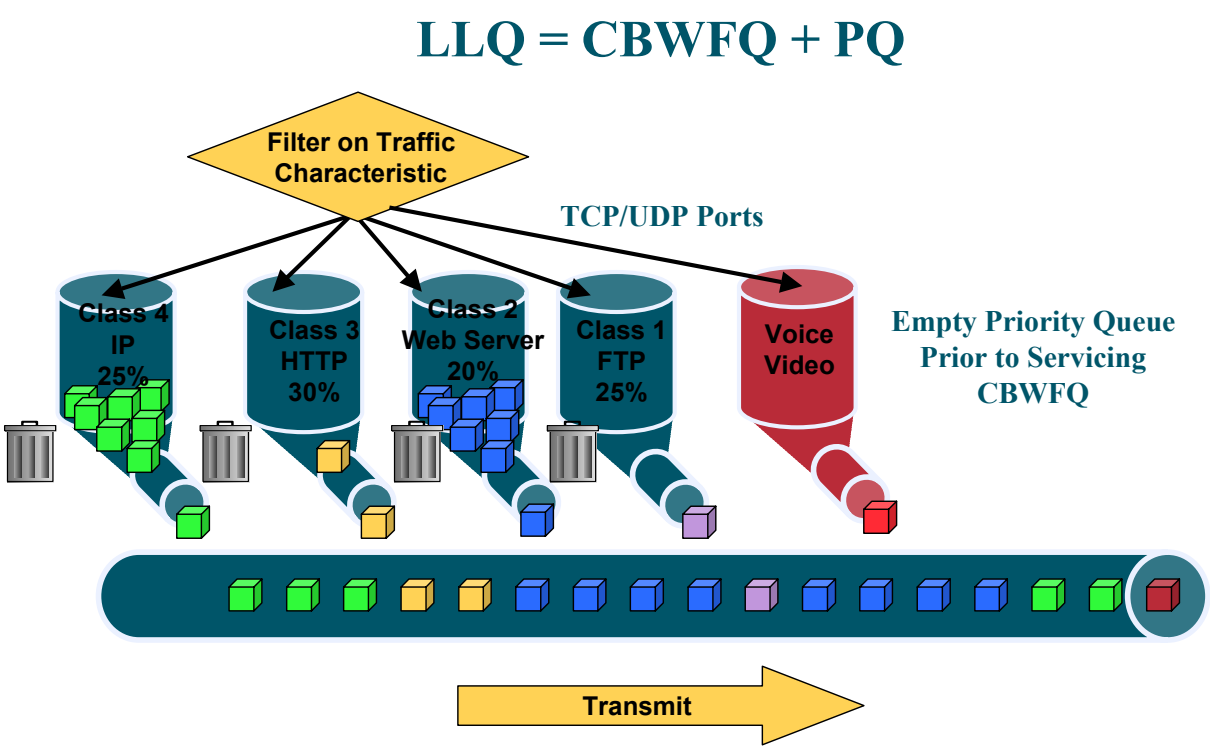
The IP RTP Priority feature does not require that you know the port of a voice call. Rather, the feature gives you the ability to identify a range of ports whose traffic is put into the priority queue. Moreover, the entire voice port range of 16384 to 32767 can be specified to ensure that all voice traffic is given strict priority service.

This feature can be used in conjunction with either Weighted Fair Queuing (WFQ) or Class-Based WFQ (CBWFQ) on the same outgoing interface. In either case, traffic matching the range of ports specified for the priority queue is guaranteed strict priority over other CBWFQ classes or WFQ flows; packets in the priority queue are always serviced first. The bandwidth allocated to the IP RTP Priority queue counts as part of the total allocated CBWFQ queue bandwidth.

Note: IP RTP priority cannot be configured on the interface when Frame Relay Traffic Shaping is enabled. IP RTP priority is not available on VIP cards.

Queuing Traffic
Low-Latency Queuing (LLQ)

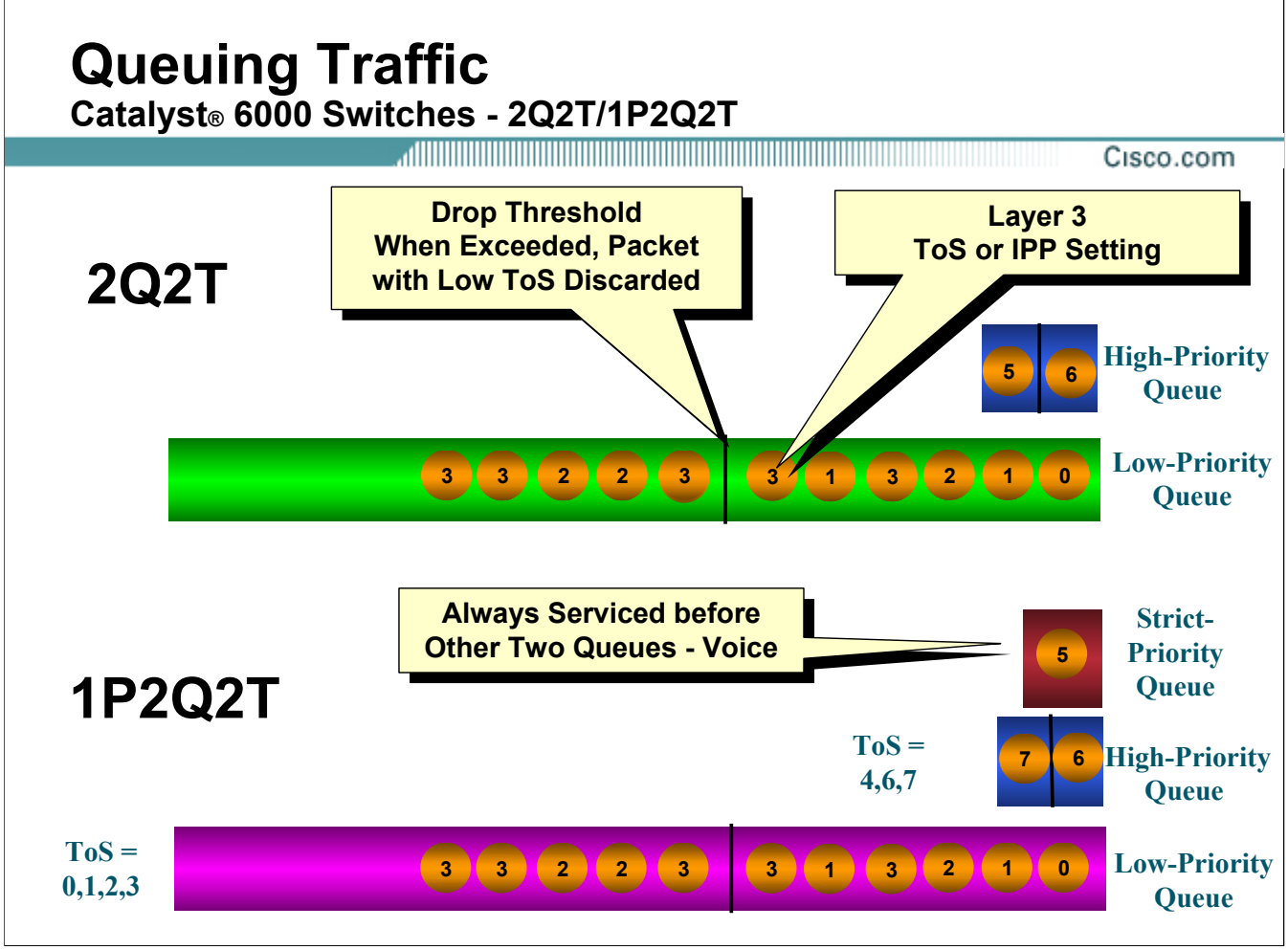
Cisco.com



Low Latency Queuing

Low latency queuing (LLQ) is used with CBWFQ to bring strict priority queuing to CBWFQ. 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 within the CBWFQ queuing properties. When several types of traffic on an interface are configured as priority classes, all these types of traffic are queued in the same, single, strict priority queue.



Queuing on Catalyst 6000 Switches

2Q2T (two standard queues, 2 thresholds) and 1P2Q2T (one strict priority queue, two standard queues, 2 thresholds) queuing on Catalyst 6000 family switches uses a packet's precedence setting to determine how that packet is serviced on the port.

2Q2T queuing uses two queues:

- One high-priority queue with two thresholds
- One low-priority queue with two thresholds

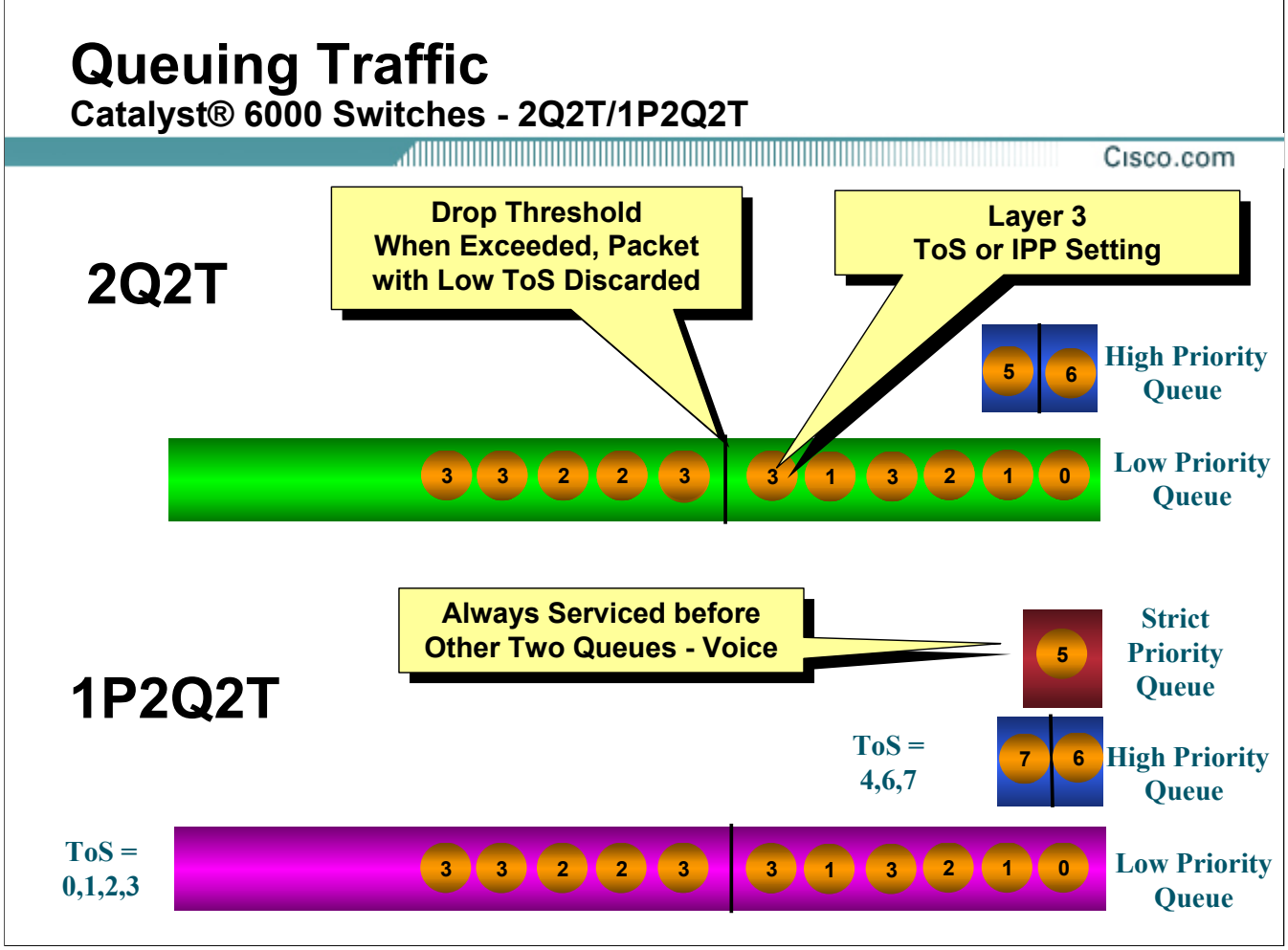
1P2Q2T queuing uses three queues:

- 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. Voice traffic can be marked or colored 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.

On 1P2Q2T interfaces, the default QoS configuration allocates 90 percent of the total transmit queue size to the low-priority standard queue, 5 percent to the high-priority standard queue, and 5 percent to the strict-priority queue.

For 1P2Q2T interfaces, the default QoS configuration assigns all traffic with IP Precedence 5 to the strict priority queue, traffic with IP Precedence 4, 6, and 7 to the high-priority standard queue, and traffic with IP Precedence 0, 1, 2, and 3 to the low-priority standard queue.



1P2Q2T Drop Thresholds - continue

Using the low priority standard transmit queue, drop threshold 1, the switch drops frames with CoS 0 or 1 when the low-priority transmit queue buffer is 80 percent full. Using the low priority standard transmit queue, drop threshold 2, the switch drops frames with CoS 2 or 3 when the low-priority transmit queue buffer is 100 percent full.

Using the high priority standard transmit queue, drop threshold 1, the switch drops frames with CoS 4 when the high-priority transmit queue buffer is 80 percent full. Using the high priority standard transmit queue, drop threshold 2, the switch drops frames with CoS 6 or 7 when the high-priority transmit queue buffer is 100 percent full.

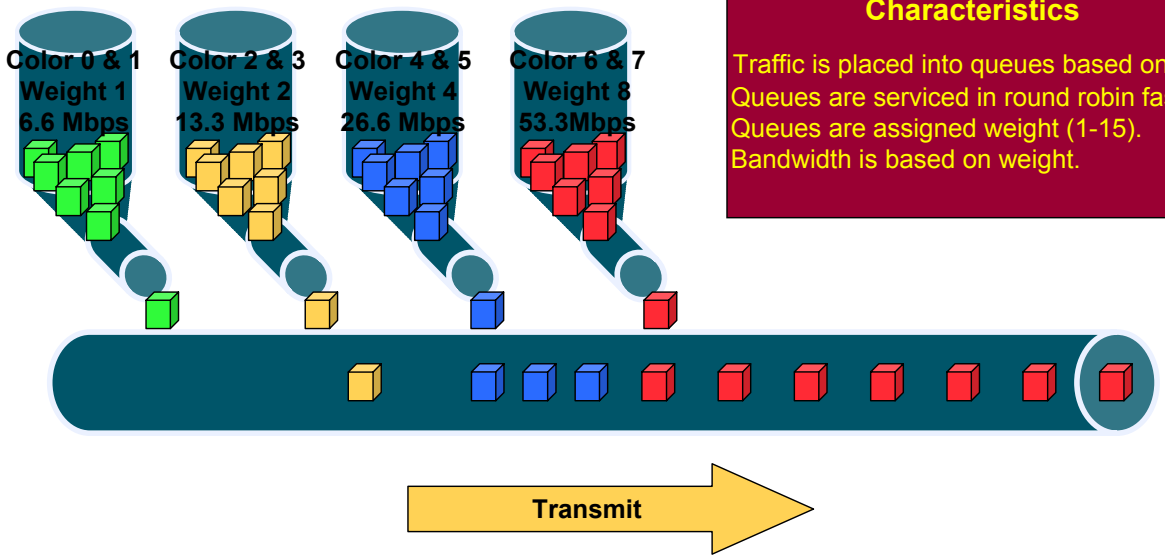
Frames with CoS 5 go to the strict-priority transmit queue (queue 3), where the switch drops frames only when the buffer is 100 percent full.

These threshold values are configurable.

Queuing Traffic
Weighted Round Robin (WRR)

Cisco.com

Available on Cisco 8510 Fast Ethernet Ports Only!



Characteristics

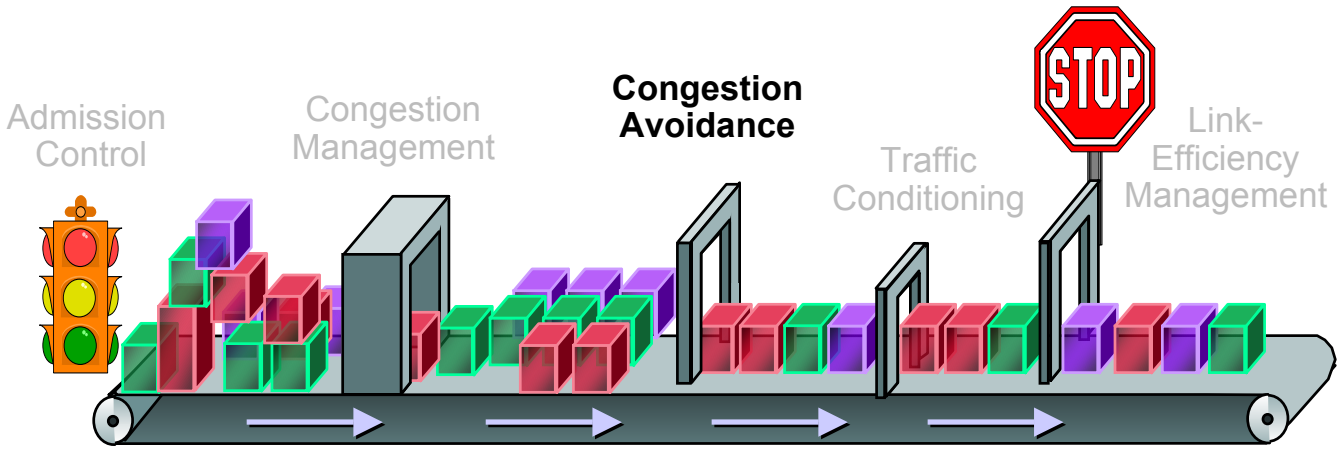
Traffic is placed into queues based on color.
Queues are serviced in round robin fashion.
Queues are assigned weight (1-15).
Bandwidth is based on weight.

Weighted Round Robin Queuing

Weighted Round Robin (WRR) is a traffic prioritization scheme for the Catalyst 8510's Fast Ethernet ports only.

There are four queues defined per interface. Traffic is placed in the queues based on the first two bits of the IP precedence (again showing the importance of correctly coloring the packets at the network's edge.) Each queue is assigned a weight, which will determine the portion of the interface's bandwidth available to the queue. The higher the queue's weight, the higher it's effective bandwidth.

Note that the queue containing IP precedence 6 and 7 packets does not necessarily have to have the highest weight. The weight assigned by the user is between 1 and 15. The sum of all four weights can not exceed 15. Effective bandwidth for the queue is determined by taking the queue's weight divided by the sum of all queues weight multiplied by the interface's bandwidth.



Terminology Review

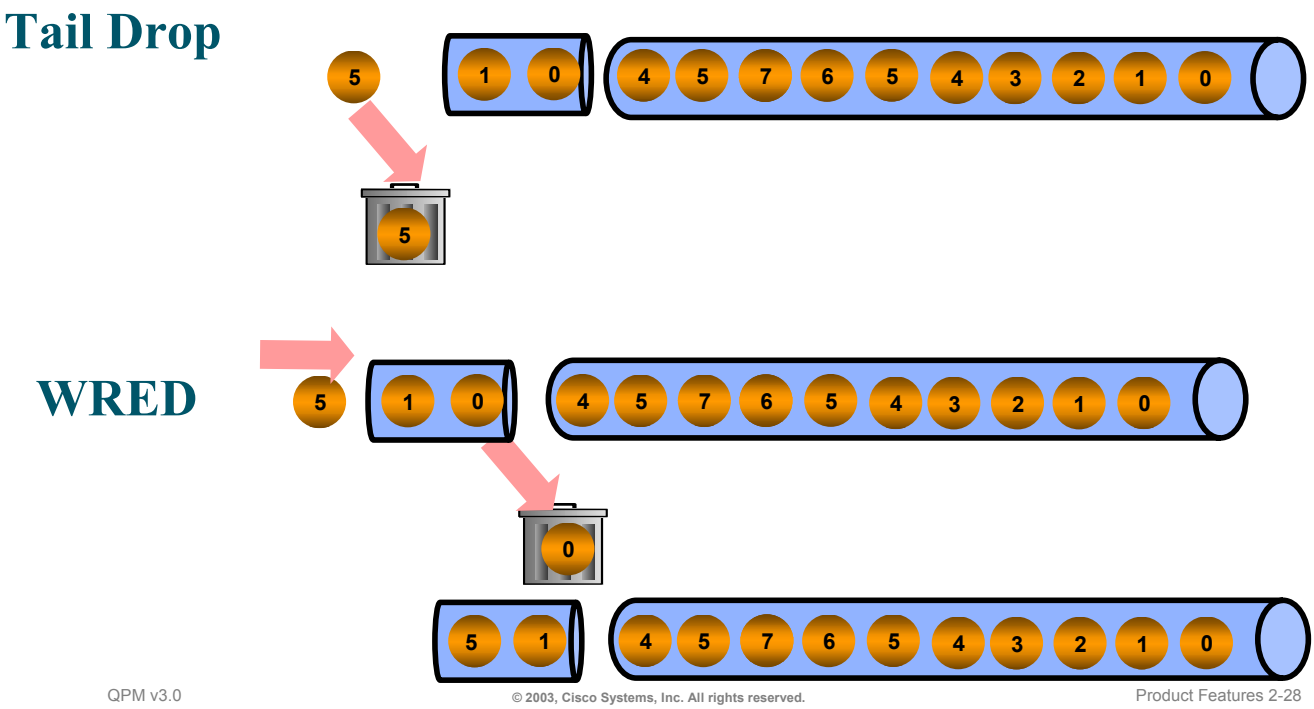
Dropping Traffic - Congestion Avoidance

- Tail Drop
- Weighted Random Early Detection (WRED)

Dropping Traffic
Tail Drop / WRED

Cisco.com

Congestion-Avoidance Mechanism



Dropping Traffic - Congestion Avoidance

A queuing technique can be configured on a device's interface to manage how packets are handled when the interface starts to get congested. The queuing techniques available for congestion avoidance are either Tail or Weighted Random Early Detection (WRED).

With Tail Drop, when the interface buffer is full, the incoming packet is simply dropped.

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.

To determine which packets to drop, WRED takes these things into account:

- RSVP flows are given precedence over non-RSVP flows, to ensure that time-critical packets are transmitted as required.
- The IP precedence 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. 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.

Dropping Techniques - Continue

When configuring an interface to use WRED, on a device using IOS software version 12.0 and a versatile interface processor (VIP), it automatically uses distributed WRED. Distributed WRED takes advantage of the VIP.

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 they retransmit 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.

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 coloring you perform on edge devices can then affect the WRED interfaces throughout the network.

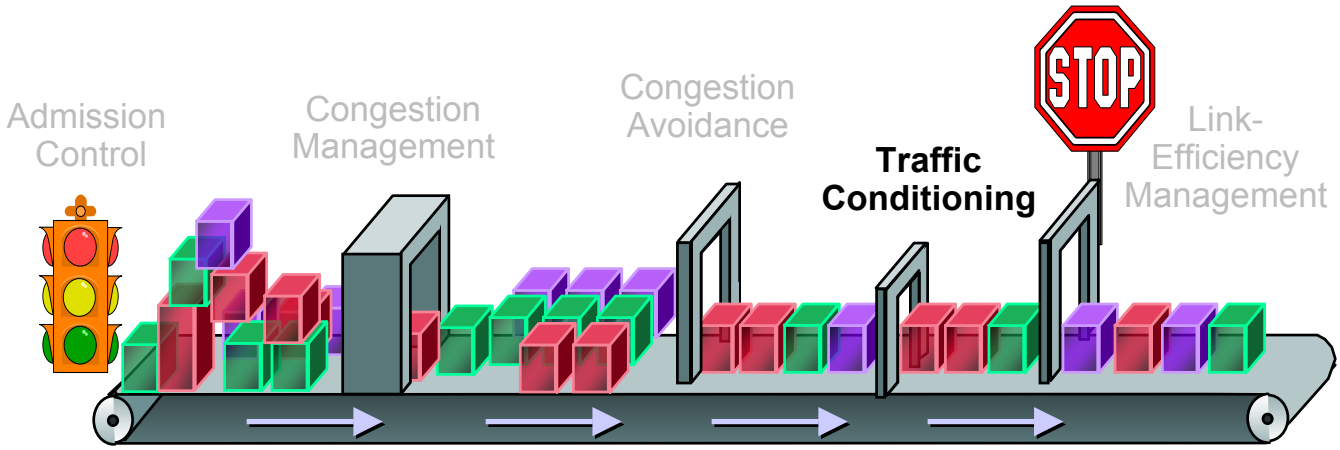
Policy Requirements for Weighted Random Early Detection Interfaces

Weighted random early detection interfaces automatically favor high priority, low bandwidth traffic flows. No specific policies are needed. However, you can also create traffic shaping policies or traffic limiting policies to affect how selected traffic is handled on the interface. A shaping policy or a limiting policy can control the bandwidth available to the selected traffic. You can also create CBWFQ policies that use WRED as the drop mechanism for the class-based queues.

Remember that WRED is sensitive to the IP precedence settings in the packets. Therefore, you can create policies on inbound interfaces on the device and have those policies implemented on the outbound interfaces that use WRED. WRED automatically prioritizes the packets without the need for you to create policies on the WRED queuing interfaces, dropping packets with low priority before dropping high-priority packets.

However, you do not need to create policies on the inbound interfaces that color traffic. If packets have the same IP precedence, WRED drops packets from the highest-bandwidth flows first. However, because WRED automatically uses the IP precedence settings in packets, consider coloring all traffic that enters the device (or color the traffic at the point where it enters your network). By coloring 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.

This page intentionally left blank.



Terminology Review

Limiting Traffic - Traffic Conditioning

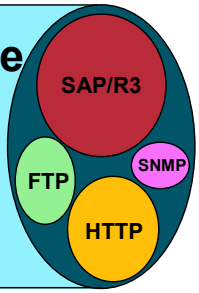
- Generic Traffic Shaping (GTS)
- Frame Relay Traffic Shaping (FRTS)
- Limiting on Routers - Committed Access Rate (CAR)
- Limiting on Switches - Catalyst 6000

Limiting Traffic
Controlling Bandwidth

Cisco.com

Manage how much of the bandwidth of an interface should be allocated to a specific traffic flow

- Affects flows even during times of little congestion
- Implemented using policies, not queuing



Shaping versus **Limiting**

- Attempts to throttle traffic
- Router buffers traffic bursts
- Packets dropped when buffers are full
- Generic Traffic Shaping (GTS)
- Frame Relay Traffic Shaping (FRTS)

- No packets dropped until rate limits reached
- All packets dropped that exceed the burst rate limit
- Committed Access Rate (CAR)

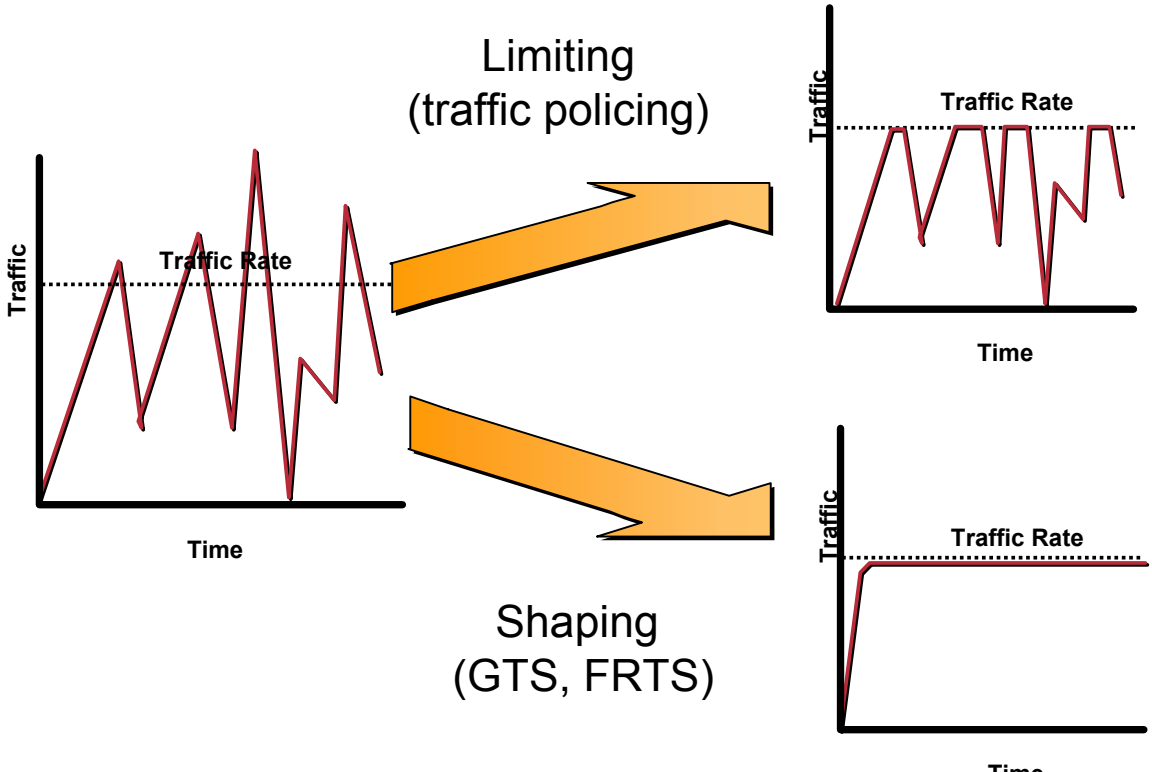
Limiting Techniques - Bandwidth Management

Certain applications or user traffic is more important than others. Not restricting all the different traffic flows can lead to congestion and to the starvation of low bandwidth, high priority traffic in favor of high bandwidth, low priority traffic. To help ensure that priority traffic flows get needed resources, QoS policies that shape or limit traffic can be employed.

Shaping and limiting policies are used to manage how much of an interface's bandwidth is allocated to a specific traffic flow. Because shaping and limiting are performed with policies, as opposed to queues, it is possible to affect flows even in times of little congestion. Shaping differs from limiting in that shaping attempts to throttle the traffic when rate limits are reached. The router is capable of buffering some of the traffic burst. Of course, when the buffers are full, packets are dropped. Limiting on the other hand will not drop any packets until the rate limits are reach, and then all packets are dropped that exceed the limit.

Techniques for shaping traffic are Generic Traffic Shaping (GTS), and Frame Relay Traffic Shaping (FRTS). Committed Access Rate (CAR) techniques are used for limiting traffic.

Controlling Bandwidth Techniques



Policy Actions for Controlling Bandwidth

Cisco uses the following techniques for limiting packet throughput on an interface. The techniques are:

- Generic Traffic Shaping (GTS)
- Frame Relay Traffic Shaping (FRTS)
- Distributed Traffic Shaping (DTS)
- Modular Shaping
- Limiting on routers using Committed Access Rate (CAR)
- Limiting on Catalyst 6000 switches using aggregate and microflow limiting

Traffic shaping smoothes the traffic flow instead of dropping packets through buffering.

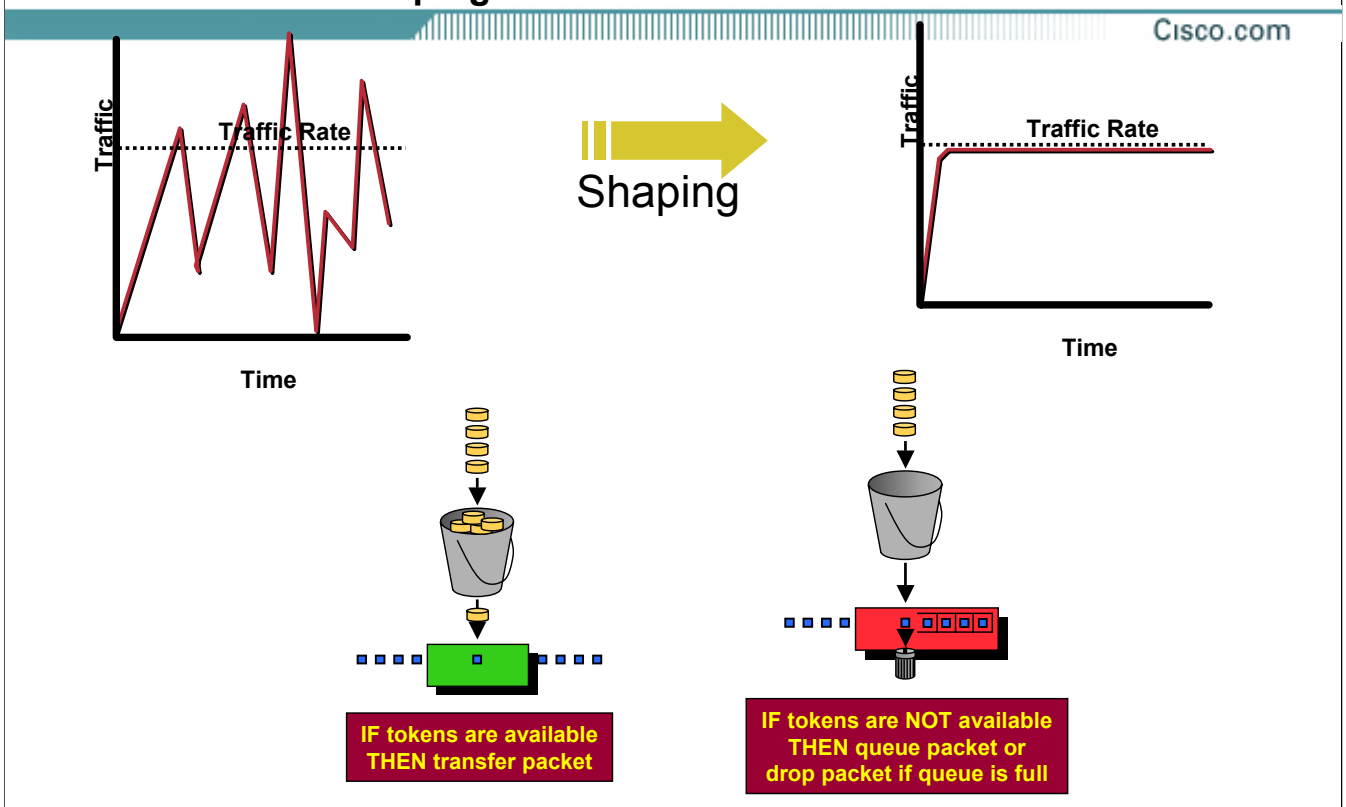
Policing (limiting) traffic sets a hard limit on the traffic rate. There is no buffering of traffic and traffic which exceeds the traffic rate is dropped. Policing is available using Cisco's CAR technique. CAR is implemented in IOS versions 11.1cc and 12.0.

GTS and FRTS are discussed next.

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.

Shaping Traffic
Generic Traffic Shaping



Generic Traffic Shaping (GTS)

Generic Traffic Shaping (GTS) allows for setting a bandwidth limit for specific types of outbound traffic. This puts a cap on the bandwidth available to the specified traffic, ensuring that the remainder of the bandwidth is available to other kinds of traffic. GTS prevents packet loss by buffering packets exceeding the rate limit set in the policy. The effect is the traffic is smoothed out over time. GTS uses a Weighted Fair Queue to delay packets in order to shape the flow.

Though neither GTS nor CAR actually implements a true token bucket or true leaky bucket algorithm, the token bucket approach can be used to explain the shaping behavior. Tokens are put into the bucket at the desired rate. The bucket size can be the rate itself (1 token) or can allow for several tokens equal to the acceptable burst rate. Tokens arriving to a full bucket are discarded. For a packet to be transmitted there must be the appropriate amount of tokens to meet the packet size.

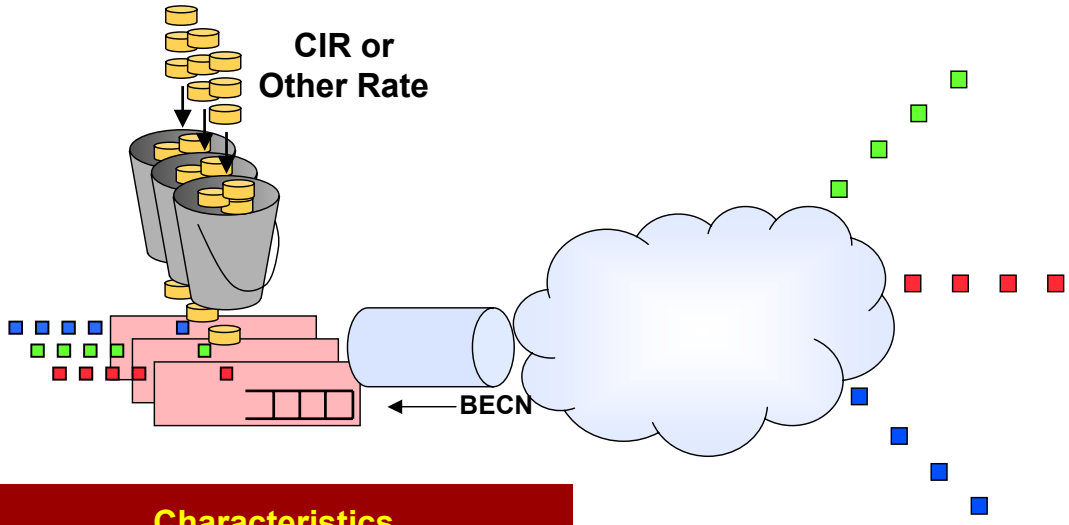
Packets arriving that do not have enough tokens to be transmitted, are delayed in a buffer until enough tokens are present. Once the buffer is full, any additional packets arriving are discarded.

Packets that do not match any of the filters for traffic shaping are passed through to the transmit buffer or are queued if the interface is congested.

GTS guarantees that the burstiness is bounded so that it will never send faster than the token bucket's capacity plus the time interval divided the established rate at which token's are placed into the bucket.

Shaping Traffic
Frame Relay Traffic Shaping

Cisco.com



Characteristics

- **Shape VC traffic to CIR or other rate**
- **Throttle traffic based on congestion indications from the network (BECN)**

Frame Relay Traffic Shaping (FRTS)

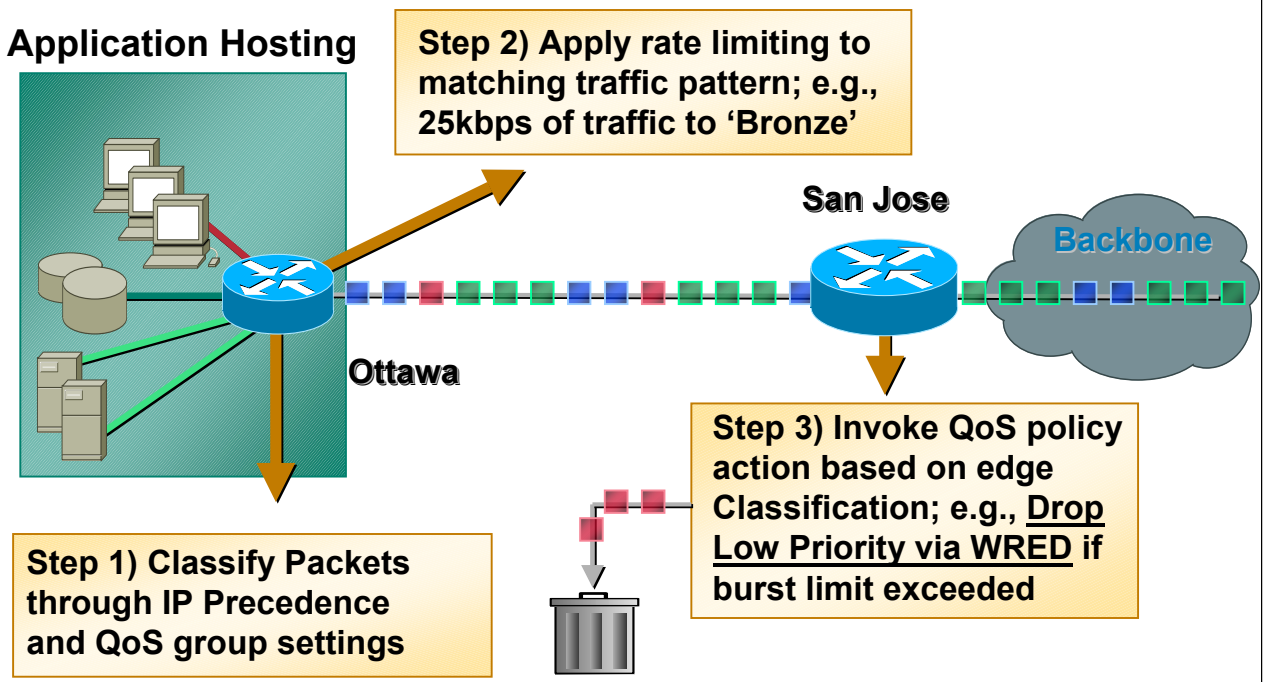
Frame Relay Traffic Shaping (FRTS) uses traditional Frame Relay congestion techniques (CIR, FECN/BECN, and discard eligibility bit), as well as, per VC traffic shaping. Combined, these two techniques allow for finer granularity in the prioritization and queuing of traffic and provide more control over the traffic flow on an individual VC.

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.

Limiting Traffic

On Routers - Committed Access Rate (CAR)

Cisco.com



Policing Traffic or Rate Limiting Actions

Rate Limiting or policing can be applied on the inbound, outbound, or both interfaces. The Limiting action is only available with CAR; therefore, the devices must be running IOS Version 11.1cc or 12.0+.

As an example, traffic can be limited or policed at the input or output interface. First, the packet is classified either through IP precedence, protocol, application port, or IP addresses. Once the traffic is classified, CAR can select limit classified traffic flows to specific levels of bandwidth. If the rate is exceeded, the policy action is triggered and the packets are dropped using WRED.

Limiting on Catalyst 6000 Switches

Traffic limiting lets you set a bandwidth limit for specific types of traffic on Catalyst switch ports or VLANs. You can also define a burst size and an exceed burst size to further model the flow. These values define how much data can be sent from the buffer per time interval. For example, you can create a policy that limits aggregate web traffic on an interface to an average rate of 1024 kilobits/second, with a maximum burst of 2048 kilobits. 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. In this example, if web traffic does not fill 1024 kilobits/second with maximum bursts to 2048 kilobits, other kinds of traffic can use the unused bandwidth. If traffic bursts exceed the limits, packets are dropped or their precedence value is reduced (markdown).

Limiting on Catalyst 6000 Switches

QPM supports limiting on Catalyst 6000 switches running CatOS software, as well as Catalyst 6000 switches with Supervisor IOS software (identified as Cat6000(IOS) in QPM).

On both types of Catalyst 6000 switches, you can set bandwidth limits for the following types of flows:

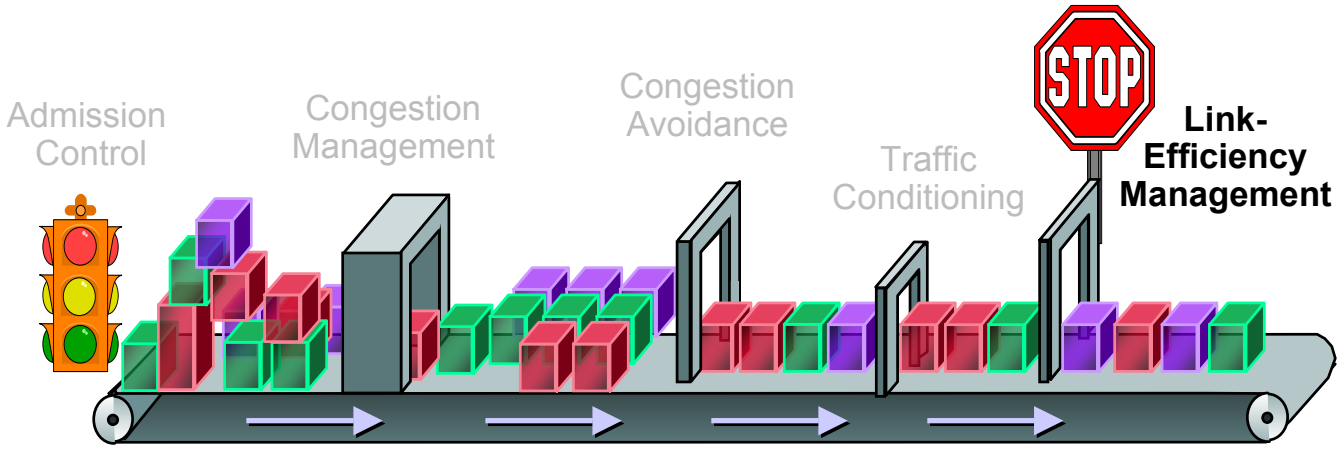
- *Individual flows (microflow limiting)*--QoS applies the specified bandwidth limit separately to each flow in matched traffic.
- *Aggregate flows on the same interface*--QoS applies the specified bandwidth limit to all matched traffic on the interface.
- *Cross-interface aggregate flows (only when defining limiting on a device group)*--QoS applies the specified bandwidth limit to matched traffic from all the interfaces in the device group.

You can select a limiting mechanism for traffic that conforms to the specified rate, either IP Precedence or DSCP.

You have two options for handling traffic that exceeds the specified limits:

- Drop the packets.
- *Markdown*--reduce the packets' IP precedence or DSCP values so that they have less relative priority. QPM does this according to a predefined markdown table, enabling you to apply different markdown values for packets with different IP precedence or DSCP values, rather than applying a fixed markdown value for all traffic that meets the filter conditions. If you have customized the markdown values for the device, these values will be used. Otherwise, the default markdown values will be used (see DSCP Markdown Dialog Box).

This page intentionally left blank.



Terminology Review

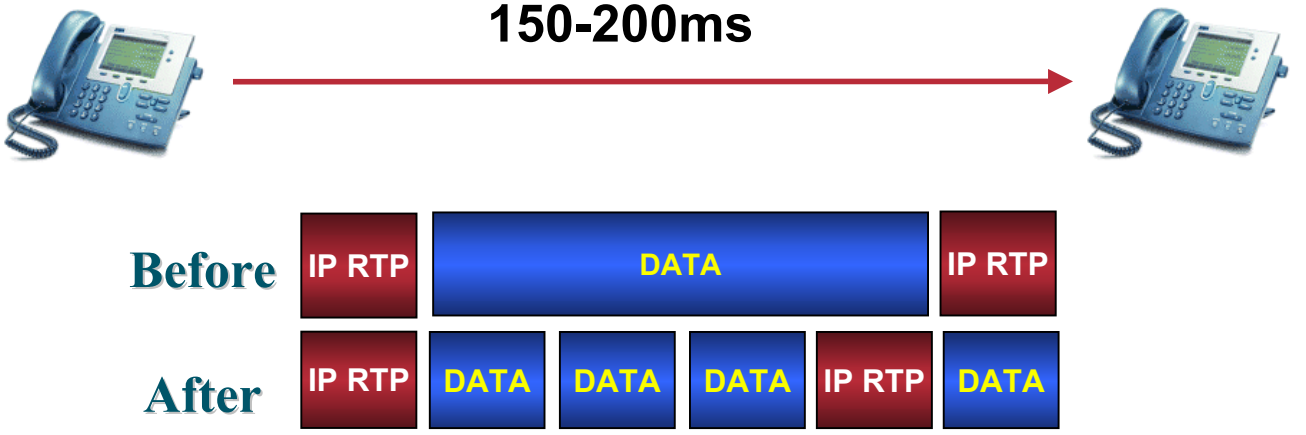
Fragmenting Techniques - Link Efficiency Management

- Link Fragmentation and Interleaving (LFI)
- Frame Relay Fragmentation (FRF.12)
- Compressed RTP (cRTP)

Fragmenting Traffic

Link Fragmentation and Interleaving Frame Relay Fragmentation

Cisco.com



Fragmenting Traffic - LFI - FRF.12

Because voice packets are small in size and the interface also can have large packets going out, the Link Fragmentation and Interleaving (LFI) feature should be configured on lower speed interfaces (as well as IP RTP discussed earlier). When you enable LFI, the large data packets are broken up so that the small voice packets can be interleaved between the data fragments that make up a large data packet. LFI prevents a voice packet from needing to wait until a large packet is sent. Instead, the voice packet can be sent in a shorter amount of time, thus helping to ensure that voice packet jitter, delay, and latency requirements are met.

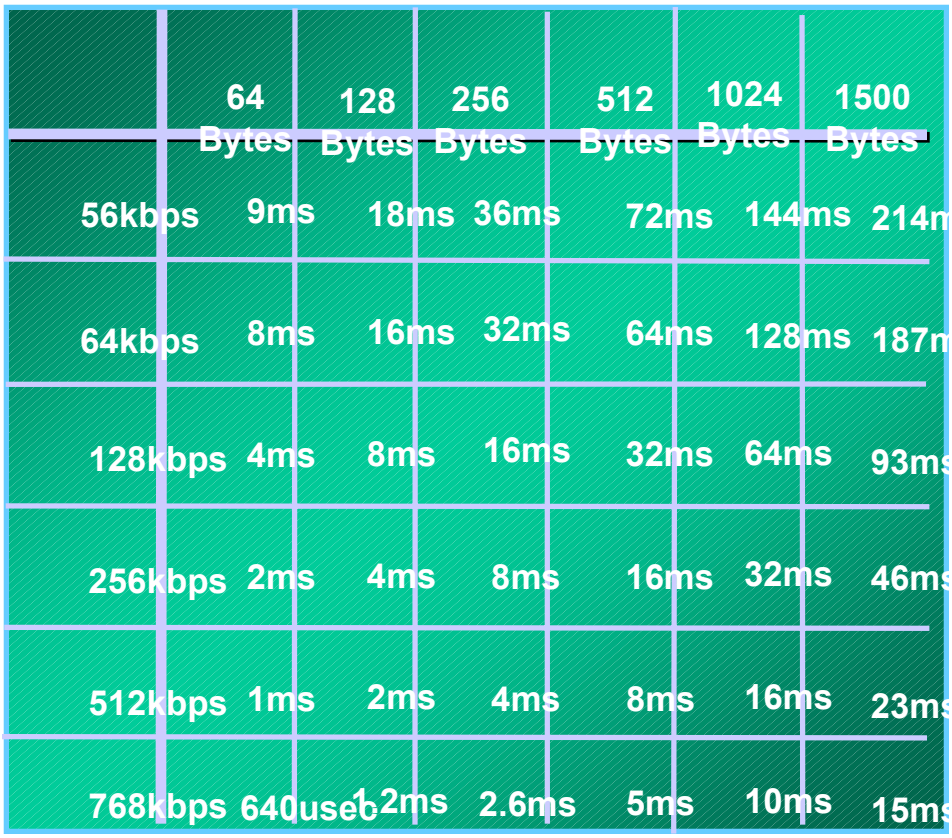
Frame Relay Fragmentation (FRF.12) ensures predictability for voice traffic, aiming to provide better throughput on low-speed Frame Relay links by interleaving delay-sensitive voice traffic on one virtual circuit (VC) with fragments of a long frame on another VC utilizing the same interface.

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 included only for frames that are greater than the fragment size configured.

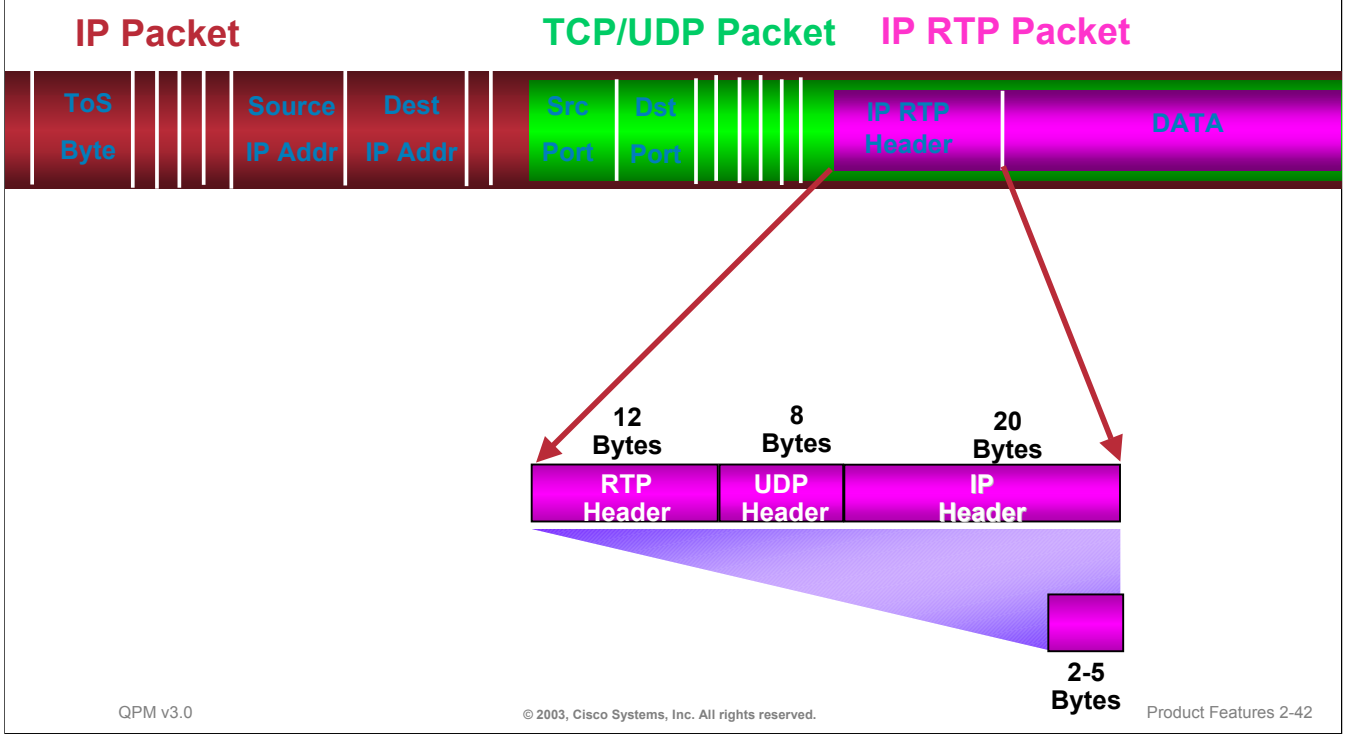
Fragmenting Techniques

The table below illustrates that large data packets can cause long delays on slow links and possible cause the voice packet to be delayed longer than the desired 150-200 milliseconds.



Fragmenting Traffic
Compressed RTP Packet Header

Cisco.com



Fragmenting Traffic - cRTP

The compressed Real-Time Protocol (cRTP) can compress the RTP Header to reduce delay.

Remember that 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, the RTP header compression feature, referred to as cRTP, is used on a link-by-link basis. RTP header compression results in decreased consumption of available bandwidth for voice traffic. A corresponding reduction in delay is realized.

RTP header compression is supported on serial lines using Frame Relay, High-Level Data Link Control (HDLC), or PPP encapsulation. cRTP compresses the IP/UDP/RTP header in an RTP data packet from 40 bytes to approximately 2 to 5 bytes.

cRTP can be defined on WFQ and CBWFQ interfaces with later IOS versions.

Part 2

QPM Features Overview

We have just reviewed the terminology that composes the basis of QoS. Next, we will touch upon some of the features of the QPM architecture that allows QPM to implement these QoS mechanisms.

QoS Policy Manager (QPM) v3.0
Overview

Cisco.com

- **A centralized management tool to configure, deploy, and analyze QoS policies for data and VoIP networks using CiscoWorks web-based user interface**
- **Traffic monitoring for setting and validating QoS**
- **IP Telephony QoS configuration using setup wizard**
- **Knowledge base of QoS mechanisms supported on different device types and OS versions**
- **Scaleable to large networks**

QoS Policy Manager v3.0 Overview

CiscoWorks QoS Policy Manager (QPM) v.3.0 ensures end-to-end quality of service (QoS) by combining traffic monitoring and configuration of Differentiated Services (Diff-Serv) for voice, video, and data applications by taking advantage of the QoS mechanisms built into Cisco routers and switches.

The following features in CiscoWorks QPM v3.0 provide network administrators with the capability to easily deploy QoS mechanisms in the LAN or WAN for data and IP telephony networks.

- *Traffic monitoring for setting and validating QoS* — Measures traffic throughput for top applications (e.g. SAP, Oracle, PeopleSoft) and service classes (e.g. business critical) plus troubleshoot problems with real-time and historical QoS feedback.
- *Web-based centralized traffic management*--Secure Web-based interface allows accurate end-to-end QoS configuration and automated, reliable policy deployment, as well as monitoring at different points in the network.
- *IP telephony QoS set-up wizard* — Intelligently determines QoS policies and properties at each network point that requires IP telephony QoS configuration. Policies are based on Cisco AVVID design recommendations.
- *Advanced user administration and security* — Centrally define user roles and permissions with linkage to Cisco Secure Access Control Server (ACS) for view, edit, and deployment privileges per device group.
- *Scalable to large networks* - through the use of a relational database (part of Common Services) for storage of policies and QoS statistics, structured management that includes deployment groups with integrated policy groups and device groups, deployment control, allowing guidelines to dictate number of devices in a concurrent deployment and schedule, support for SSL policy distribution to devices, and policy libraries that include Cisco or user-defined templates that can be copied/modified or attached to multiple policy groups for "one-to-many" configuration.

QoS Policy Manager (QPM) v3.0
Overview (continued)

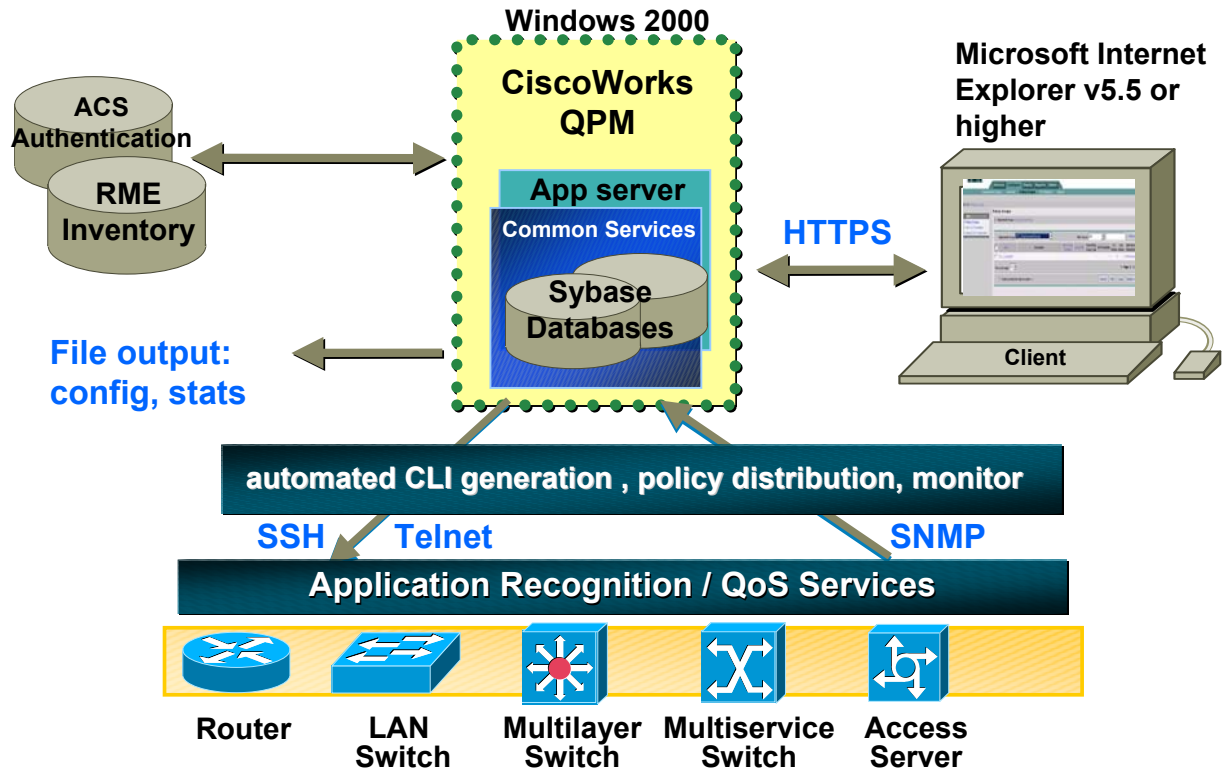
- **Differentiated services for various types of traffic**
- **Extensive application-level classification**
- **Structured traffic management**
- **Access control policies to permit or deny traffic**
- **Advanced QoS policy administration (uploads, previewing CLI syntax, rollback, etc.)**

QoS Policy Manager v3.0 Overview (continued)

- *Differentiated services for various types of traffic* — Achieve business-driven service levels across the enterprise network by configuring traffic classification and allowing QoS policy enforcement through Cisco devices.
- *Extensive application-level classification* — An integral part of Cisco content networking, QPM 3.0 delivers the appropriate service levels to business-critical applications by supporting the extension of IP packet classification to include application signature, Web URLs, and negotiated ports.
- *Structured traffic management* — Enables congestion management, congestion avoidance, and bandwidth control by selectively activating QoS mechanisms on intelligently grouped LAN and WAN interfaces and providing support for external application programming interfaces (APIs) to trigger event-based policy distribution.
- *Access control* — Extend security by defining access control policies to permit or deny transport of packets into or out of device interfaces.
- *Advanced QoS policy administration* — Exposes QoS policy conflicts, uploads existing device configurations, presents command-line interface (CLI) syntax that corresponds to policies, allows previewing configuration changes before deployment, supports incremental access control list (ACL) updates, defines ACL ranges, and restores or applies a previous version of a policy database and backup to a remote server.

QPM has two purchasing options. QPM with a 20 device restriction offers a more cost-effective solution for smaller networks such as IP telephony pilots. CiscoWorks QPM unrestricted is designed for enterprise production network deployments.

QoS Policy Manager (QPM) v3.0
Architecture



CiscoWorks QPM v3.0 Architecture

QPM consists of a client/server architecture. The application server can reside on a Windows 2000 platform that may or may not have other CiscoWorks applications such as Resource Manager Essentials (RME) already installed. The QPM application server is accessed using the Microsoft Internet Explorer web browser over a secure connection (HTTPS).

The network administrator populates the QPM inventory (either manually or from the CiscoWorks RME device inventory) with the devices to be configured with QoS mechanisms. QoS policies can then be created in an abstract manner and assigned to various device interfaces. QPM contains the knowledge-base on valid device commands removing this complexity from the user.

Policies are deployed to the various devices using telnet or Secured Shell (SSH). If QPM is configured to work with Cisco Secure Access Control Server (ACS), access and configuration changes to devices by an administrator using QPM is controlled by the user and device group permissions defined in ACS. Otherwise, QPM utilizes the use access and authorization features available with the CiscoWorks user roles.

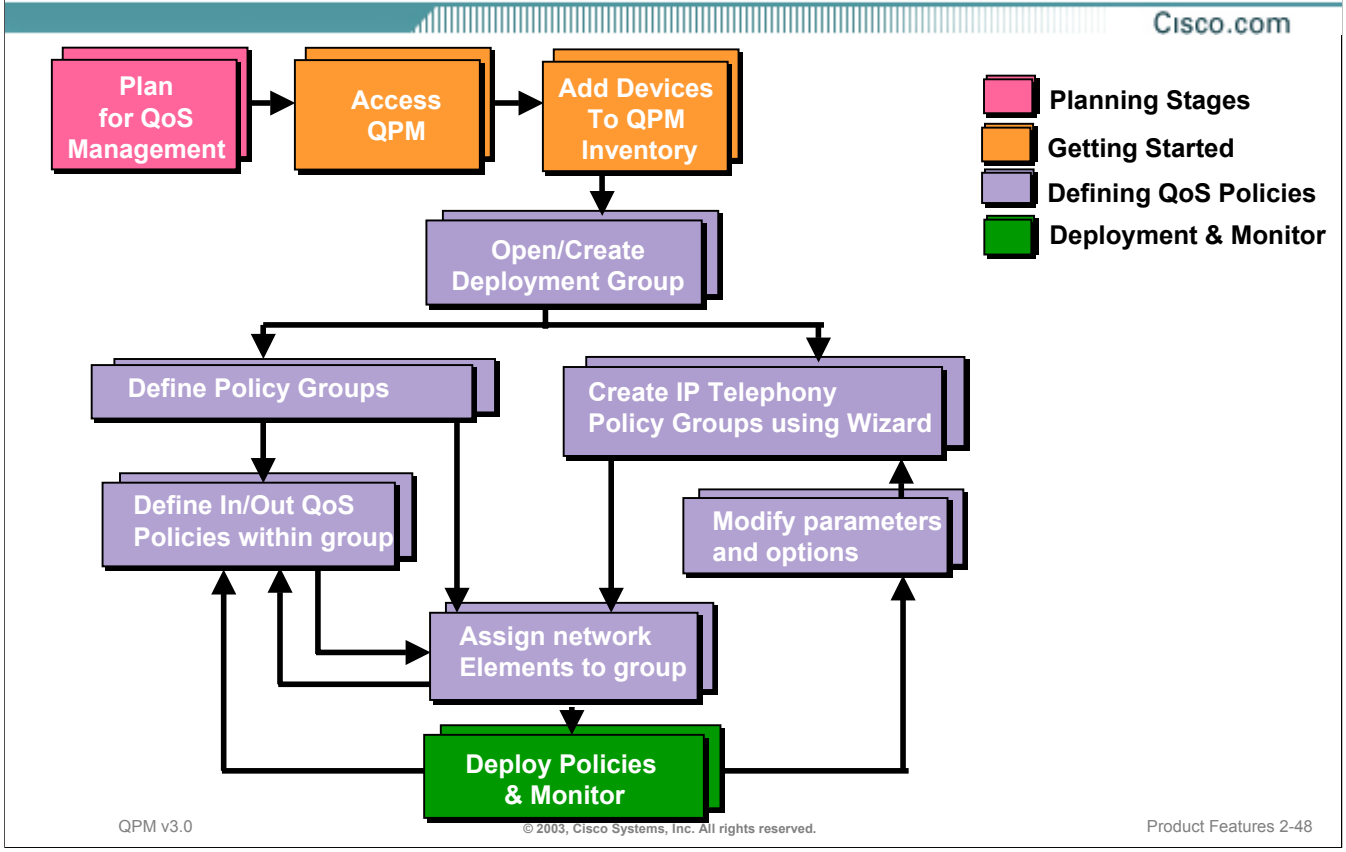
QPM can also analyze the effectiveness of QoS policies by monitoring the devices using SNMP (Simple Network Management Protocol) for reading the device MIBs (Management Information Base).

Details about these various QPM tasks are discussed throughout the remainder of this chapter.

Part 3

Using QPM

This section provides a roadmap to using QPM.



Typical QoS Management Workflow

Now let's get ready to use QPM to assist the network manager in defining and distributing QoS policies. The above workflow attempts to ease the process.

The main workflow tasks are planning, getting QPM ready for use, using QPM to create QoS policies, and finally deploying and monitoring the policies in the network.

As with any project, if planning is done correctly, the rest will come easier. QPM can help ease the syntax and will provide guidance on the QoS mechanisms supported by device type and OS version. However, it will be up to the network administrator to know the QoS mechanisms and how they should be used.

After the *planning stage*, *add or import the devices into the QPM inventory*. The devices can be added manually, from a CSV file, or imported directly from Essentials. Added devices are placed in a single default device group if using CiscoWorks user roles for QPM permissions. If ACS is used for PM permissions, the ACS device groups are imported and determine user access and command authorization on a group of devices.

Next, *open or create a deployment group*—QPM QoS policies are defined within the framework of deployment groups. When beginning to work with QPM, a default deployment group is automatically opened. Users can create and manage multiple deployment groups for phased deployment, or for testing what-if scenarios.

Now the user is ready to *create policy groups*—Policy groups are constrained sets of QoS policies. The user must define the device constraints and QoS properties for their policy groups before they can begin to define policies. The user can upload the existing QoS configuration on their devices into policy groups.

Once policy groups have been defined, the *individual QoS policies within the group can be defined*—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).

Typical QoS Management Workflow (Continued)

Next the *network elements will be assigned to the policy group*—The user 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. The user can assign network elements to policy groups before or after defining policies.

Though the concept is similar, the *creation of IP telephony policy groups and policies* is achieved using an IP telephony wizard, which automatically creates the QoS policies required at each network point in the IP telephony network, according to the IP telephony network topology defined by the network administrator. The QoS policies are defined using voice policy group templates that follow the Cisco IP Telephony QoS Design Guide recommendations.

Once the policies have been defined an assigned to network elements, they can be *deployed to the network.*

After deploying the QoS configuration to the network, validate their effectiveness by *monitoring* various MIB variables on a device related to QoS. Based on the monitoring results, the QoS policies can be refined to achieve optimum performance.

The upcoming sections will look at each of the workflow steps in more detail. So let’s get started!

Planning for QoS Management

Cisco.com

Identify Application Traffic:

- Determine traffic distribution of the applications
- Classify applications
- Evaluate the resources requirements for each application (bandwidth, latency, real-time, burst, etc)
- Based on these calculations, decide what level of service each application requires

Analyze Network for QoS Implementation:

- Capacity (link speeds, overhead, CPU)
- Decide whether domain boundaries are trusted or un-trusted
- Analyze the network topology and traffic flow
- Analyze the network links in each layer of the network, and the possible QoS mechanisms that can be implemented on those links

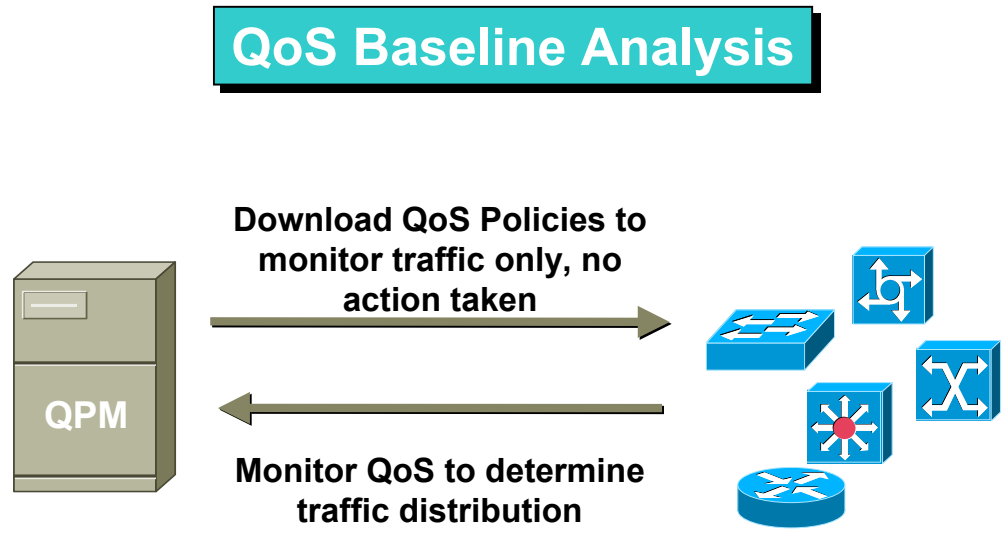
Planning for QoS Management

Like any configuration task, effective use of Quality of Service (QoS) capabilities requires careful planning. Before deploying QoS to the network, carefully consider the types of applications used in the network and their requirements for proper operation. Once this is determined, choose which QoS techniques might improve the performance of those applications, and where to place the QoS mechanisms based on the network topology. Once the planning is completed, use QPM to create and deploy the QoS policies to the network, and analyze QoS performance.

Let's look first at how to identify the network application traffic and then classify the traffic into classes of services. Later in this chapter we will discuss how to analyze the network following the implementation of QoS mechanisms.

Planning for QoS Management
Identify Application Traffic

Cisco.com



Planning QoS Management – Identifying Application Traffic

The QPM QoS analysis function can be used to perform a baseline QoS analysis by simply deploying QoS policies that identify the important traffic classes on the network, but do 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 without QoS implementation.

Tip: Use an RMON device (Cisco Network Analysis Module (NAM)) or Sniffer-like device to assist in determining the traffic already on the network.

Baseline QoS analysis works best when ten or fewer traffic classes are identified to monitor. Each traffic class can contain one or more traffic types. For example:

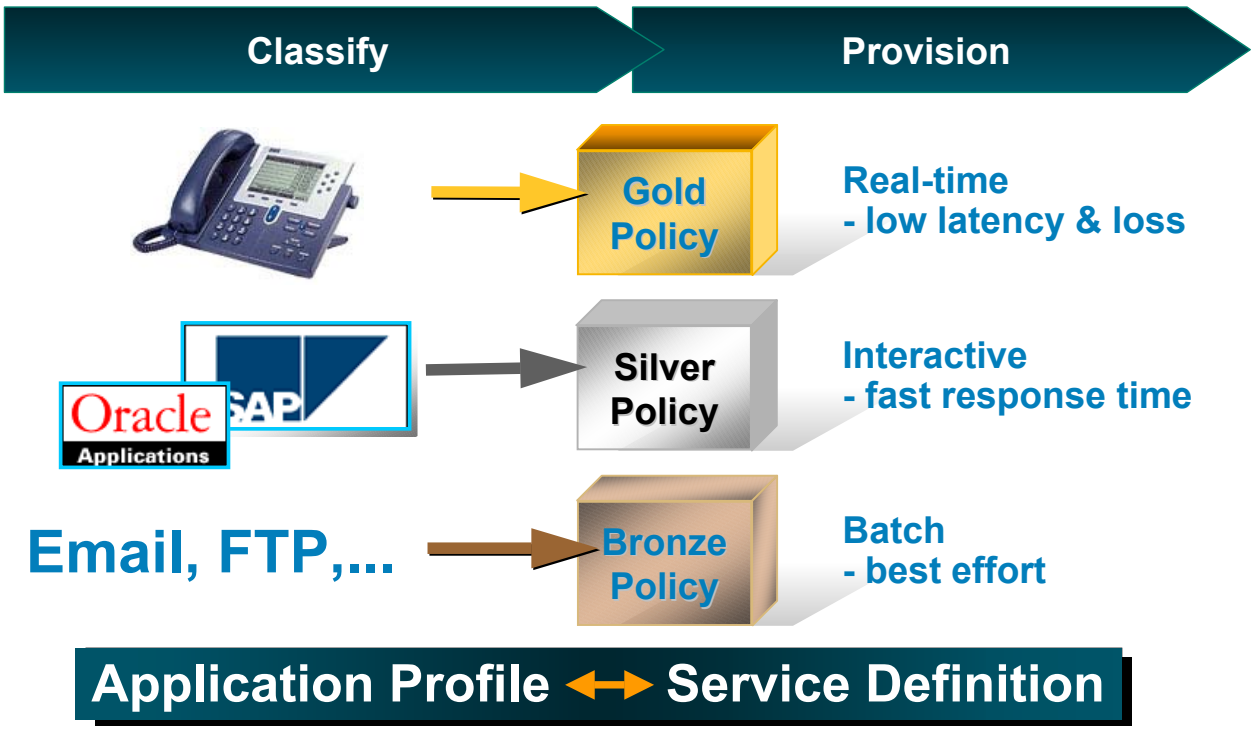
- Gold class for voice and vide,
- Silver class for SAP, Oracle
- Best Effort class for web traffic

These traffic classes can then be defined within QPM as policies that filter for each of the applications and the policy actions will be defined accordingly. Keep in mind that the QPM reports show network activity at the policy (class) level, so a breakdown of the applications within a class is not viewable.

View the QoS analysis reports in QPM to show the results of the traffic classification. Of course, this activity requires the user to first understand the QPM product prior to creating and deploying these baseline QoS policies to the network. Thus, we will assume for this tutorial, that the user already understands the applications and traffic flows on the network and is ready to begin using QPM to help configure, deploy, and monitor QoS mechanisms.

Planning for QoS Management
Classifying Application Traffic

Cisco.com



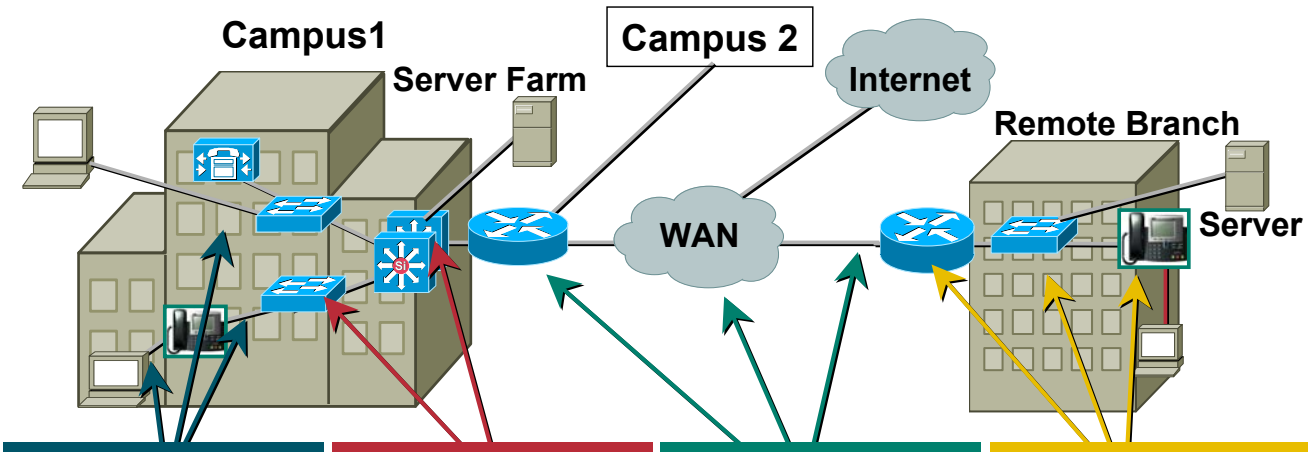
Planning QoS Management – Classifying Application Traffic

Here is an example of how one service provider classifies and provisions their application traffic. Keep in mind that it would be difficult to differentiate many different service classes and even more difficult to tariff and bill.

- A Gold service would guarantee latency and delivery for the transport of mission critical business applications like voice, video, or SNA.
- The Silver class would guarantee delivery and be used for more general applications that are not as sensitive to delay like e-commerce.
- The Bronze class could be used to support small business and e-mail and other Best Effort applications.

Planning for QoS Management
Analyze Network for QoS Implementation

Cisco.com



QoS—Campus Access	QoS—Campus Distribution	QoS—WAN	QoS—Branch
Speed and Duplex Settings Classification/trust on IP Phone and Access Switch Multiple Queues on IP Phone and Access Ports	Layer 3 Policing Multiple Queues on All Ports; Priority Queuing for VoIP WRED Within Data Queue for Congestion Management	Low-latency Queuing (LLQ) Link Fragmentation and Interleave (LFI) Bandwidth Provisioning Admission Control	Classification and Trust Boundaries on IP Phone , Access Layer Switch and Router Multiple Queues on IP Phone and All Access Ports

Planning for QoS Management – Analyze Network for QoS Implementation

After identifying the traffic classes to monitor, you will see later in this chapter on how to use QPM to create policies that mark the packets without taking any QoS actions that affect traffic flow for baselining and QoS policies that limit, shape, or queue traffic.

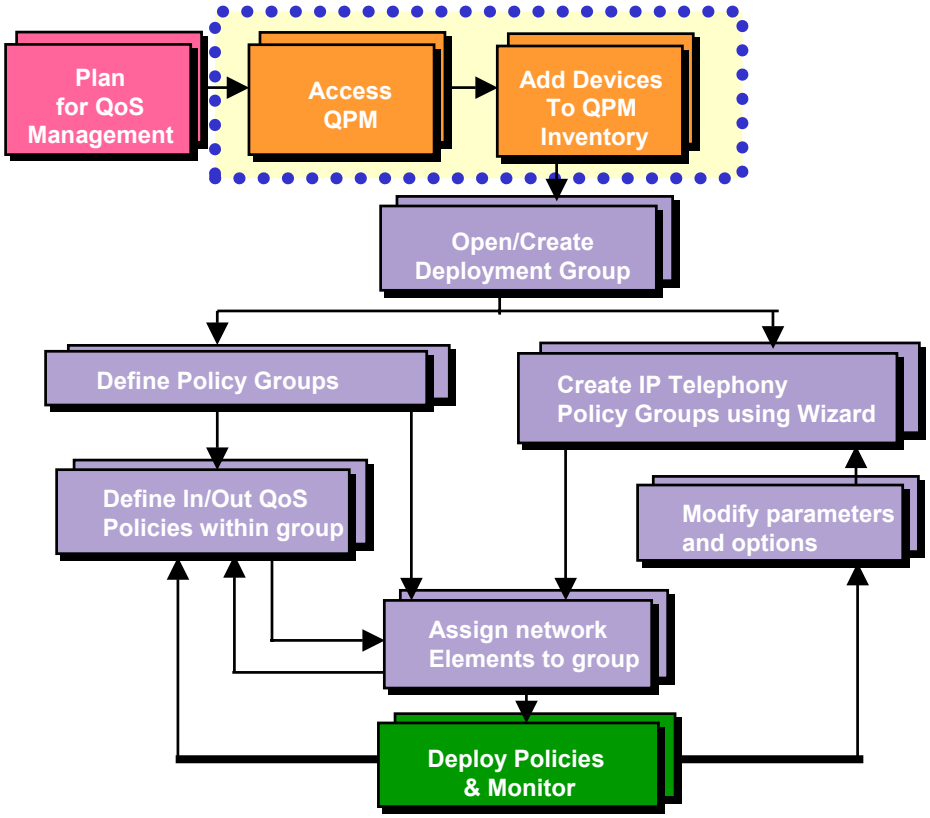
When ready to implement QoS policies across the network, use the illustration above and the Cisco Design Guides to help identify the type of QoS mechanisms at the various network points. Then use QPM to configure and deploy the policies.

The last part of the workflow will be to create a QPM report to view the percentage of each defined traffic class at the interfaces where the baseline QoS policies were placed.

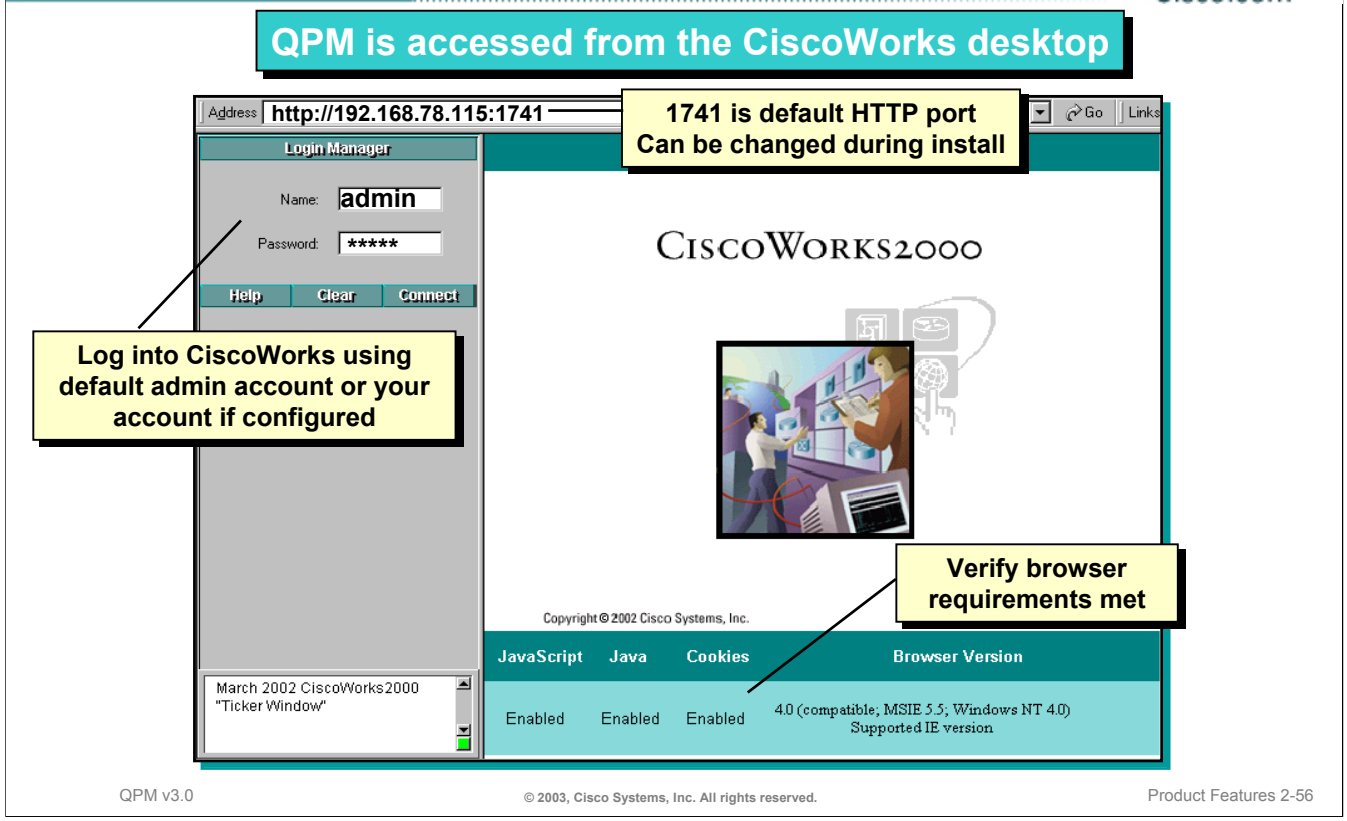
This page intentionally left blank.

Roadmap

Getting Started



Getting Started
Accessing CiscoWorks



Getting Started – Accessing CiscoWorks

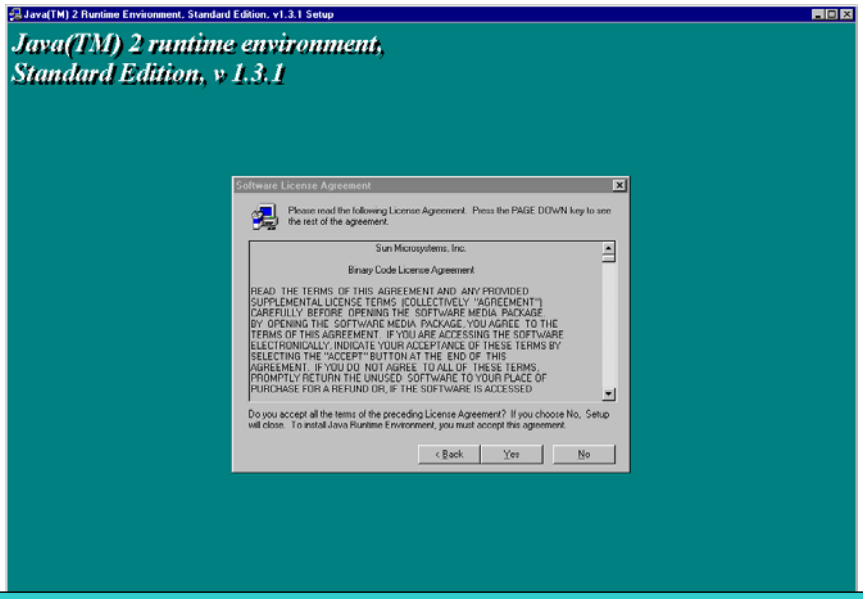
QPM is accessed from the CiscoWorks desktop, therefore the first order of business is to access the CiscoWorks desktop. Access to the CiscoWorks desktop can be achieved from anywhere on the network as long as the client is capable of reaching the CiscoWorks server via HTTP (Hypertext Transfer Protocol). The client accesses the CiscoWorks desktop using the web-browser supported by CiscoWorks QPM, Microsoft Internet Explorer. For the desktop to properly display, the user must ensure that the browser has been properly configured. For example, Java and JavaScript must be enabled, the browser must accept all cookies, and the browser should compare documents in cache to documents on the network every time to ensure that the most up-to-date information is displayed in reports and dialog boxes. For more information regarding client configuration see chapter 4.

During installation, the administrator can choose to set the HTTP port to be used for CiscoWorks access or can accept the default port – TCP 1741. The user would then simply enter the following URL to access the CiscoWorks desktop

http*://<server IP address or hostname>*:1741

The CiscoWorks login window is displayed. The login window will display the browser's conformance to the required browser configuration. During installation a default administrator account was created, use this account to log into CiscoWorks for the first time. The default administrator account can be used to define additional CiscoWorks users or to associate user authentication for CiscoWorks login and QPM user permissions with Cisco Secure Access Control Server (ACS).

Getting Started
Accessing CiscoWorks – The Java Plug-In



CiscoWorks clients requires version 1.3.1 of the Java Plug-In

Automatically downloaded to client, if not already installed, when first accessing the CiscoWorks Desktop

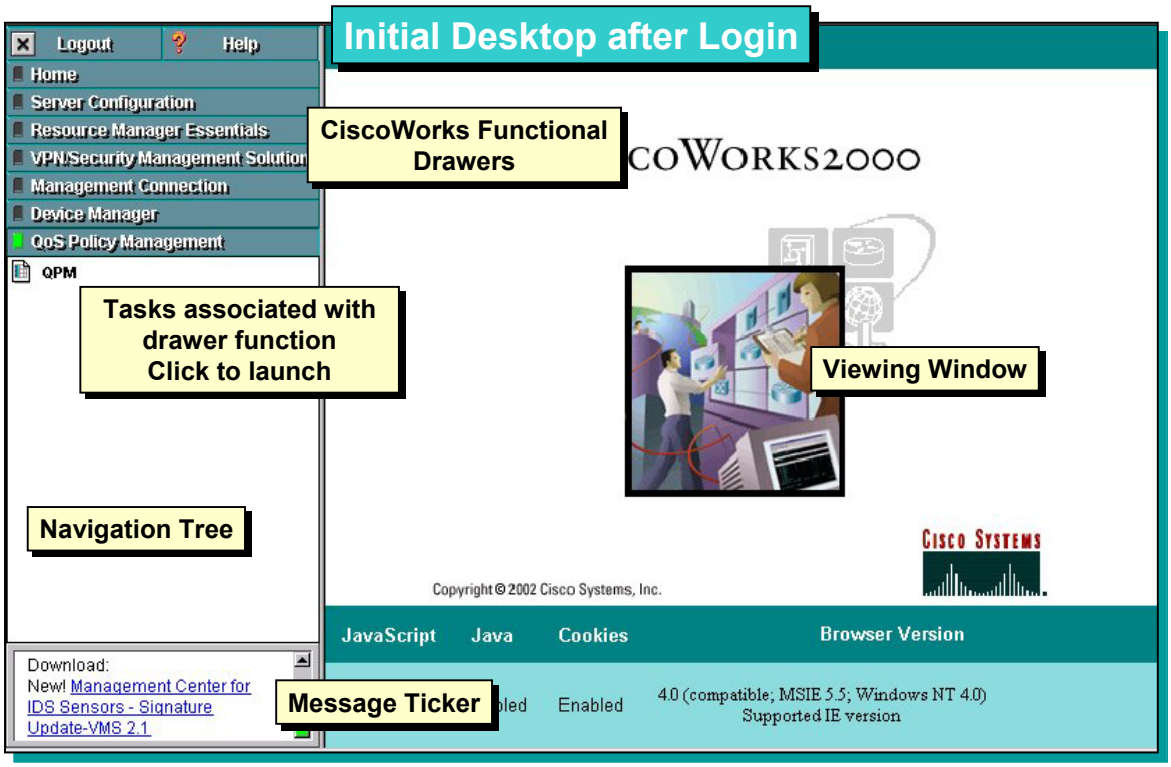
Accessing CiscoWorks - The Java Plug-In

Many CiscoWorks applications require the client browser to use the Java plug-in v1.3.1 to properly execute. One of the main reasons for using the Java plug-in is to increase performance. Installation of the plug-in is mostly automatic. When accessing the CiscoWorks desktop, CiscoWorks will determine if the client machine has the proper plug-in loaded. If not, it will warn the user, and provide a dialog box to download the plug-in from the server. The above screen will be displayed and the user is required to simply click *Yes* to accept the license agreement and then select the directory for the plug-in to reside. Once the Java plug-in is installed on a client machine, the use of the plug-in becomes transparent to the user.

The CiscoWorks desktop will be displayed after the plug-in is downloaded and installed, or if the plug-in was already installed.

Note: Java Plug-In versions are not backward compatible. Make sure you are using the plug-in version specified for the release of CiscoWorks loaded.

Getting Started
Accessing CiscoWorks - The CiscoWorks Desktop



Accessing CiscoWorks - The CiscoWorks Desktop

Often times the most difficult part of using CiscoWorks is finding the task you wish to run. This topic provides a quick primer for navigating within CiscoWorks.

The CiscoWorks desktop is divided into three separate areas. The upper left-hand portion of the window is the navigation tree. Located in the lower left-hand portion of the window is the message ticker. Finally the right-hand portion of the window is used to view the configuration and results of executed CiscoWorks tasks.

Note: Some CiscoWorks tasks and reports will open a new browser window.

The navigation tree displays the major CiscoWorks applications or functions installed. These applications or functions are organized in "*drawers.*" You can open a drawer to view the tasks related to the CiscoWorks application or function by clicking on the drawer. The insides of the drawer may be further organized by the use of folders to group related tasks. Again, click on the folder to see the tasks it contains. To execute a task, simply locate it and then click on it. The navigation tree also contains buttons to logout of the CiscoWorks desktop and a button for content-sensitive help.

Note: Remember to select the *Logout* button after finishing use of CiscoWorks. This closes the CiscoWorks session and returns the browser to the Login Manager. Even though the CiscoWorks session times out, leaving the session open with system administrator privileges is asking for trouble.

Getting Started
QPM User Permissions

Cisco.com

Two Ways:

- **Local CiscoWorks (default method)**
  - **QPM permission mapped to CiscoWorks user role**

CiscoWorks Role	QPM Permissions		
	View	Modify	Deploy
Help Desk	Yes	No	No
System Administrator	Yes	Yes	No
Network Administrator	Yes	Yes	Yes
Network Operator	Yes	No	No
Approver	Yes	No	No

- **Cisco Secure Access Control Server (ACS v3.1)**
  - **Three new ACS permission roles are created when QPM associated with ACS v3.1**
  - **QPM permission mapped to ACS permission role**
  - **Privileges further defined by ACS user and group permissions (command, device, etc.)**

ACS Role	QPM Permissions		
	View	Modify	Deploy
Help Desk	Yes	No	No
System Administrator	Yes	Yes	No
Network Administrator	Yes	Yes	Yes

Getting Started - QPM User Permissions

Before accessing QPM, it is important to understand the security of the application. Access to the various QPM functions is handled by associating user roles with the QPM user. QPM user permissions can be handled locally by CiscoWorks (default) or in conjunction with ACS for more control of access by users to various devices.

If QPM permissions are being handled by CiscoWorks, CiscoWorks users are assigned one or more user roles. For QPM functions, all user roles have permission to view any QPM functions, but only users with either the System Administrator or Network Administrator user role can modify QPM. Finally, only users with the Network Administrator user role can deploy QoS to the network.

Note: The default administrator account created during installation is assigned all user roles.

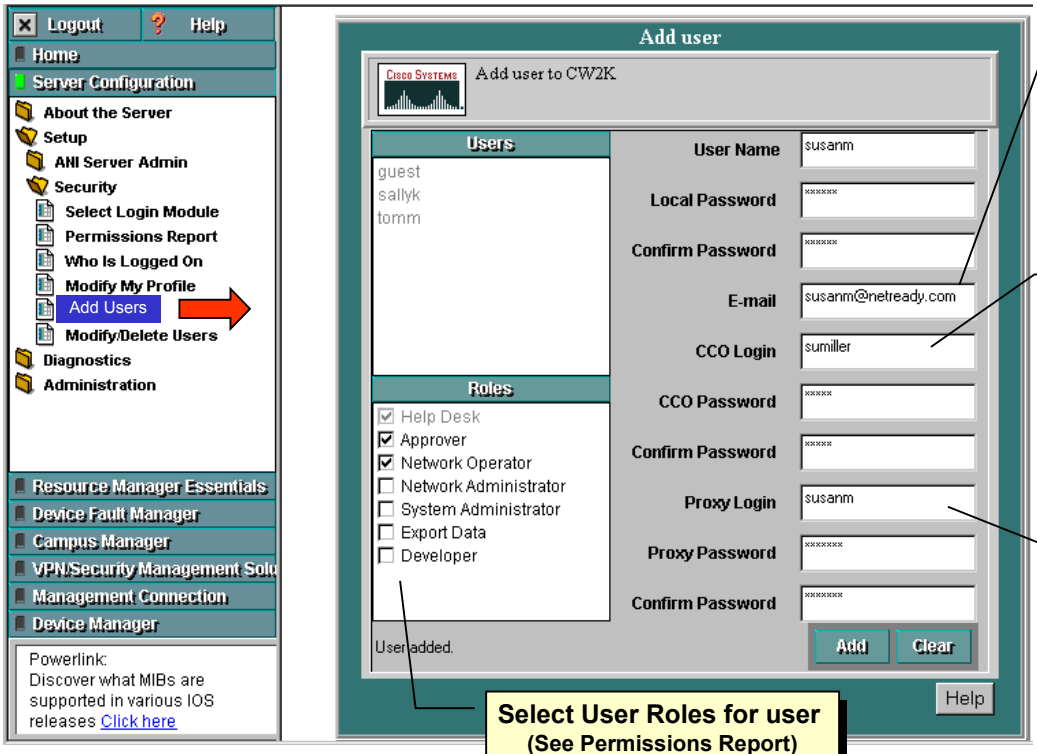
If QPM permissions are being handled by ACS, ACS creates three new user permission roles that can be assigned to individual users. All user roles will be able to view, the System Administrator and Network Administrator user roles allow the user to modify QPM, and only users with the Network Administrator user role can deploy QoS to the network. These user roles are assigned to users in ACS and not CiscoWorks. Further, ACS users are further constrained by user and group permissions on device groups. See ACS documentation for more information on ACS users and user groups.

Note: To use ACS authentication and authorization, ACS 3.1 must be installed on the network.

If a user does not have certain permissions within QPM (based on either CiscoWorks or ACS user roles) then those items will not be displayed in the QPM menus and navigation bars.

The next two pages describe how to configure user roles for the different authentication mechanisms.

Getting Started
QPM User Permissions – Using CiscoWorks



QPM User Permissions – Using CiscoWorks

If using CiscoWorks for authentication and authorization (default method), new users can be added by any current user with the System Administrator user role.

To add a new CiscoWorks user, first execute the *Add User* task by selecting *Setup* > *Security* > *Add Users* from the *Server Configuration* drawer. Choose a user log in name, initial password, e-mail (some functions e-mail users when complete), the users CCO login information if applicable (user can add later), any proxy information if necessary, and of course the user roles to be assigned to this user. A user can have multiple roles, consult the QPM permissions on the previous page to determine the QPM capabilities for each user role.

When navigating to the Security folder, a non-System Admin user will only be able to modify his account (excepts user roles) and view the permissions report (displays permissions for CiscoWorks tasks).

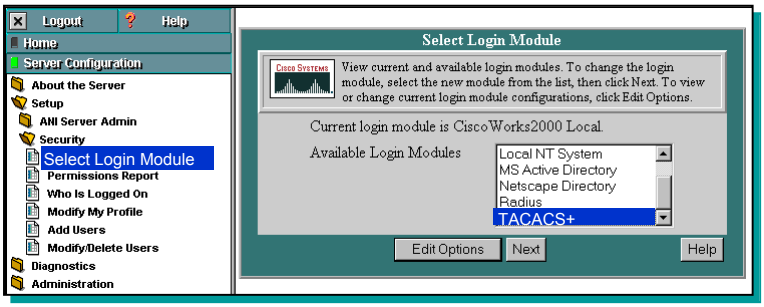
The predefined users, admin and guest, have predefined user roles. The admin user has all user roles and the guest user has only the Help Desk role.

Getting Started
QPM User Permissions – Using ACS v3.1

Cisco.com

1. **Define QPM Server in ACS**

2. **Define Login Module in CiscoWorks as TACASC+**



3. **Synchronize CiscoWorks Common Services with the ACS server configuration**

4. **Define users, user groups, and device groups in ACS**

QPM User Permissions – Using ACS v3.1

The following steps are required to configure both CiscoWorks in general and QPM specifically to work in conjunction with ACS.

Define the QPM server in ACS

1. In ACS, select *Network Configuration.*
2. Add the QPM server to a device group, or add it as an individual device, depending on the ACS setup.
3. Enter the ACS shared key in the Key field.

Define the Login Module in CiscoWorks as TACACS+

1. From the CiscoWorks desktop, select *Server Configuration* > *Setup* > *Security* > *Select Login Module*.
2. Select TACACS+, if it is not already selected. Click *Next.*
3. Enter the ACS server name. Change the default port, if required. You do not need to enter a key.
4. Click *Finish.*

Synchronize CiscoWorks Common Services with the ACS server configuration

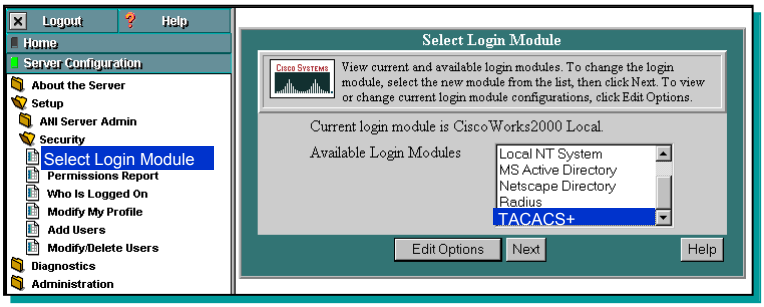
1. From the CiscoWorks desktop, select *VPN/Security Management Solution* > *Administration* > *Configuration* > *AAA Server.*
2. In the AAA Server Information dialog box, click *Synchronize.*
3. Add Login details. Enter the ACS shared key that you defined for QPM server in ACS.
4. Click *Register*.
5. Select *QPM*, and click the *Add* button, to add the QPM permission roles in ACS. Click *OK*.
6. Click *Finish*.

Getting Started
QPM User Permissions – Using ACS v3.1 (Continued)

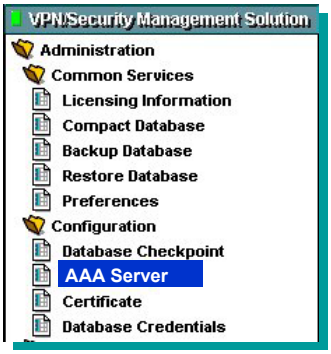
Cisco.com

1. **Define QPM Server in ACS**

2. **Define Login Module in CiscoWorks as TACASC+**



3. **Synchronize CiscoWorks Common Services with the ACS server configuration**



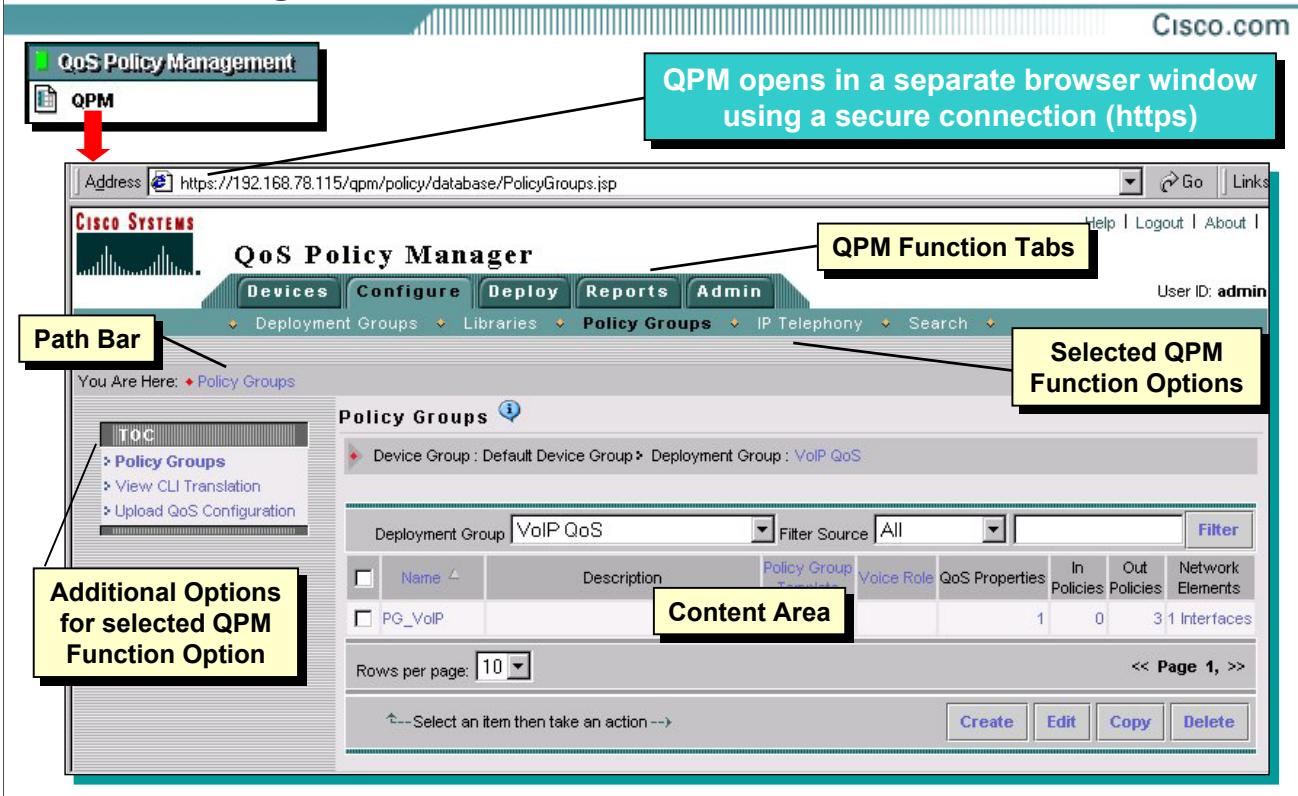
4. **Define users, user groups, and device groups in ACS**

QPM User Permissions – Using ACS v3.1 (Continued)

Define usernames, device groups and user groups in ACS

1. In ACS, select ***User Setup*** to define usernames. Define the same username and password as you define for CiscoWorks authentication (other CiscoWorks tasks require authentication using the local CiscoWorks user permissions).
2. Select *Group Setup* to define permissions for device groups.

Getting Started
Accessing QPM



Accessing QPM

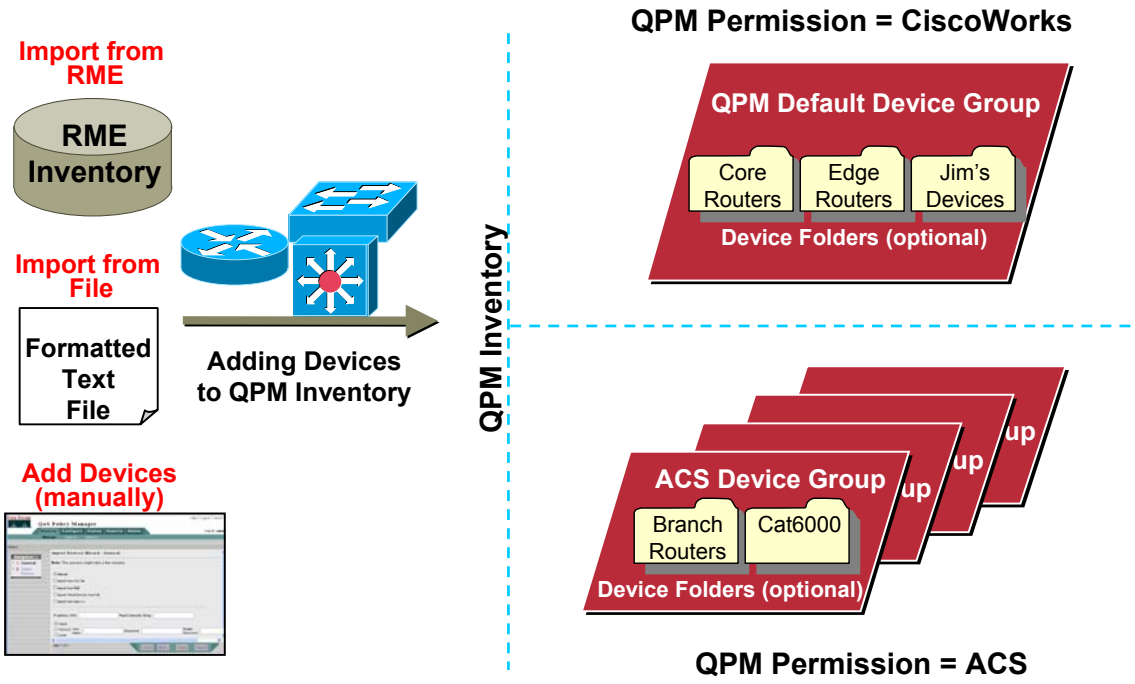
To access QPM, select the *QPM* task found in the *QoS Policy Management* drawer on the CiscoWorks desktop. A security alert is displayed informing the user is about to open a secure connection. QPM opens in a separate browser window and uses https as the connection protocol.

All the displays in QPM have a consistent look, feel, and navigation. Major QPM functions are accessed by selecting one of the tabs found towards the top of the window. The selected tab will be a teal color with black lettering. Sub-functions related to the selected QPM function are found on the bar beneath the tabs. The currently selected sub-function will display black lettering. Simply click on any of the sub-functions to access them. Additional tasks to the sub-functions can be found on the left hand portion of the window in the TOC menu. Select one of these tasks to access it. To quickly view the current QPM location, refer to the path bar found under the sub-function menu. The selected QPM task results or dialog will be displayed in the right-hand portion of the window. Operations for the selected task (buttons) are available in the content area.

Now that navigating through QPM shouldn't be a problem, the first order of business is to add devices to the QPM inventory.

Getting Started
Adding Devices to the QPM Inventory

Cisco.com



Adding Devices to the QPM Inventory

Before creating any policies, QPM must first be populated with the devices to be managed for QoS by QPM. 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, sub-interfaces, and VLANs.

Devices can be added to QPM in 3 ways:

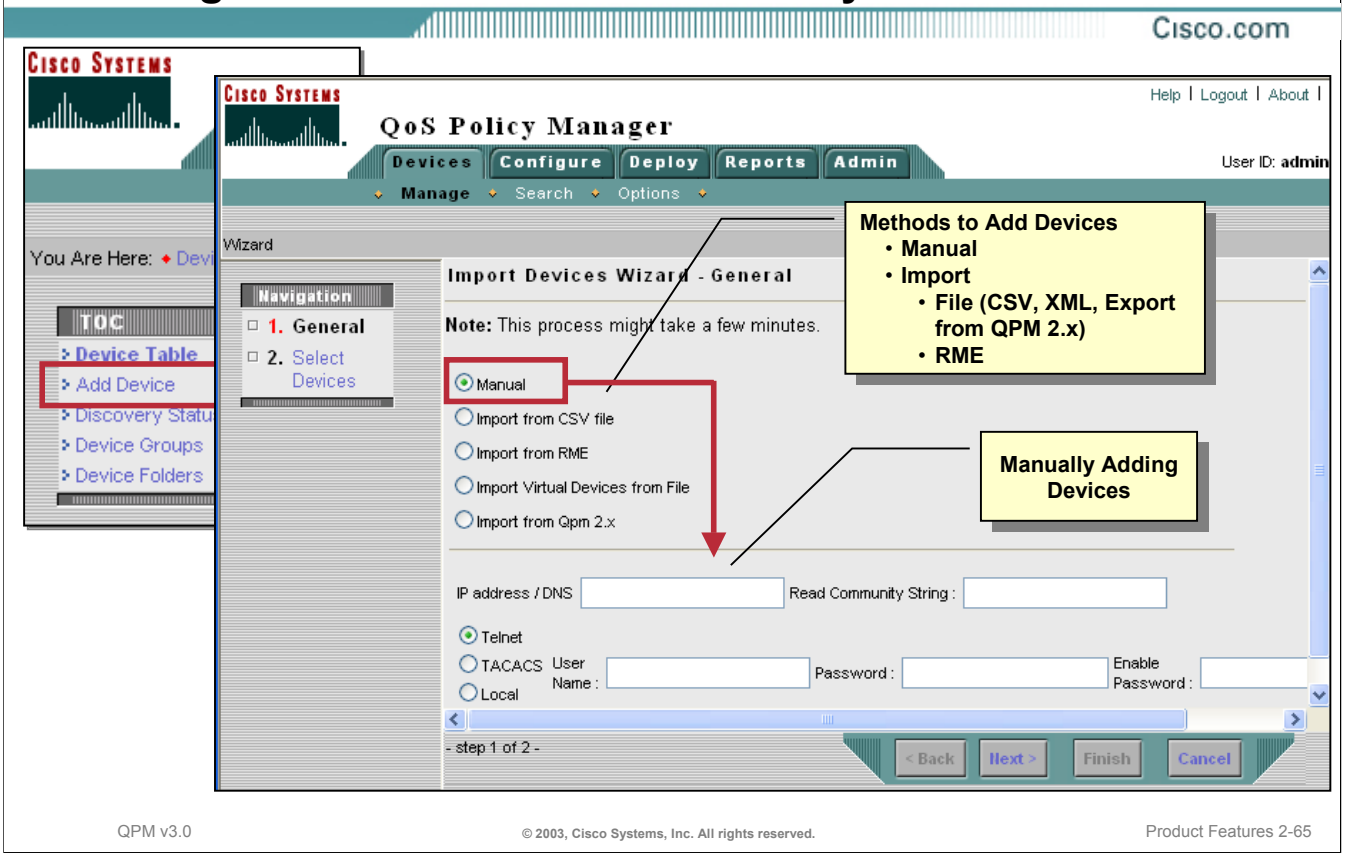
- Manually through the QPM user interface
- Imported from a CSV file
- Imported from the CiscoWorks RME inventory

The devices are place in an appropriate device group, depending upon the user authentication and authorization method chosen. Device groups define user access parameters and device settings for the devices within the group.

- If QPM is configured to use CiscoWorks for user permissions, QPM will place all added devices into the default device group defined by QPM.
- If QPM is configured to use ACS for user permissions, QPM will place devices in device groups as defined by ACS.

As illustrated, the devices within the device groups can be organized for administrative purposes into device folders. How to create and add devices to device folders will be discussed after the devices have been added to QPM.

Getting Started
Adding Devices to the QPM Inventory



Adding Devices to the QPM Inventory

To manage the QoS configuration on a device or any of its interfaces with QPM, the user must first add the device to the inventory. Devices can be added to the QPM inventory by one of the following ways:

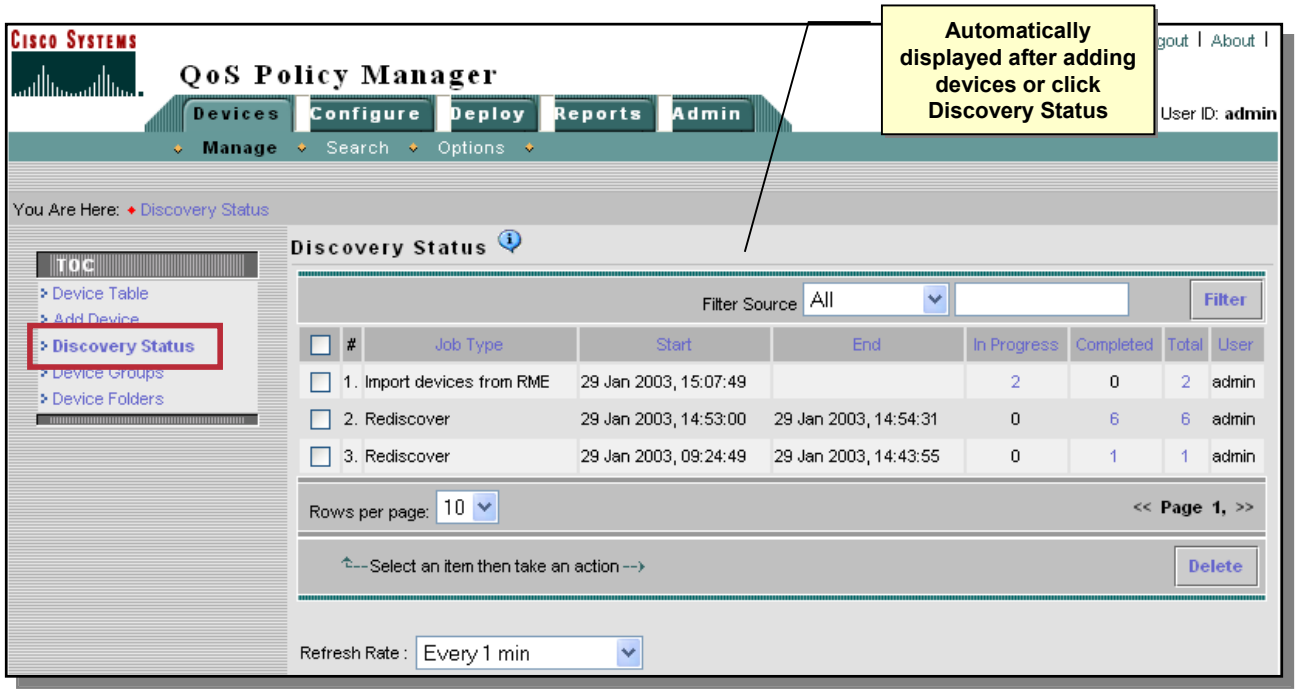
- Manually add the device by providing the IP address, SNMP read community string, and telnet, TACACS, or local passwords
- Import the device(s) from a file stored on the client (CSV, XML, or exported file from QPM v2.x)
- Import the device(s) from a local or remote CiscoWorks RME inventory

When a device is added to the QPM 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 they can be added to the inventory.

A QPM user can only add a device to the inventory if the user has sufficient access permissions to it. The Import Devices Wizard shows which devices cannot be imported because of insufficient permissions.

When a device is added to the inventory, all of its network elements that QPM supports are automatically added.

Getting Started
Verifying Device Discovery

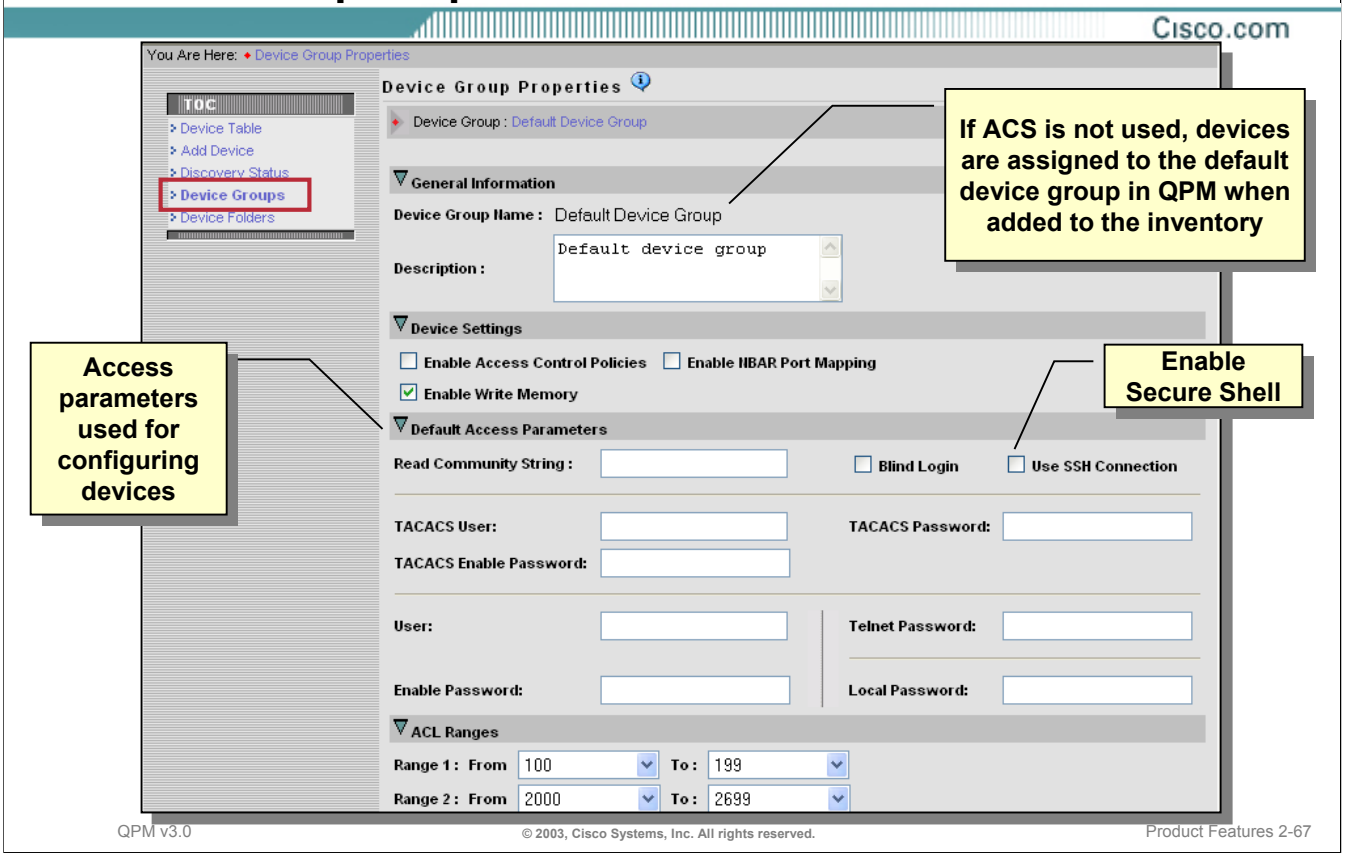


Verifying Device Discovery

After importing devices, use the *Discovery Status* task in the TOC navigation menu to verify the status of the process.

Prior to adding the device to the inventory, QPM accesses the device using the imported passwords. If the process fails, check the device access parameters.

Getting Started
Device Group Properties



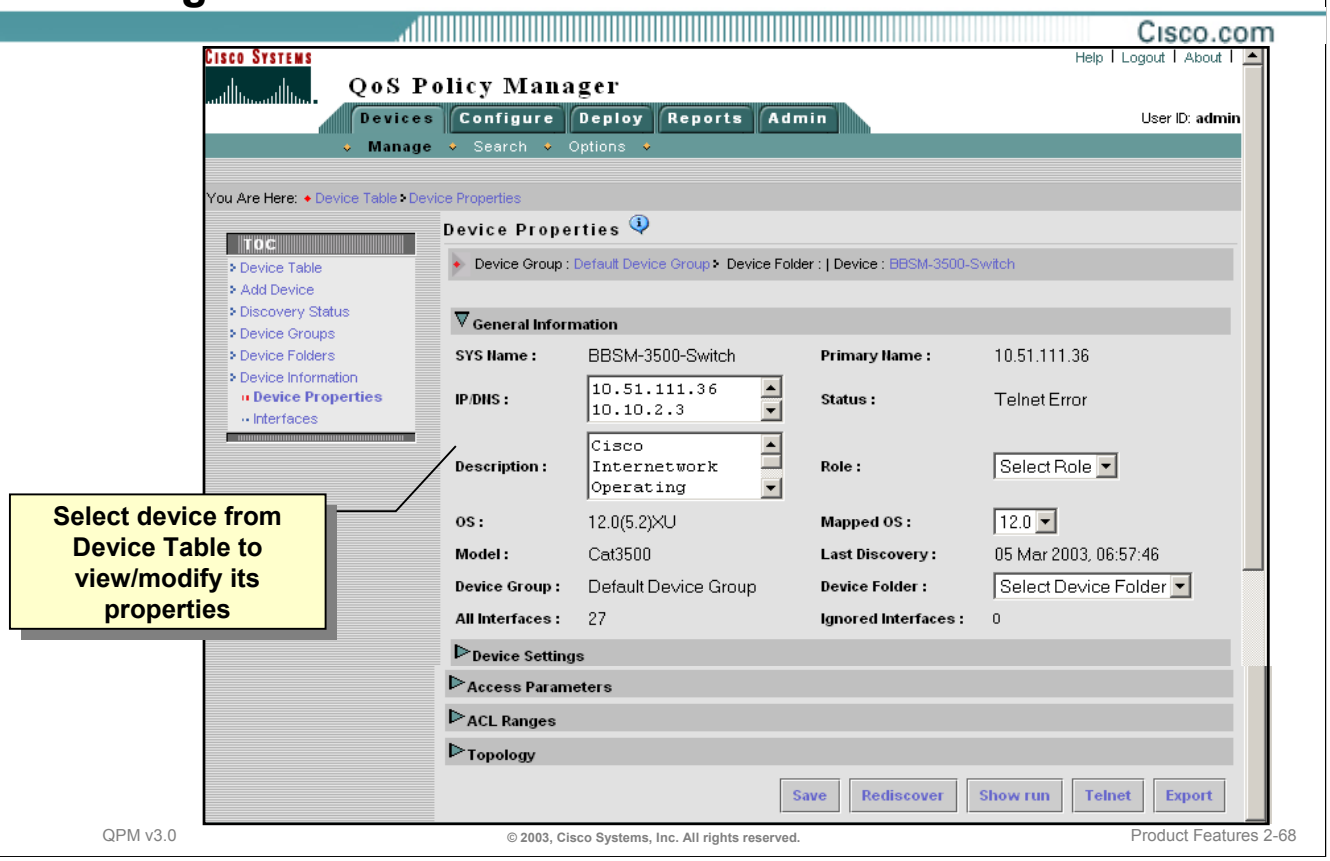
Device Group Properties

Device groups are applicable only for users who use ACS permissions, and are working with ACS device groups . If you do not use ACS or only use a single device group in ACS, then only the default device group will be available in QPM.

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

To view the default access parameters and settings for the QPM device group or the imported ACS device groups, use the *Device Groups* task from *Devices* > *Manage*.

Getting Started
Editing Device Information



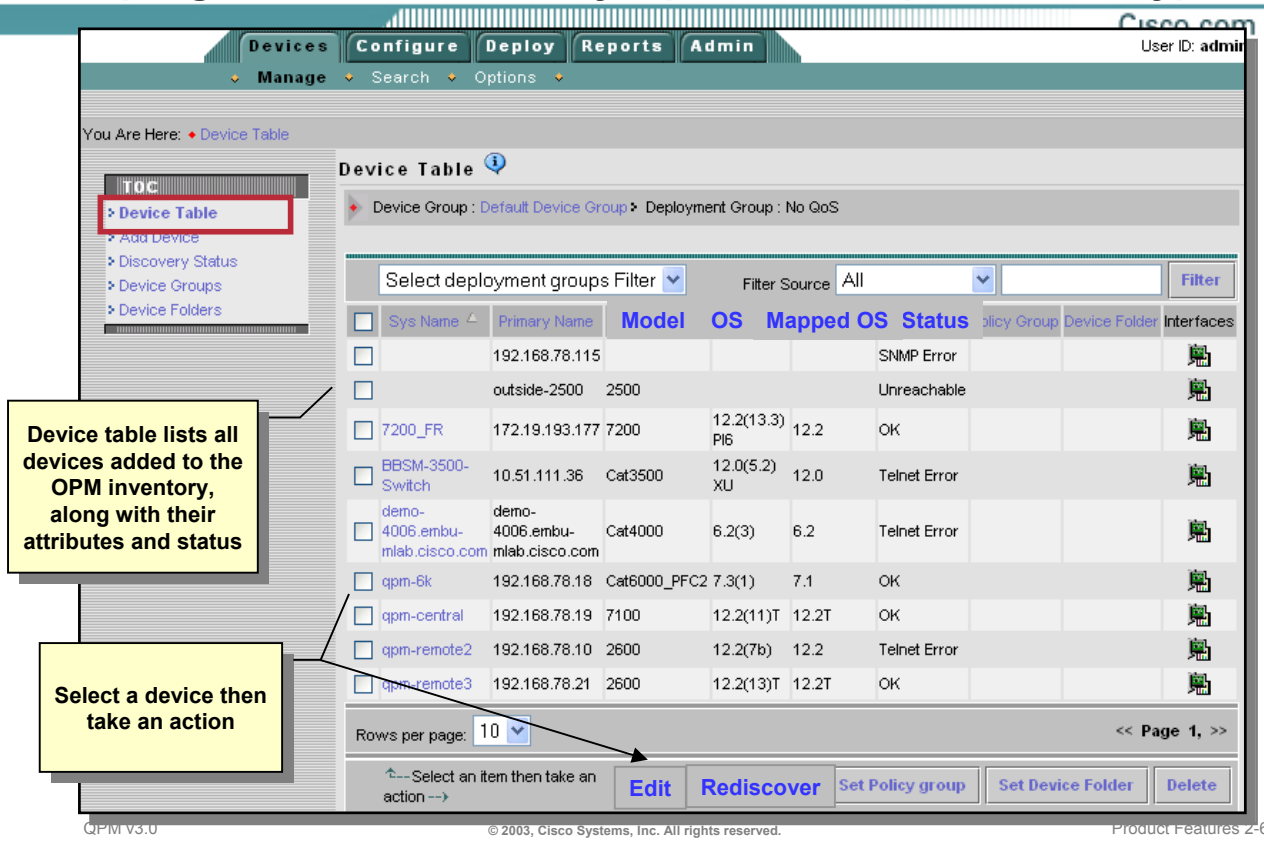
Editing Device Information

After a device has been added to QPM, it will be listed in the Device Table. From the Device Table, select a device to view and/or modify its properties. These properties have been gathered by QPM either during the import or add process or they have been discovered by QPM by reading the MIB table on the device using SNMP.

In this illustration, there is a Telnet Error. Therefore, the user should open the Access Parameters section of this page and enter or verify the Telnet password.

To learn more about each of the device property fields, refer to the scenarios in Chapter 3, the QPM User Guide, or the on-line help.

Getting Started
Keeping the QPM Inventory Up-To-Date (Rediscovery)



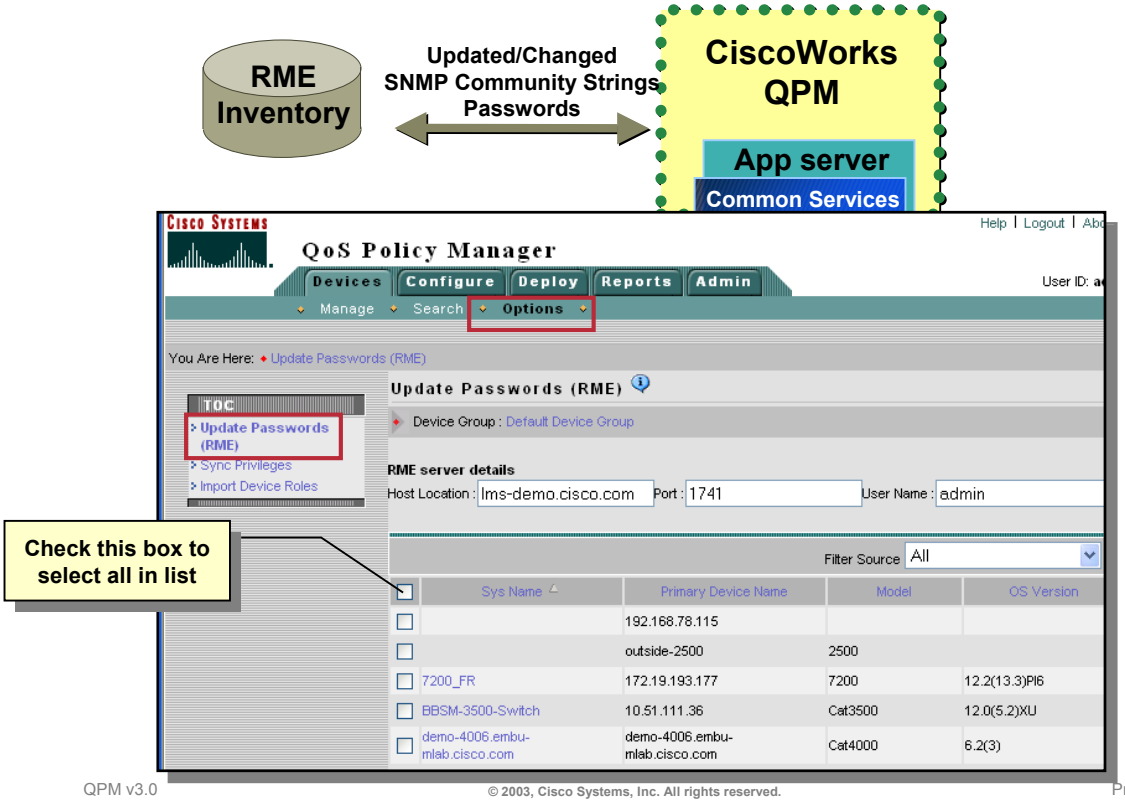
Keeping the QPM Inventory Up-To-Date (Rediscovery)

Rediscovering device information causes QPM to connect to the device on the network and obtain its device information again. Device information should be rediscovered if configuration changes to a device are made to ensure that the device can still support the policies and configurations that are 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.

To rediscover the devices in the inventory, follow these steps.

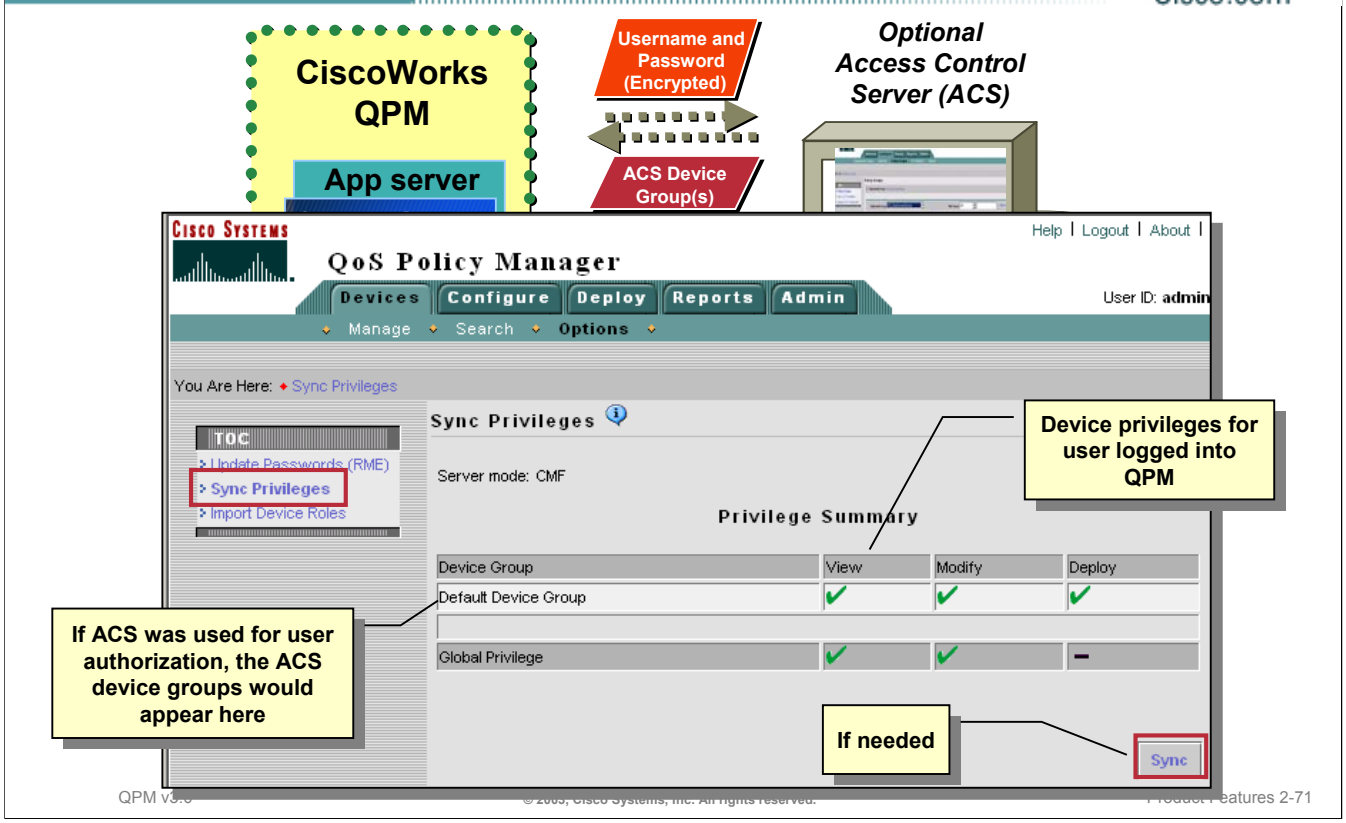
1. Select *Devices* > *Manage*. The Device Table page appears.
2. Select the check boxes next to the devices you want to rediscover, then click *Rediscover*. The Device Table page refreshes. The rediscovery status is displayed in the Status column.
3. Run the Assignments report by selecting *Reports* > *Conflicts* > *Assignments* to see if any policy group assignments were deleted as a result of the rediscovery.



Keeping the QPM Inventory Up-To-Date (Passwords)

If using CiscoWorks RME in the network, device access parameters in the device inventory can be updated with the information already available from RME. This is a convenient way to update the device inventory when device access parameters changes. Select the *Update Passwords (RME)* task from *Device* > *Options* menu. Then select the devices to have the access parameters updated.

Getting Started
Keeping the QPM Inventory Up-To-Date (Privileges)



Keeping the QPM Inventory Up-To-Date (Privileges)

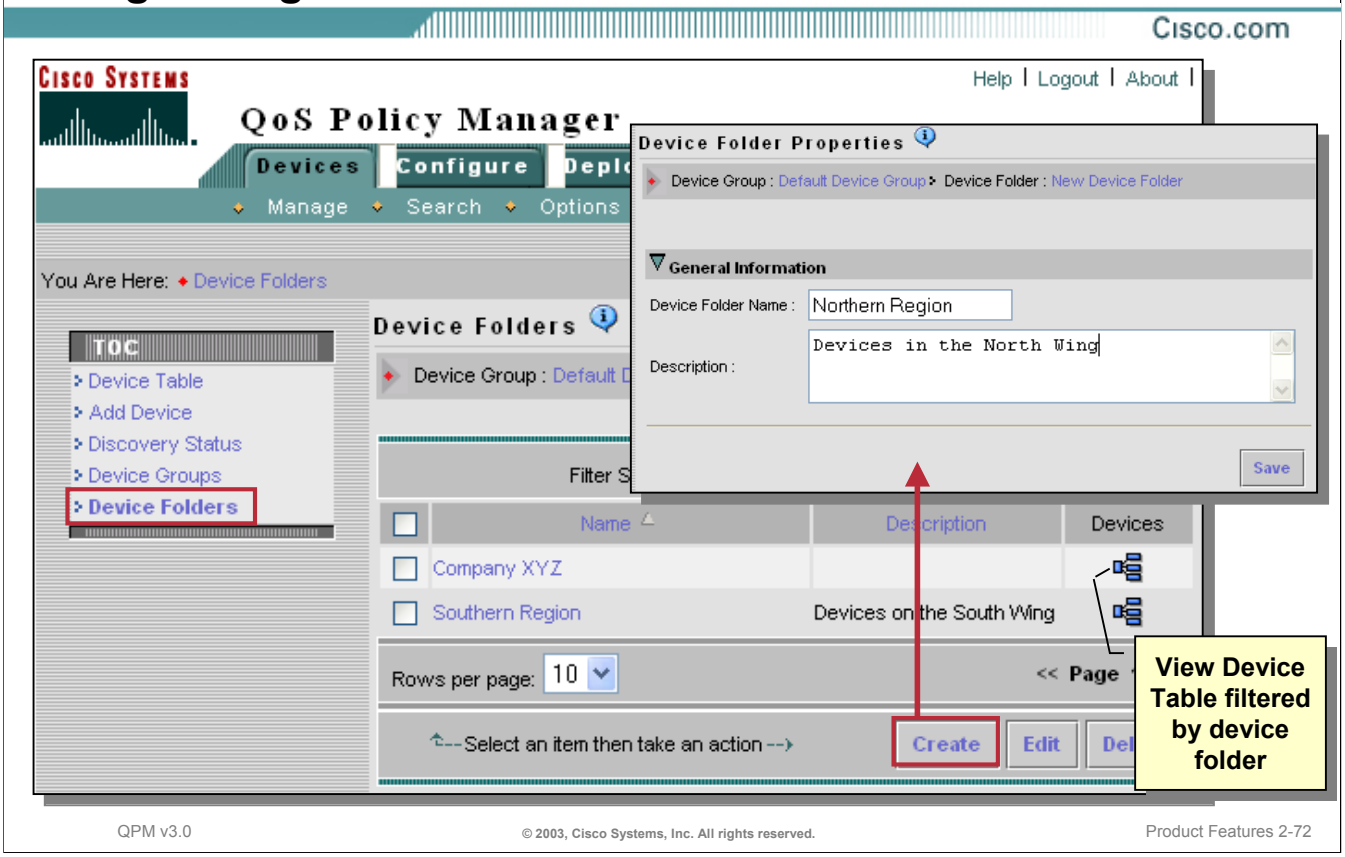
User permissions and device group information in the inventory can be manually synchronized with ACS or CCS (depending on which is being used to administer device groups and user permissions). Synchronization is needed when:

- Change have been made to the ACS or CCS device group assignments or access privileges.
- Changes have been made to the CiscoWorks user role since last logged into QPM.

The Sync Privileges page displays the permissions for the logged in user to the QPM device groups on the system so it can be determined if synchronization is needed to update the QPM permissions. From this page, determine whether the logged in user can view, modify, or deploy device configurations.

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.

Getting Started
Organizing Devices into Device Folders



Organizing Devices into Device Folders

For large networks with many devices, it may be convenient to keep track of the devices in the QPM inventory using device folders. Device folders are groups of devices, used for organizational purposes. For example, the user might create a device folder for each network region in the network and assign the devices in each region to their corresponding device folder.

After a device has been added to QPM, the device is added to the appropriate device group for user/device authorization. No folders exist.

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

Unlike device groups, access privileges can not be assigned 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 within QPM.

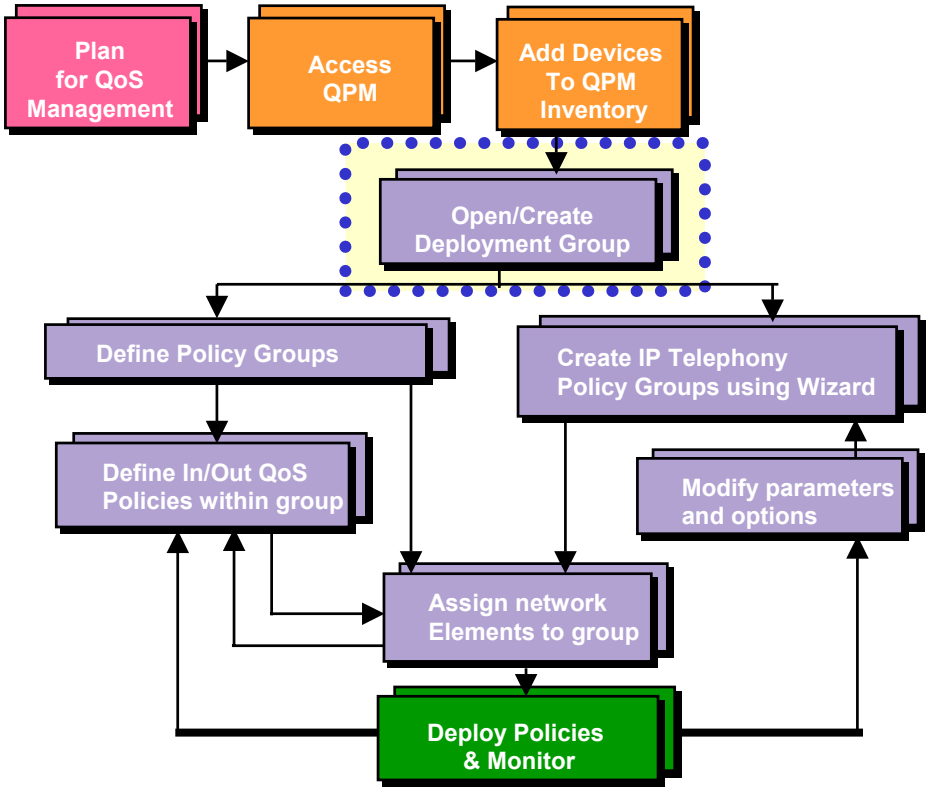
Use the *Devices* > *Manage* > *Device Folders* page to view, create, edit, and delete device folders.

Add devices to a Device Folder by going to the *Device Table*, select the devices to move to a folder, and then click the *Set Device Folder* button. The assignment of the device folder will be illustrated in the Device Table.

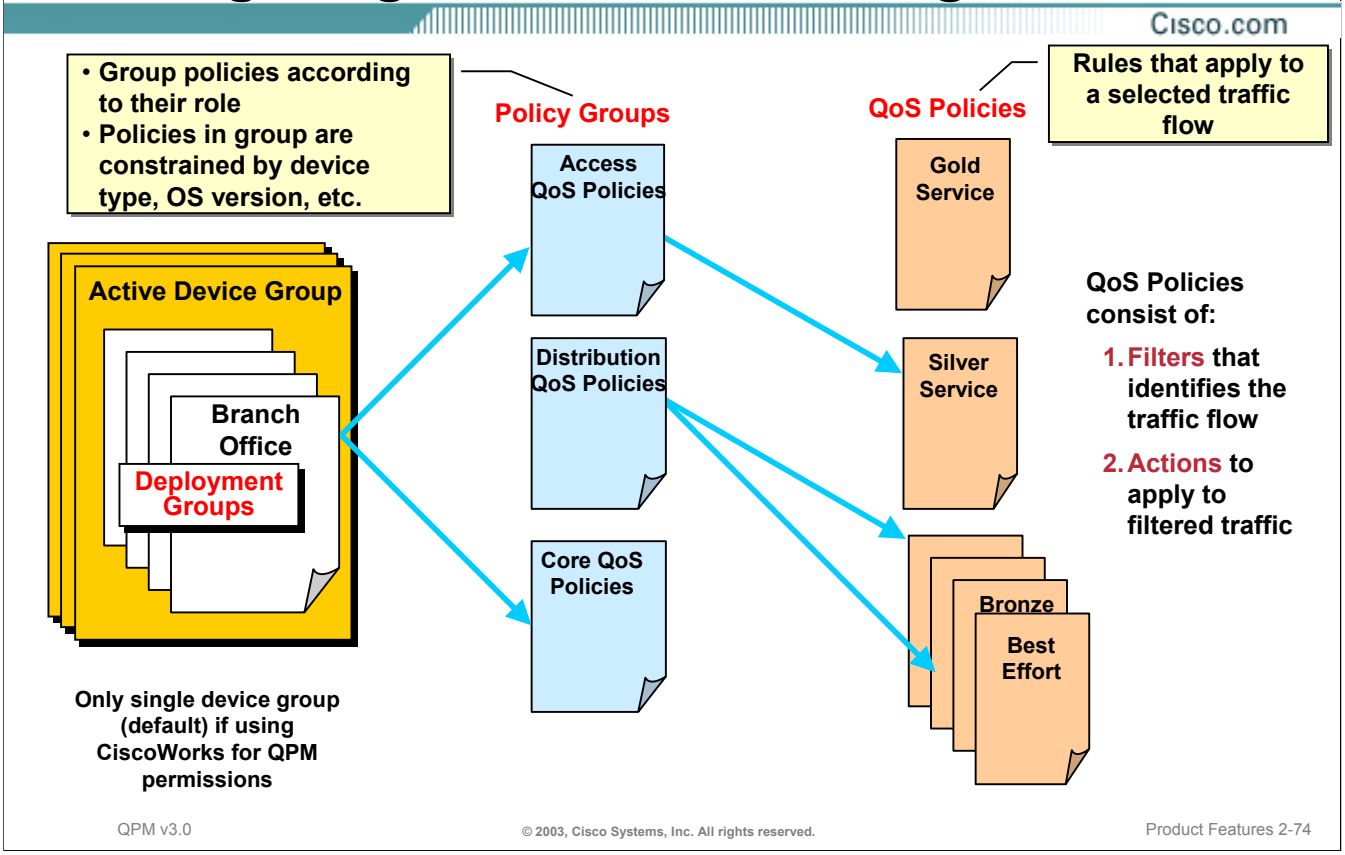
Tip: Easily locate devices by filtering using the device folder name.

Roadmap

Deployment Groups



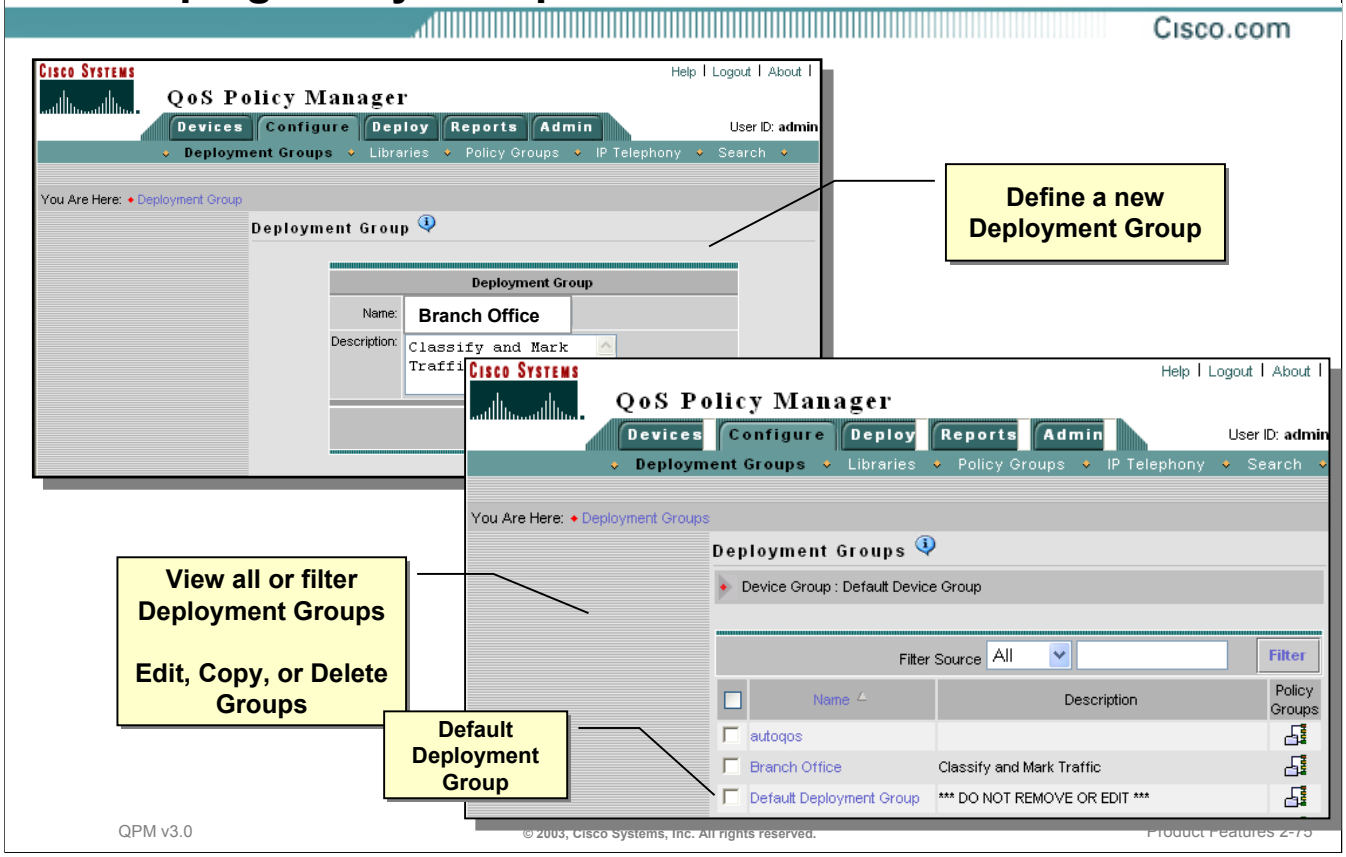
Configuring QoS Policies Using QPM



Configuring QoS Policies using QPM

QPM facilitates management of large networks by allowing the user to create multiple QoS deployment groups, formerly called databases in QPM v2.x, each of which manages a sub-set of the network devices. In this way, the network can be partitioned (typically by region and/or types of devices) and the QoS policies can be deployed in groups across the network. The number of devices managed in a single deployment group will vary and should be limited to a manageable subset of devices. Each QoS deployment group can be managed separately, and can thus be assigned to specific individuals according to areas of administrative responsibility. A device can be associated with one or more deployment groups.

Defining a Deployment Group
Grouping Policy Groups



Grouping Policy Groups

Deployment groups are used in QPM to help organize and separate QoS policies based on functional deployment. Deployment groups contain policy groups and associated information required to deploy policies to devices, such as the QoS policies for the group, IP aliases, application aliases, and network elements assigned to the group. 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. These audit trails can be viewed under the *Admin* tab.

To create a new deployment group, follow these steps:

1. Select the *Configure* tab.
2. Select the *Deployment Group* sub-category under the Configure tab.
3. Enter a name and description for the new deployment group, and then click *OK*.

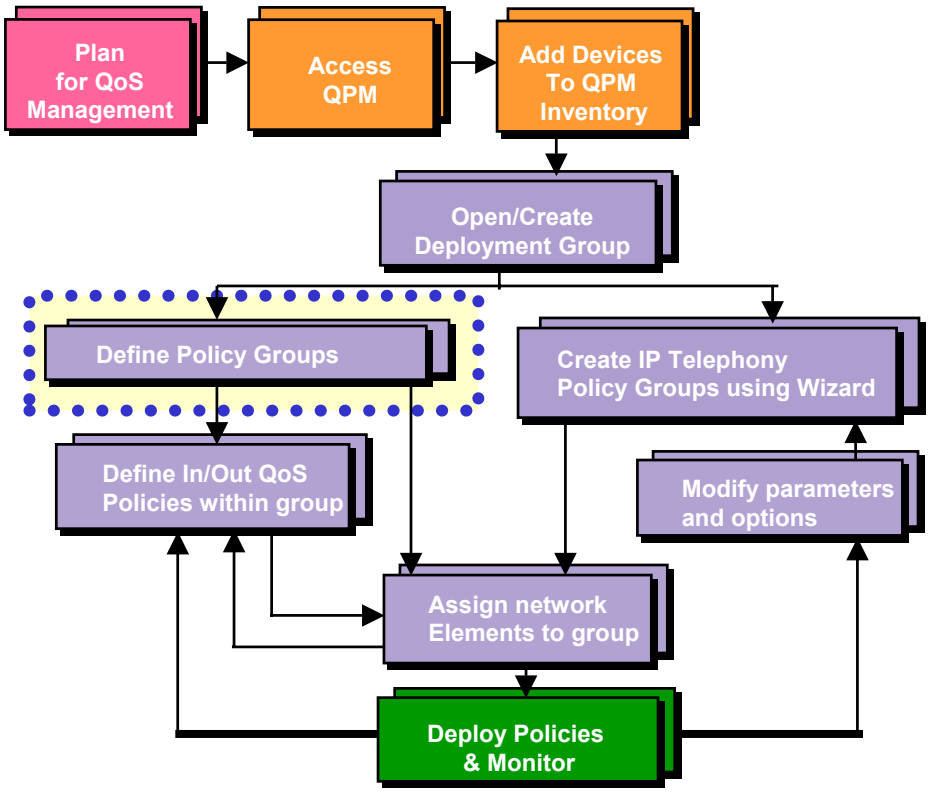
To edit, copy, or delete a new deployment group, follow these steps:

1. Select the checkbox next to the Deployment Group name.
2. Then select the action to take from the buttons in the lower portion of the window.

This page intentionally left blank.

Roadmap

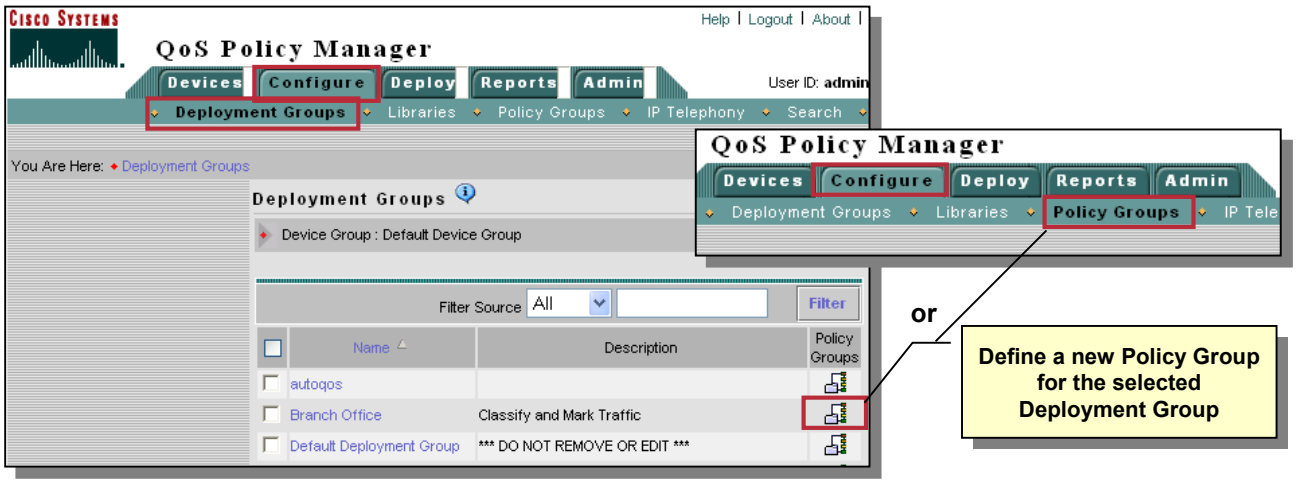
Define Policy Groups



Defining a Policy Group

A Policy Group contains one or more QoS policies.

The policies within the group are constrained by the device type, OS version, interface type,



Defining a Policy Group

Policy groups are constrained sets of QoS policies, and assigned network elements. A policy group consists of the following four components:

- 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.

Each of these are defined using the Policy Group Definition Wizard. To create a policy group, follow either of these two steps:

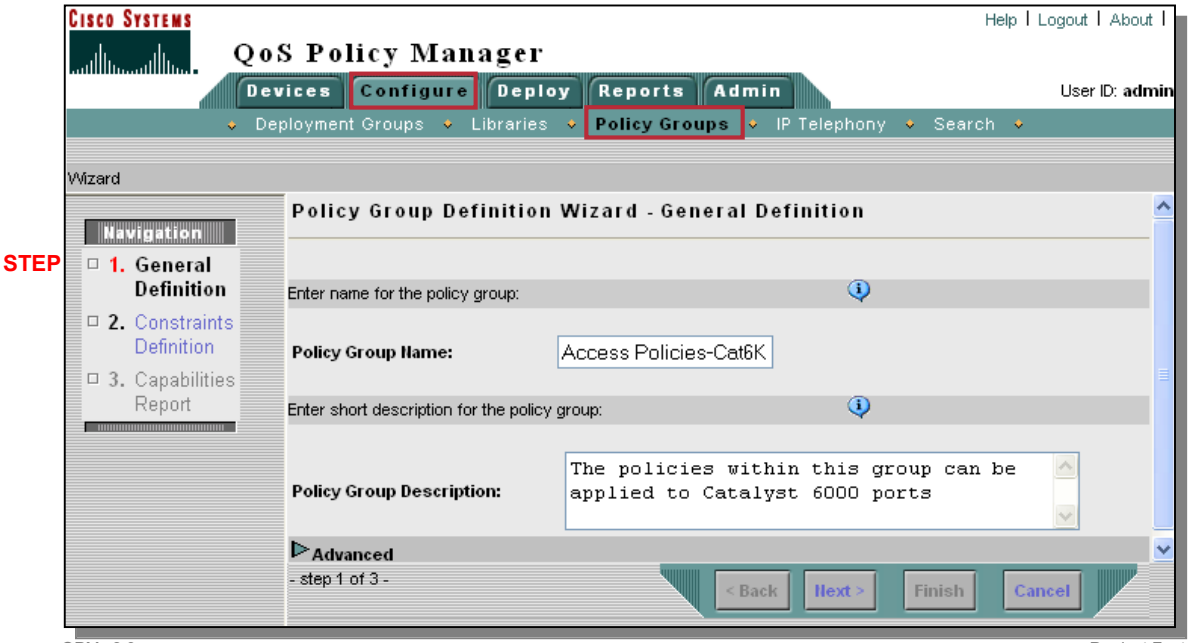
1. From the list of deployment groups, select the Policy Group icon for the associated deployment group; or
2. Select *Configure* > *Policy Groups* from the main tabs in QPM.

A list of existing policy groups is listed for the selected deployment group. Click *Create* to define a new policy group.

Defining a Policy Group
General Information

Cisco.com

Define Policy Group using a 3-step Wizard.



STEP

General Information

The first step to defining a new policy group is to provide a meaningful name and short description for the policy group. Since a policy group limits the type of QoS policies that are defined within the group by defining the device constraints, it is likely that multiple policy groups will need to be defined for the various device types and software versions.

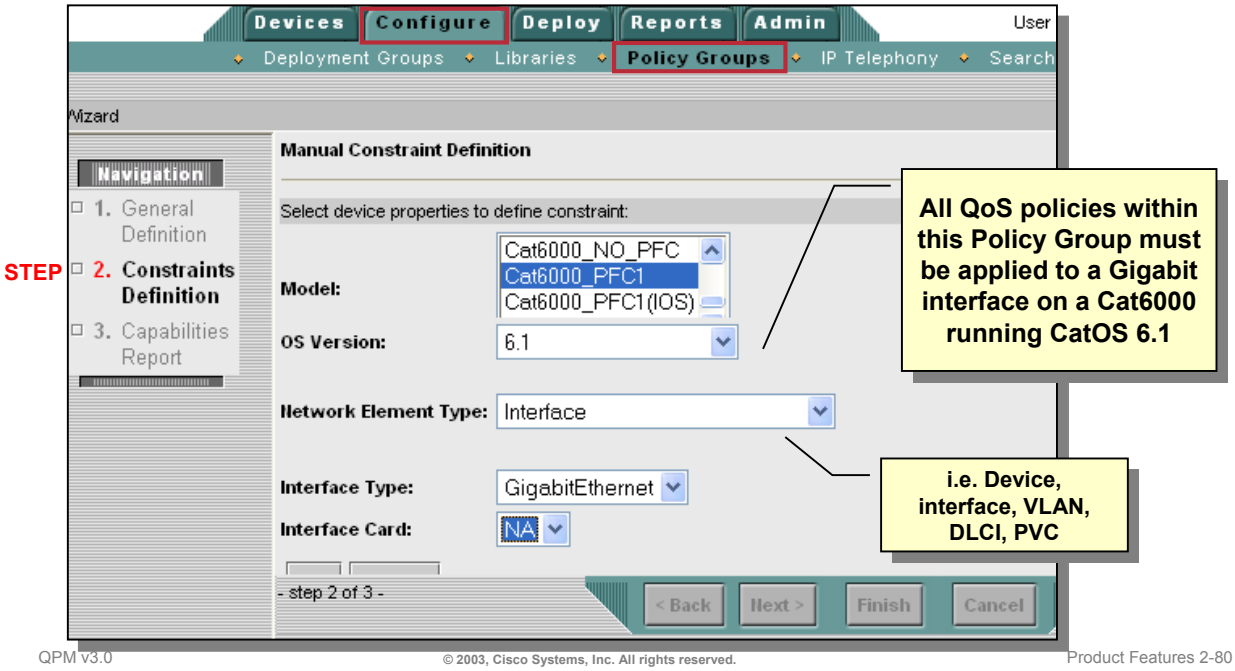
Also, policy groups can be assigned to only one type of network element, such as an interface, DLCI, or VLAN. For some devices, the user will need to define several policy groups to consolidate the QoS configurations on the device.

To create a complete QoS configuration for a single type of network element, the user might need to define more than one policy group. For example, when configuring Frame Relay traffic shaping policies, and when configuring VLAN policies.

There are other cases, where the user might need two policy groups. For example, to configure markdown in policing policies on Catalyst ports at the *port* level, and to change the default markdown mapping values, an additional policy group must be defined at the *device* level.

Defining a Policy Group
Device Constraints

All QoS Policies added to a Policy Group are limited by the device constraints defined by the Policy Group.

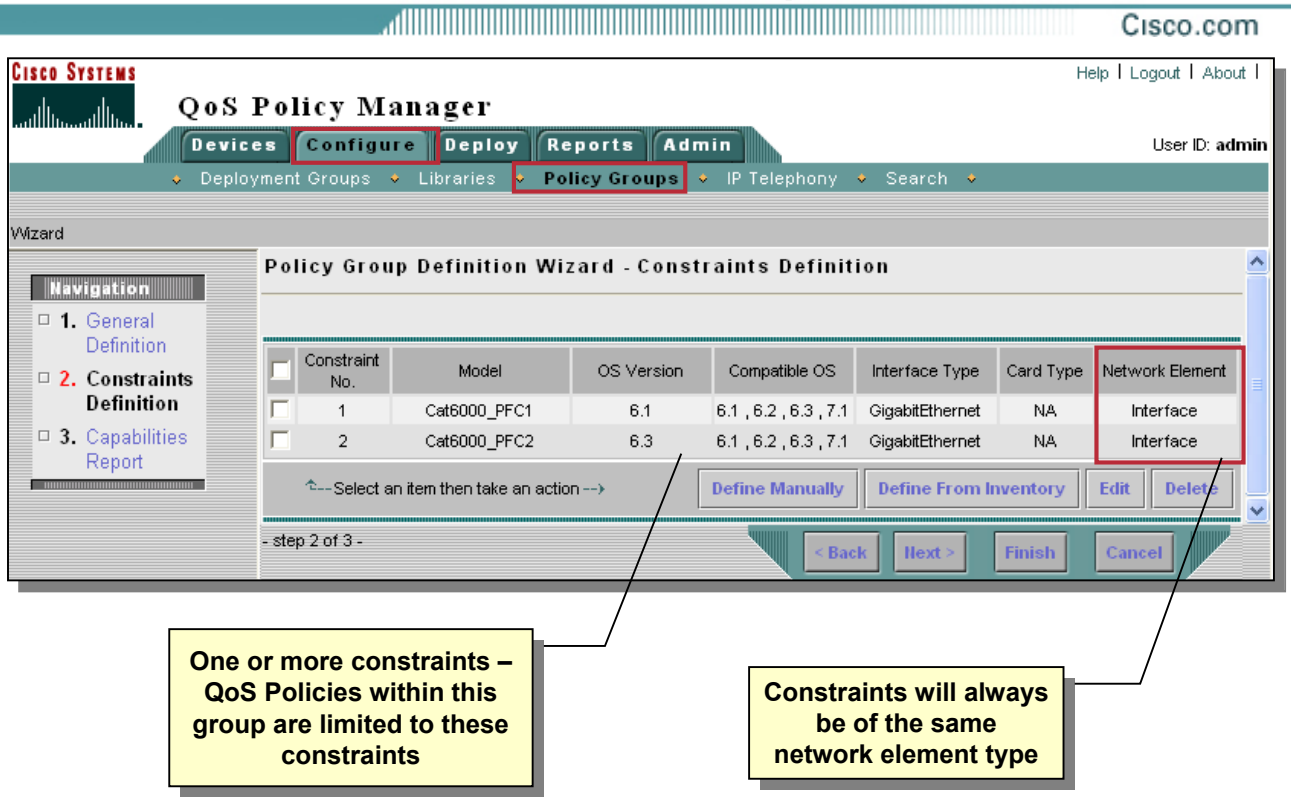


Device Constraints

The next step after providing a name and description is to define the device constraints for the policy group. The device constraint definitions determine the available QoS capabilities for the policy group or template. Thus, all policies saved in this policy group and all network elements assigned to this policy group must meet the constraints. Using constraints is the way that QPM helps the user configure policies that are supported by the OS, interface, and device model.

Prior to this illustration, the user can choose to define the device constraints manually or to define the device constraints by listing the device models, interfaces, and OS versions that exist in the inventory for selection.

Defining a Policy Group
Device Constraints within the Group

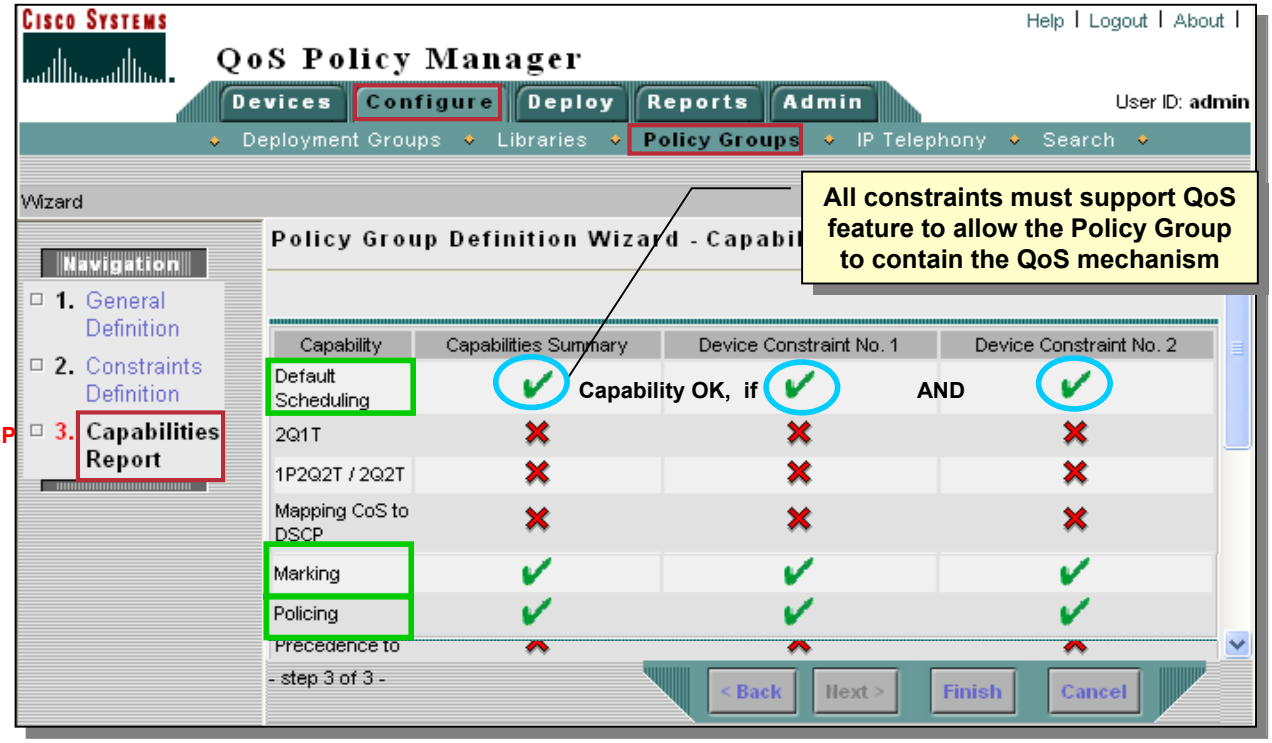


Device Constraints within the Group

A policy group can consist of one or more device constraint definitions, just as long as the network element type is the same. In this illustration, the policy group has two device constraints defined. Thus, all policies in this group must be written for Catalyst 6000 devices with PFC1 or PFC2 (policy feature cards), with a range of OS versions, and can only be applied to Gigabit Ethernet interfaces.

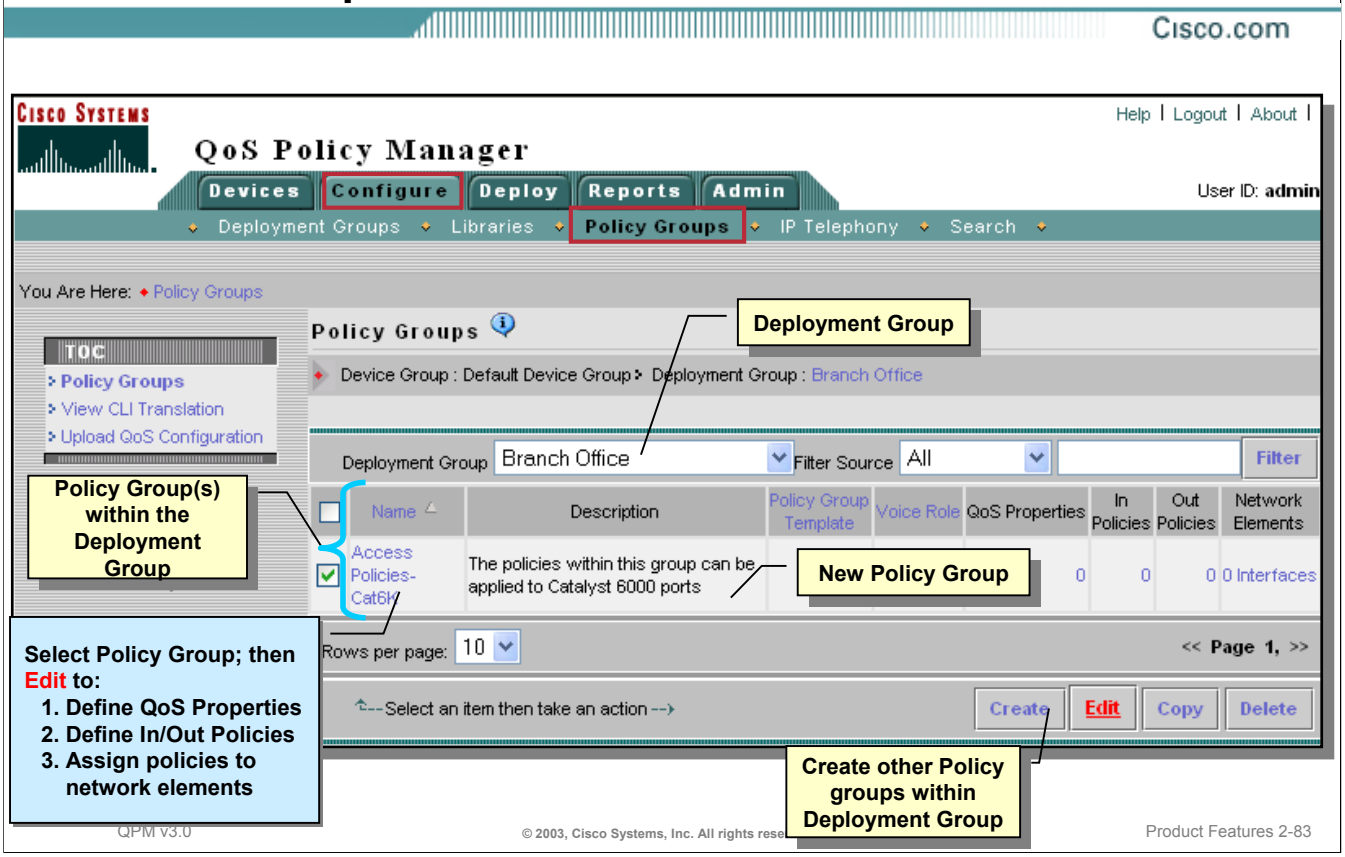
Notice in the table that the selected OS version will also accept devices with other OS versions. These compatible OS versions are acceptable since they have the same QoS capabilities.

Defining a Policy Group
QoS Mechanisms Available for the Group



STEP

Defining a Policy Group
The Next Steps …



The Next Steps

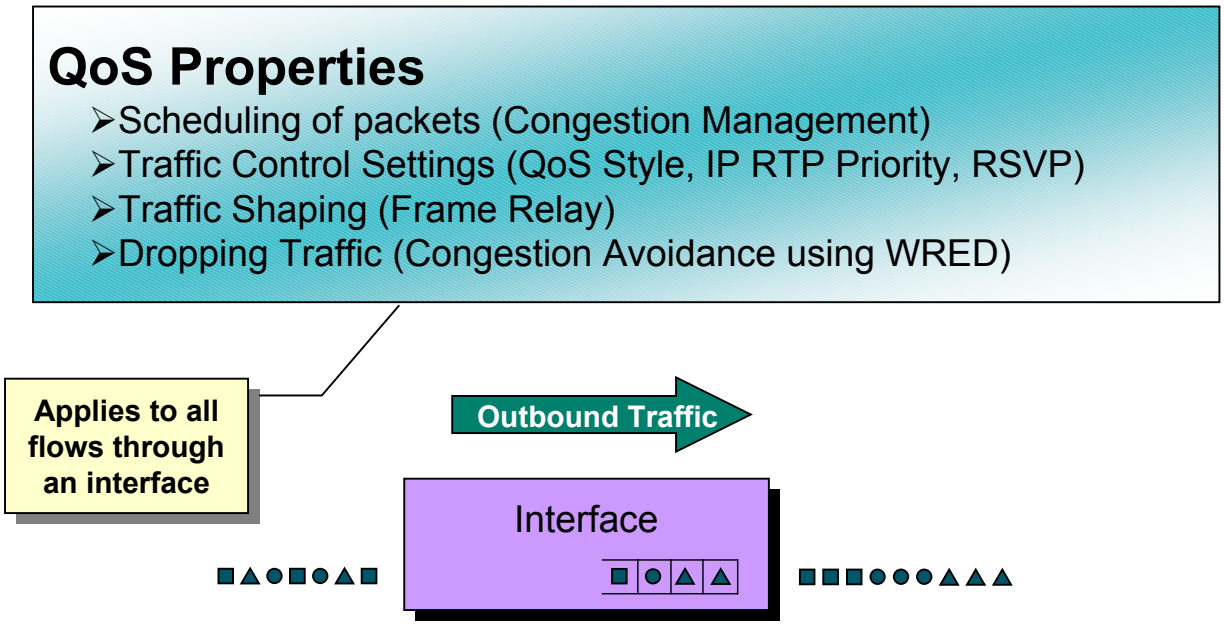
Once a policy group has been named and the device constraints for the group have been defined, the next step is to edit the policy group and perform the following steps:

1. Define the QoS properties for the policy group. The QoS properties define how the packets are to be handled for congestion management, traffic shaping, or congestion avoidance.
2. Define the individual In/Out QoS policies within the policy group.
3. And finally, assign the policies to the network elements. The network elements are the individual interfaces, sub-interfaces, or VLANs on a device.

To edit a policy group to perform these steps, simple check the box next to the name of the policy group and then click *Edit*.

Defining a Policy Group
What are QoS Properties?

Cisco.com



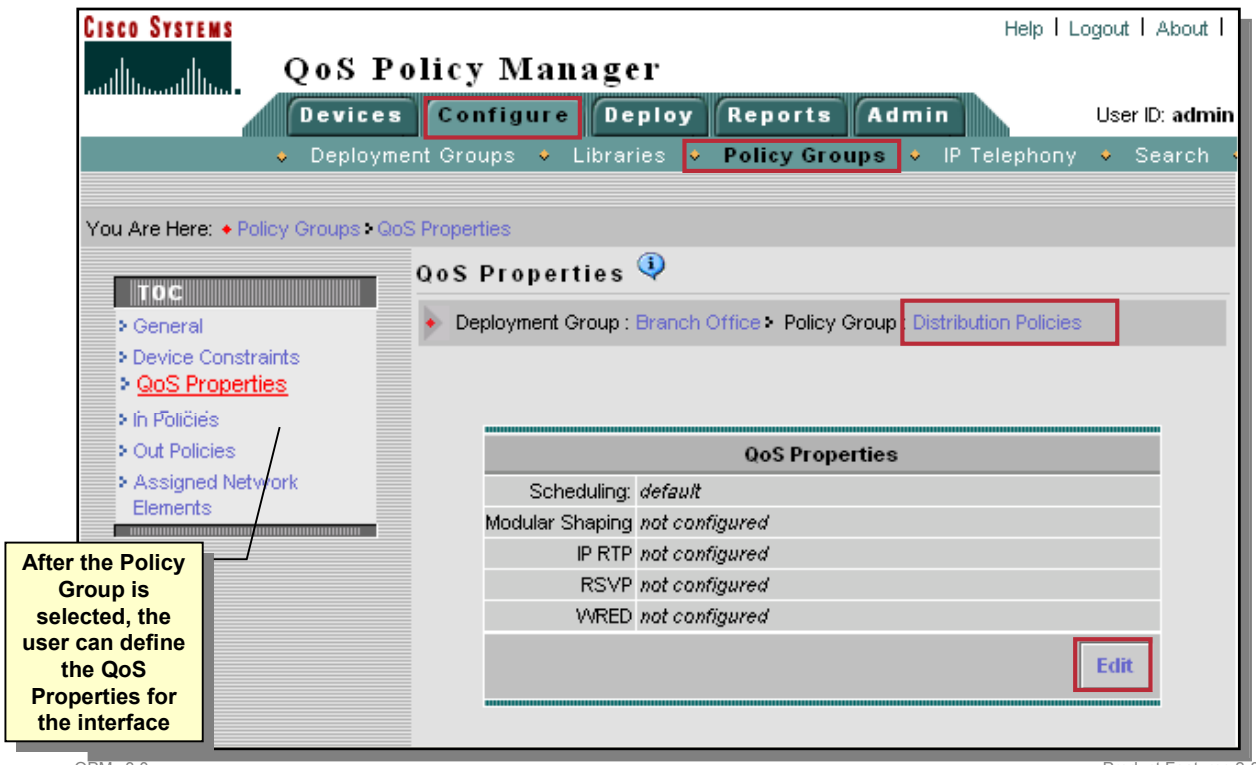
What are QoS Properties?

Defining the QoS Properties is a very important step when defining the QoS policy actions later. The QoS Properties are not defined as a policy action. The QoS Properties may be used to determine which traffic is placed in which queue using priorities, how to smooth the traffic flow, or how to drop packets when congestion is detected.

When packets incoming to an interface exceed the available outgoing bandwidth of the interface, it is desirable to queue the packets until bandwidth becomes available and transfer is possible. By employing different scheduling techniques, it is possible to grant preferred treatment to certain types of packets. This effectively grants different qualities of service to different traffic flows. The queuing technique employed on an interface or device group is known as the QoS Property.

Each interface can only have one QoS property defined on it. This property in conjunction with various device characteristics (IOS version, device model, interface type), will dictate the possible QoS policies actions available to the interface.

Defining a Policy Group
Defining the QoS Properties



Defining the QoS Properties

After selecting the policy group for editing, the user can select to edit the name and description of the policy group by clicking on *General* or revisit the Device Constraints list. Here, in this dialog window, the user will define the QoS properties for the policy group using the QoS Properties wizard.

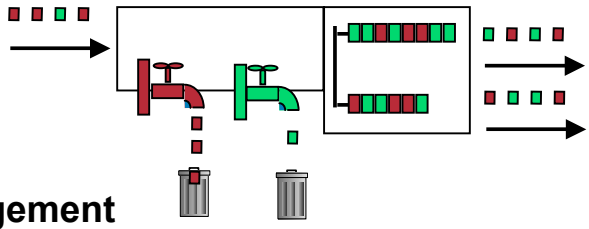
The QoS Properties wizard allows the user to configure only those QoS properties that conform to the device constraints of the policy group. (These capabilities are viewable in the Capabilities report, described earlier.) Some QoS properties are inter-dependent, therefore the selection of available QoS properties might change as the user proceeds through the wizard.

The current QoS properties are displayed when *QoS Properties* is selected in the TOC window. To change the QoS properties, click *Edit*. First, the Scheduling page of the QoS Properties wizard appears.

Defining a Policy Group
Defining the QoS Properties - Scheduling

Cisco.com

Dependent upon the device type and OS version



- **Congestion Management**
  - **–FIFO**
  - **–Priority Queuing (PQ)**
  - **–Custom Queuing (CQ)**
  - **–Weighted Fair Queuing (WFQ)**
  - **–Class-Based WFQ (CBWFQ)**
  - **–Weighted Round Robin (WRR) (Catalyst® 8510)**

Defining the QoS Properties – Scheduling

The Scheduling Tools define the Congestion Management technique that should be applied to the policies within the group. Below is a list and brief description of available queuing algorithms. Refer to the Terminology section found earlier in this chapter for more details on each of these techniques.

FIFO (First In, First Out) - This algorithm is the simplest queuing mechanism. No attempt is made to prioritize packets. The first packet in is the first packet transmitted.

Priority Queuing - In this algorithm, packets are classified by policies into 4 priority queues. The highest priority queue is completely transmitted before servicing the lower priority queues. This algorithm can lead to starvation of low priority packets.

Custom Queuing - This algorithm is a more flexible queuing approach that eliminates starvation. Policies are used to place packets into 16 different policy defined queues. Each queue is weighted to determine how much bandwidth it will receive. Queues are serviced in a round robin fashion. Packets from a queue are transmitted until the allocated amount (based on weight) has been sent, then the next queue is serviced.

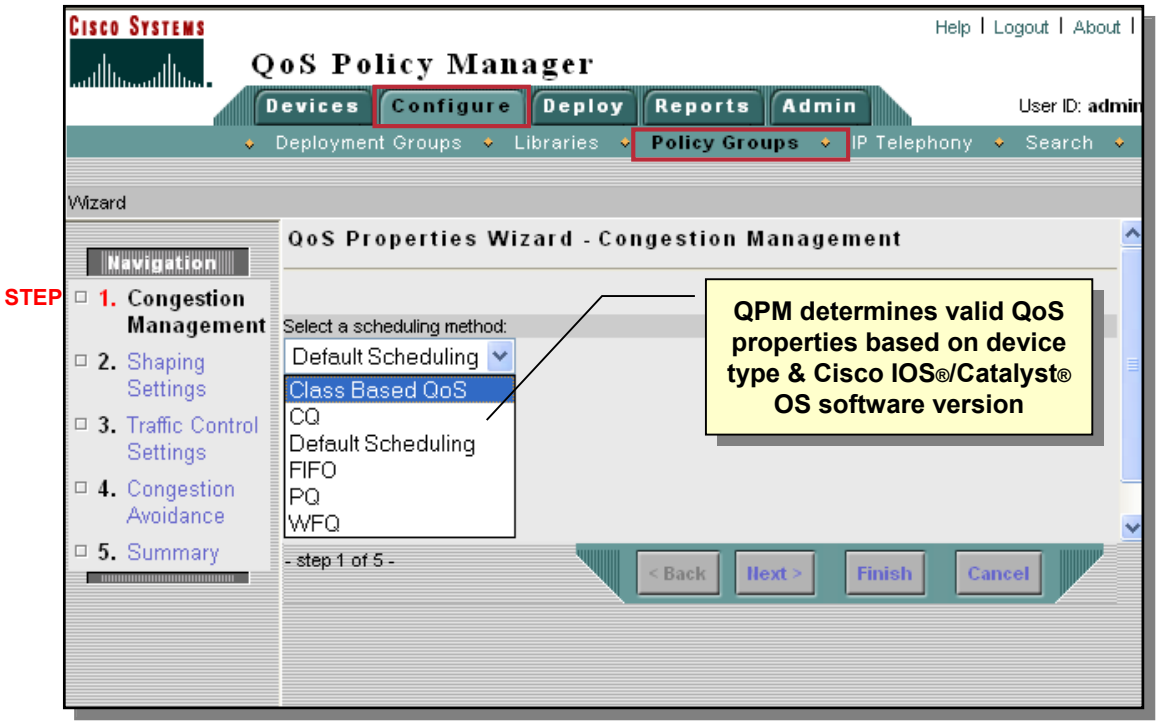
Weighted Fair Queuing - This algorithm automatically prioritizes traffic flows based on packet classification and bandwidth usage. High priority, low bandwidth flows are given highest priority.

Class Based WFQ - This algorithm combines the best characteristics of weighted fair queuing and custom queuing. CBWFQ uses WFQ processing to give higher weight to high priority traffic, but derives that weight from classes that you create on the interface. 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.

Weighted Round Robin - This algorithm is used exclusively on the Catalyst 8510. Packets are queued based on packet classification in one of 4 queues. Each queue is assigned, by policy, a weight which determines how much of the queue will be transmitted during its turn in the round robin scheduling.

Defining a Policy Group
Defining the QoS Properties - Scheduling

Cisco.com



Defining the QoS Properties – Scheduling

Use the Congestion Management dialog window to define the type of scheduling, and the scheduling parameters for a policy group. QPM determines which type of scheduling is valid based on the device type and OS versions defined in the device constraints section for the policy group.

Select *Default Scheduling* to use the default scheduling method already configured on the device. Additional fields might appear in the dialog window according to the scheduling method chosen. For example, if PQ (Priority Queuing) is selected, the maximum queue lengths can be specified for each queue designated for High, Medium, Normal, and Low priority packets.

Click *Next* to proceed to the next QoS Properties page or *Finish* if all QoS Properties are properly defined.

Refer to the QPM User Guide for additional details on each of the scheduling fields that appear.

Defining QoS Properties for QoS Monitoring

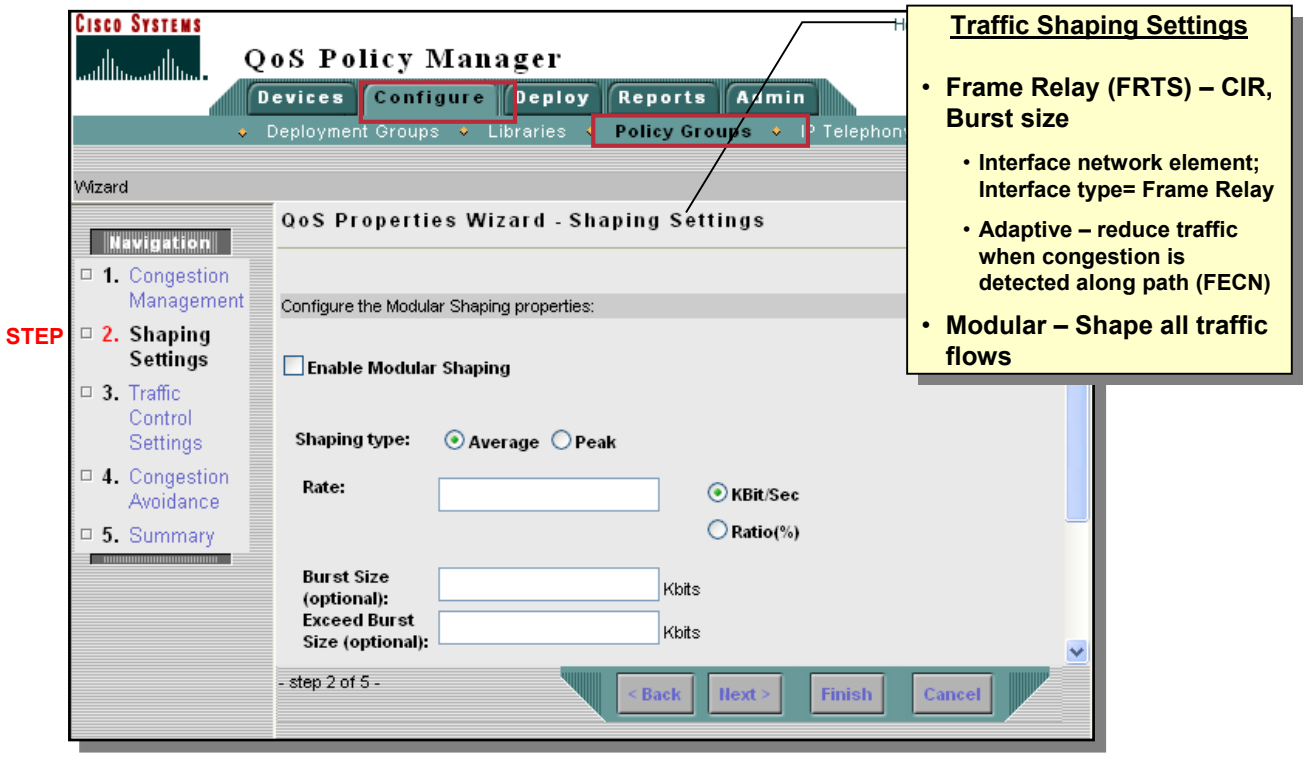
When using QoS policies to monitor and analyze traffic for baselining, set the QoS Property to Class-Based QoS.

Defining the QoS Properties – Scheduling

The table below provides a list of the valid QoS Property settings on interfaces for the various devices and software versions. The user will not have to remember which scheduling methods are valid; this knowledge is built into the QPM product. But it is often nice to know why a particular scheduling method is not listed. So, refer to this list and also check the User Guide for more information.

Interface Type	QoS Property Settings on Interface
Catalyst 6000 Interfaces (Ports or VLANs)	2Q2T/1P2Q2T Trusted IPP, DSCP, CoS, or non-Trusted Apply to port or VLAN
IOS v 11.2 (Ports or VLANs)	Priority Queuing Custom Queuing FIFO WFQ (Weighted Fair Queuing) WRED
IOS v 12.1 (Ports or VLANs)	Priority Queuing Custom Queuing FIFO WFQ (Weighted Fair Queuing) WRED Class Based QoS (CBWFQ)
IOS v 12.1(2)+ (Ports or VLANs)	Priority Queuing Custom Queuing FIFO WFQ (Weighted Fair Queuing) WRED Class Based QoS (CBWFQ) Class Based QoS (Coloring) Class Based QoS (Shaping) Class Based QoS (Limiting)

Defining a Policy Group
Defining the QoS Properties – Traffic Shaping



Defining the QoS Properties – Traffic Shaping

To configure Frame Relay Traffic Shaping (FRTS) properties, or Modular Shaping properties, use the Shaping Settings page.

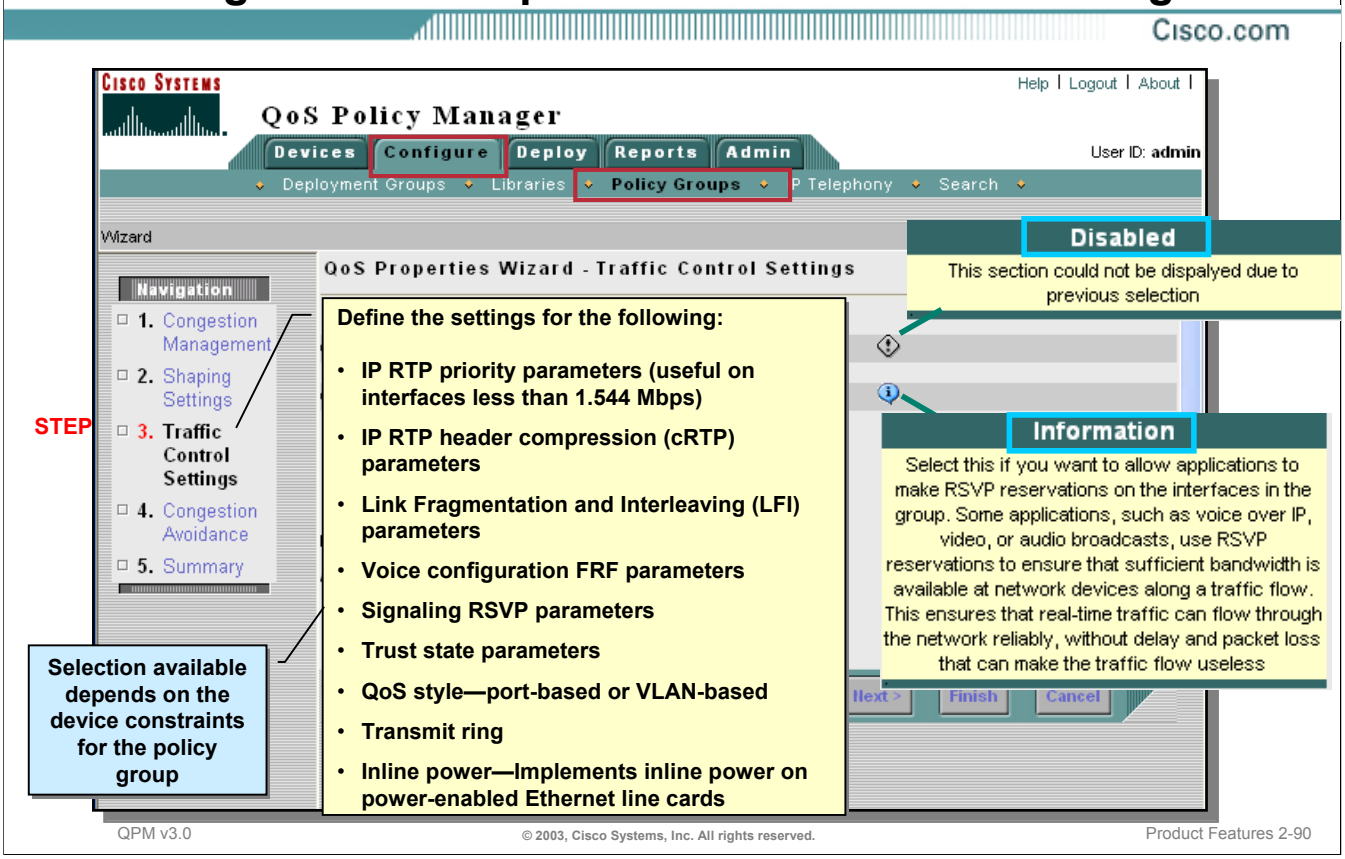
Note on Frame Relay Traffic Shaping – To configure FRTS for frame relay sub-interfaces or DLCIs, the user must create two policy groups since frame relay main interfaces and sub-interfaces can have different QoS capabilities; thus create two policy groups:

- A policy group to enable FRTS on the frame relay main interface to which the sub-interfaces or DLCIs belong and
- A policy group to configure FRTS for the sub-interfaces or DLCIs

Click *Next* to proceed to the next QoS Properties page or *Finish* if all QoS Properties are properly defined.

Refer to the QPM User Guide and the Terminology section found earlier in this chapter for additional details on FRTS and Modular shaping.

Defining a Policy Group
Defining the QoS Properties - Traffic Control Settings



Defining the QoS Properties – Traffic Control Settings

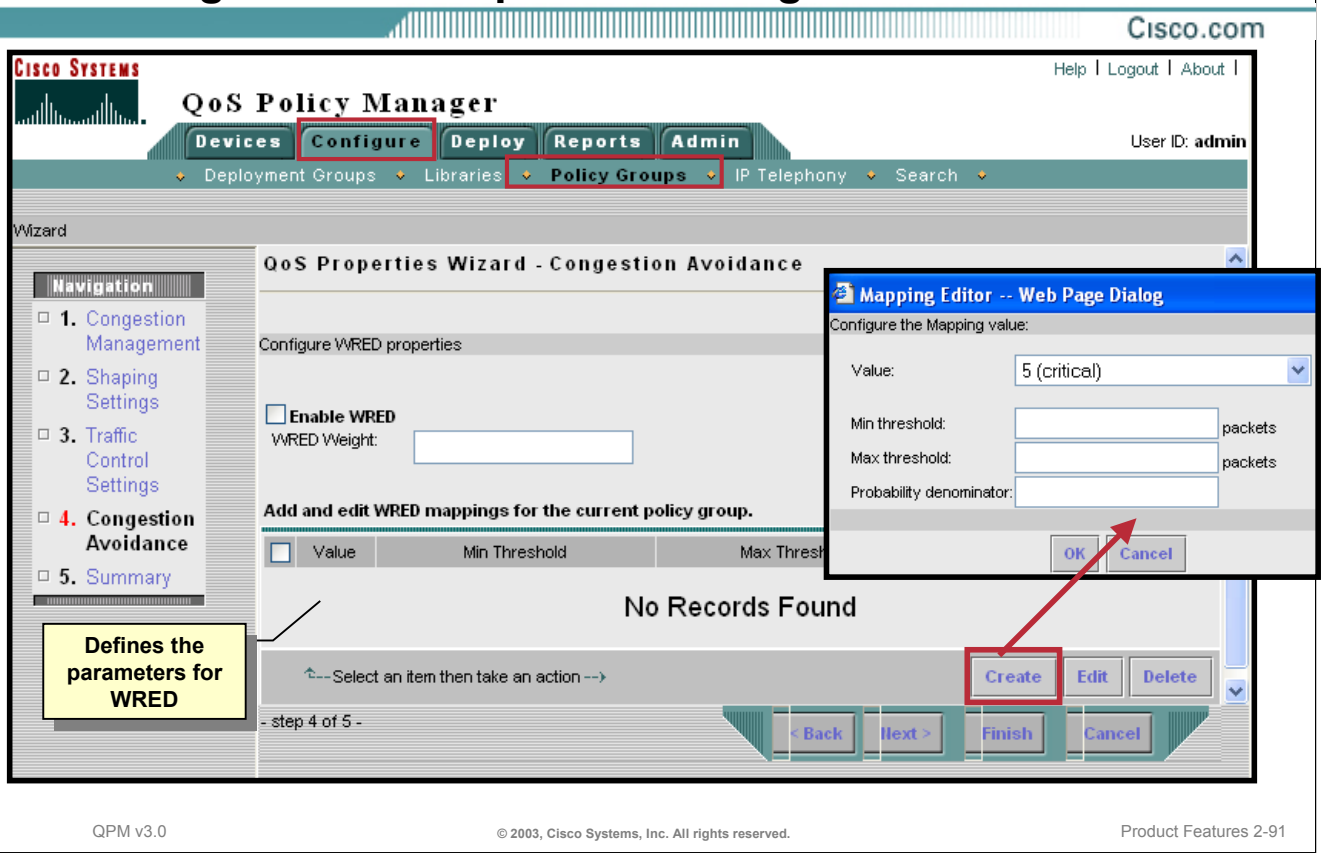
Use the Traffic Control Settings page to define traffic control parameters for a policy group. Examples of Traffic Control settings include:

- IP RTP (Real Time Protocol), available with WFQ and Class Based QoS, can be used to prioritize voice traffic over slow WAN links and can not be used with frame relay traffic shaping (FRTS) or VIP cards. By enabling IP RTP Priority, the interface creates a strict-priority queue for 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 low bandwidth, enabling this feature typically give voice traffic absolute priority without starving other data traffic. This ensures that voice quality is adequate. (IP RTP Priority is not defined as a policy action. The IP RTP Priority configuration defined in the QoS Properties, determines which traffic is placed in the priority queue.)
- Enable LFI to reduce delay on slower-speed links for delay-sensitive traffic.
- Enable RSVP 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.

Refer to the QPM User Guide for details on the other traffic control settings and their associated fields that appear.

Click *Next* to proceed to the next QoS Properties page or *Finish* if all QoS Properties are properly defined.

Defining a Policy Group
Defining the QoS Properties – Congestion Avoidance



Defining QoS Properties – Congestion Avoidance

Use the Congestion Avoidance page to define the packet drop mechanism using WRED (Weighted Random Early Detect) for a policy group. This technique tries to slow down the sender by selectively dropping packets before congestion occurs. If the interface still becomes congested, a FIFO buffer is used.

Enter the factor (WRED Weight) used to determine the rate at which packets are dropped when traffic congestion occurs. The weight must be between 1 and 16.

To define WRED mappings, click **Create** and define the following.

- Select the value for which you want to define threshold values—an IP precedence value, or RSVP.
- 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 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 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.

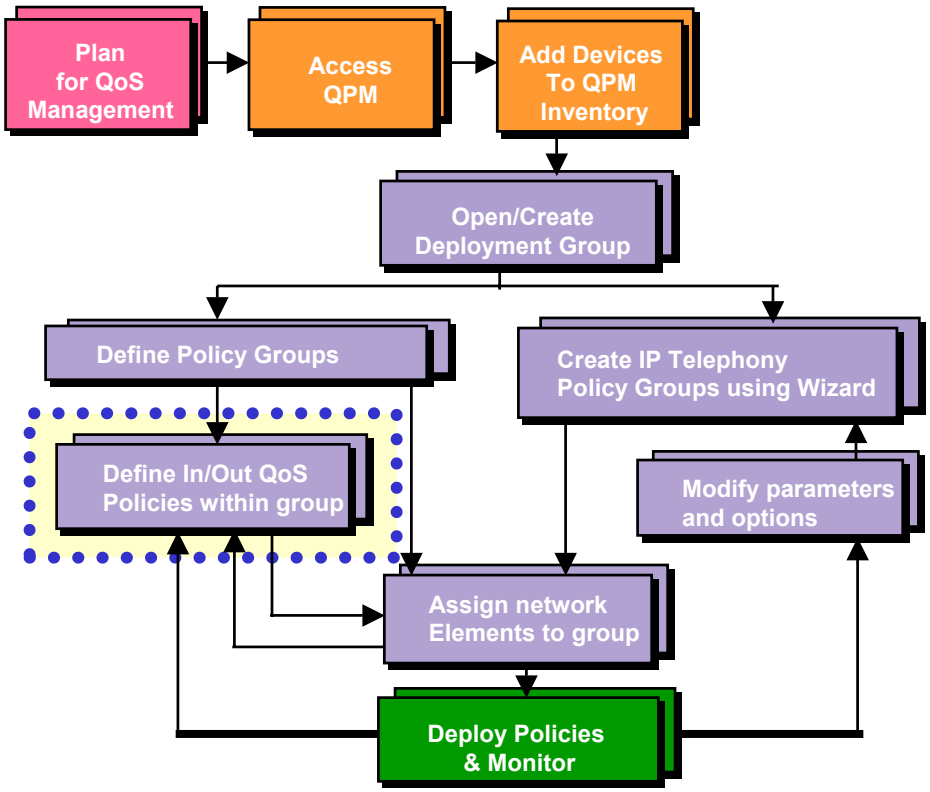
Click *Next* or *Finish* to view a Summary page for all QoS Properties defined for the policy group.

Refer to the QPM User Guide for additional details on each of the QoS Properties pages.

This page intentionally left blank.

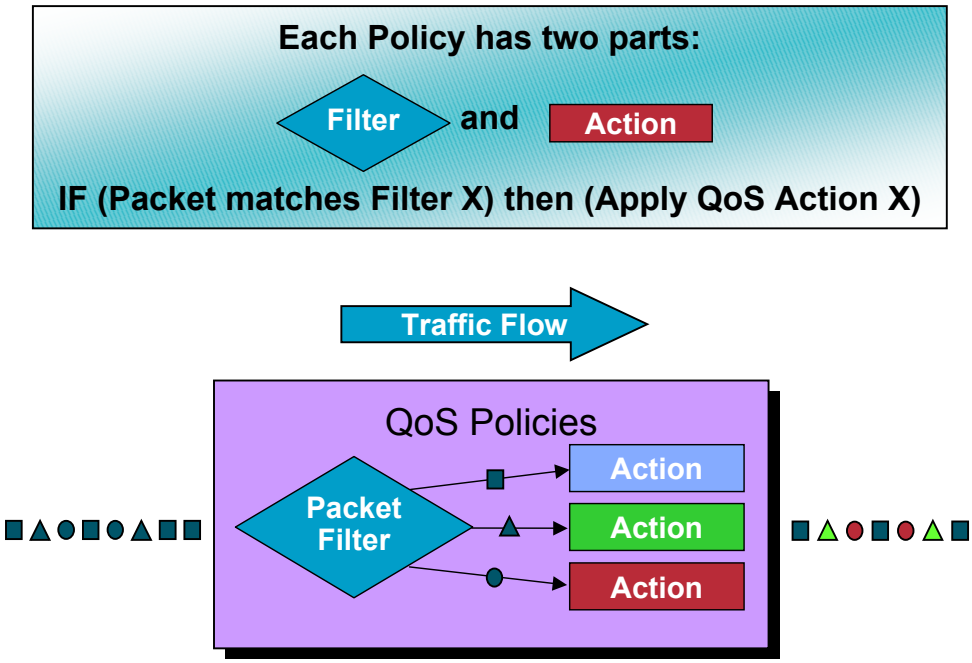
Roadmap

In/Out QoS Policies



Defining the In/Out Policies

Cisco.com



QPM v3.0

Defining the In/Out Policies

A QoS policy classifies a subset of traffic in which an action should be applied. The action in turn will have an affect on the handling (priority) of the classified traffic flow.

A policy can have two components:

- A Policy Filter - the conditions the packet must meet and
- A Policy Action - the QoS action applied to the above traffic.

For example, a policies can be thought of as Boolean logic expressions as shown in the following example:

IF (Source Port is FTP (20) AND Source is 192.9.200.18)

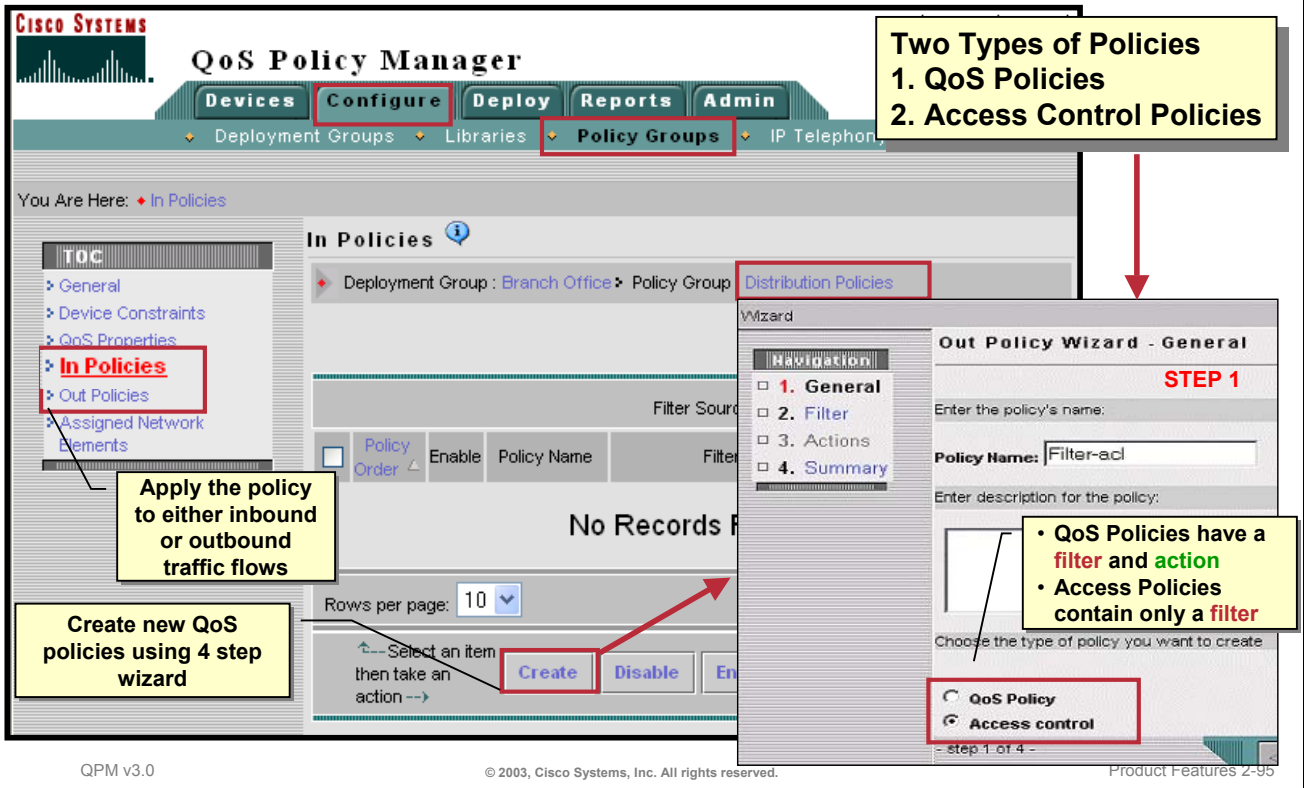
THEN limit rate to 200K bps

Some policies actually determine how the packet will be queued. Therefore, the QoS building blocks, QoS Properties and QoS policies, work together to give the traffic flow the desired level of service.

As you will see later when previewing the commands sent to the devices, policies are defined in the configuration file of a device using access control lists (ACLs). Packets are compared to each matching criteria in the list of policy expressions until a match is found, just like ACLs. Once a match is made, the action is executed and in most cases the packet is transmitted. This normal flow makes the order of the policy statements in the configuration file important. The exception to this is when using Committed Access Rate (CAR) which allows for further policy matching using a continue statement; allowing for finer granularity policies. (The ordering of policies is discussed later in this tutorial.)

Note that only certain actions are available for selected queuing algorithms on the interface and this is dependent upon the type of QoS property defined on the interface. QPM has the built in knowledge to ensure that only valid actions can be chosen based on the selected queuing algorithm assigned.

Defining the In/Out Policies
Types of Policies



Types of Policies

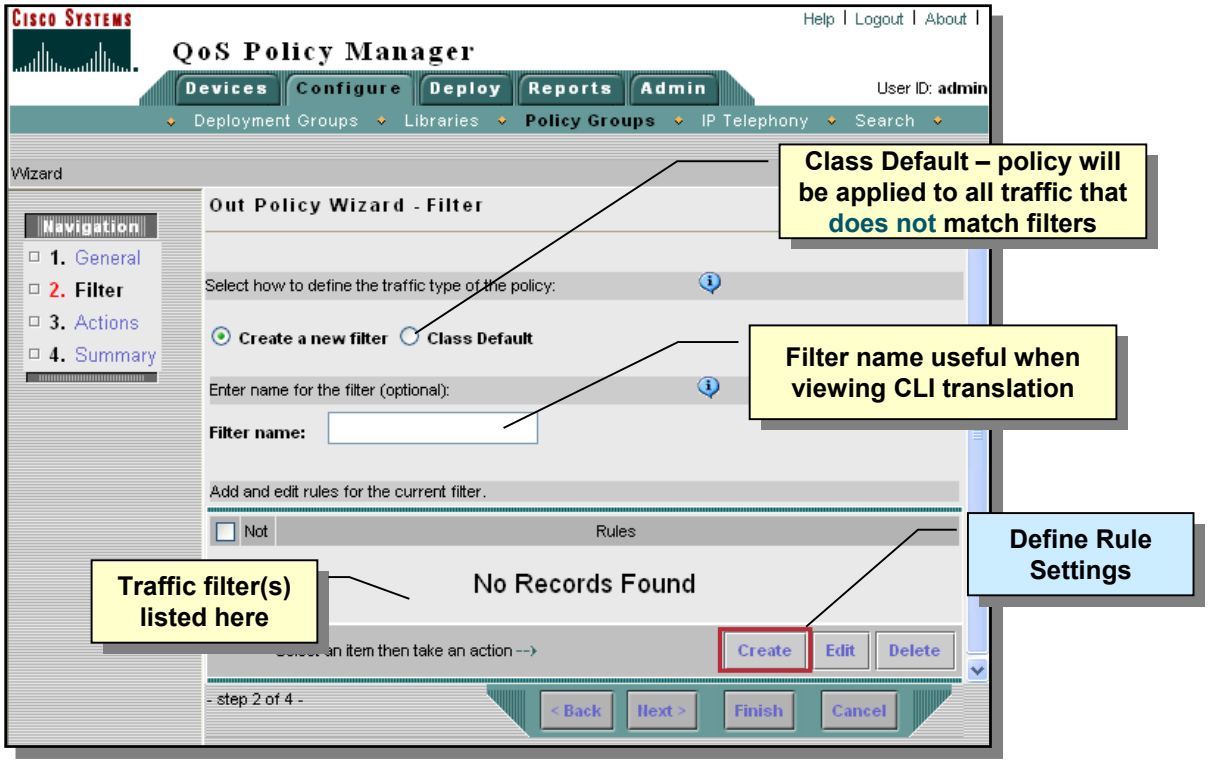
Now that the QoS Properties have been defined, the individual policies within the policy group can be added. If the policy is to be applied to the inbound traffic, select *In Policies*; for outbound traffic, select *Out Policies*. The In Policies or Out Policies page appears, displaying the inbound or outbound policies already defined.

To create (or modify) a new policy, select the Create (or Edit) button from this page. The 4-step Policy Wizard dialog appears. Using QPM, the user can create two 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 condition (filters) defined in the policy. The policy action could be packet coloring, limiting, etc.
- *Access Control Policies* - An access control policy permits or denies the flow of data if the data packet satisfies the conditions or filters defined in the policy. An access control policy does not have an associated QoS action. *Note that access control policies can not be created on Catalyst 5000 and Catalyst 6000 switches*.

Defining the In/Out Policies

Defining the Policy Filter



Defining the Policy Filter

The second step of the Policy Wizard allows the user to define a filter to specify the traffic to which the policy should be applied. From the Filter page, the user can define a new filter or define a Class Default filter. A Class Default filter is a “catch all other” traffic filter. Select the *Class Default* radio button option to match unclassified traffic or traffic that does not match any other filter condition. Class Default can be defined if the QoS Properties are either PQ or CBWFQ.

Also from this page, optionally specify a name for the filter. Providing a name is useful for when you are viewing the translation of the policies.

Initially, the policy contains no filters, as illustrated above by “*No Records Found*”. To define the filters, click *Create*. 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 defined in the Rule Settings window, illustrated next.

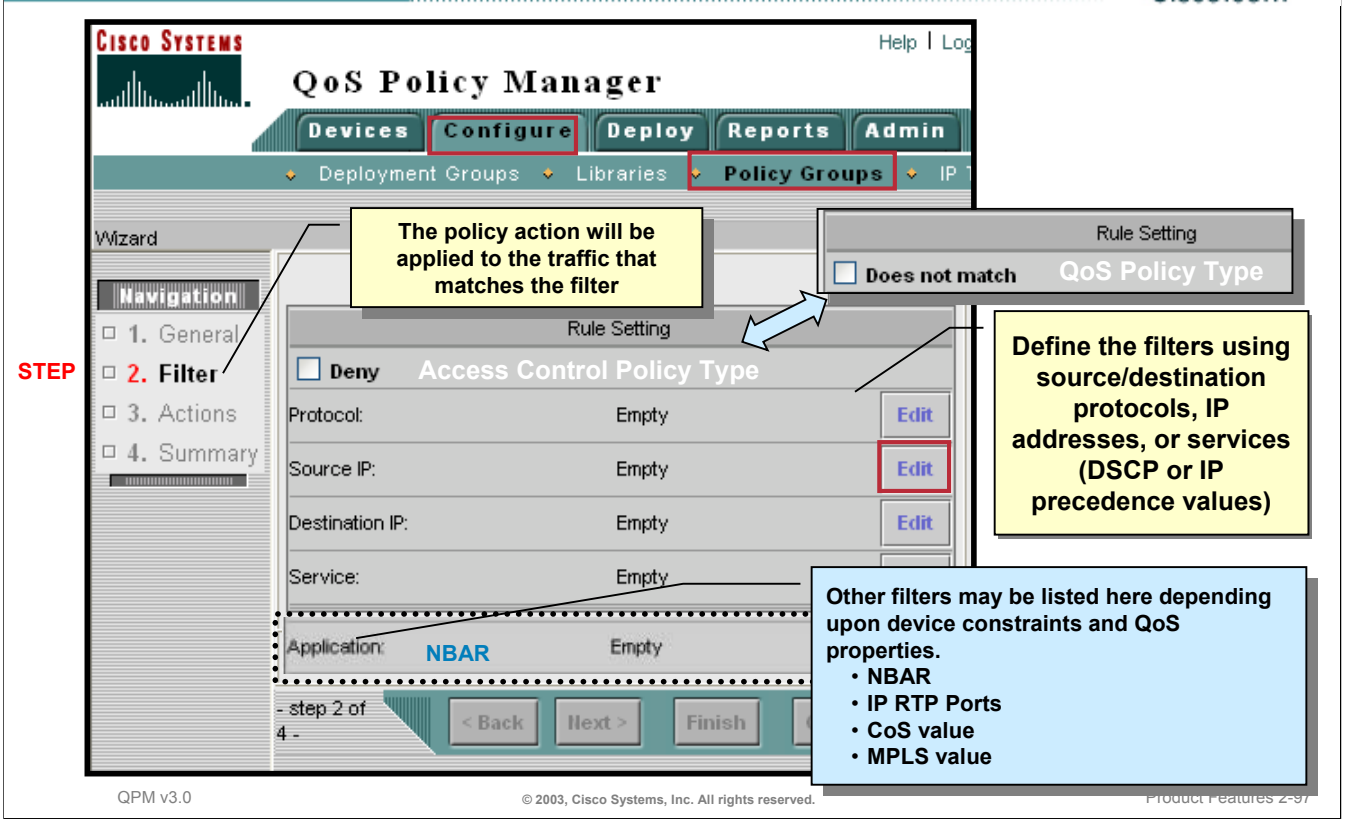
Note: To apply a policy to all traffic, do not define any filters.

Defining Policy Filters for QoS Monitoring

When using QoS policies to monitor traffic for baselining, set the policy filter to recognize the applications based on DSCP, IP precedence values, or other protocol information.

Defining the In/Out Policies

Defining the Policy Filter



Defining the Policy Filter

The Rule Settings window looks slightly different depending upon the type of policy selected (Access Control type or QoS type). Access Control policy types define Permit or Deny like statements based on extended ACLs. QoS policy types define inclusive or exclusive like statements based on the check box “Does not match” that applies an action defined later to the traffic that matches the rule (filter).

The available rule (filter) settings change according to the device constraints and congestion management QoS Properties defined for the policy group. Typically, the user can identify the traffic by any of the following characteristics:

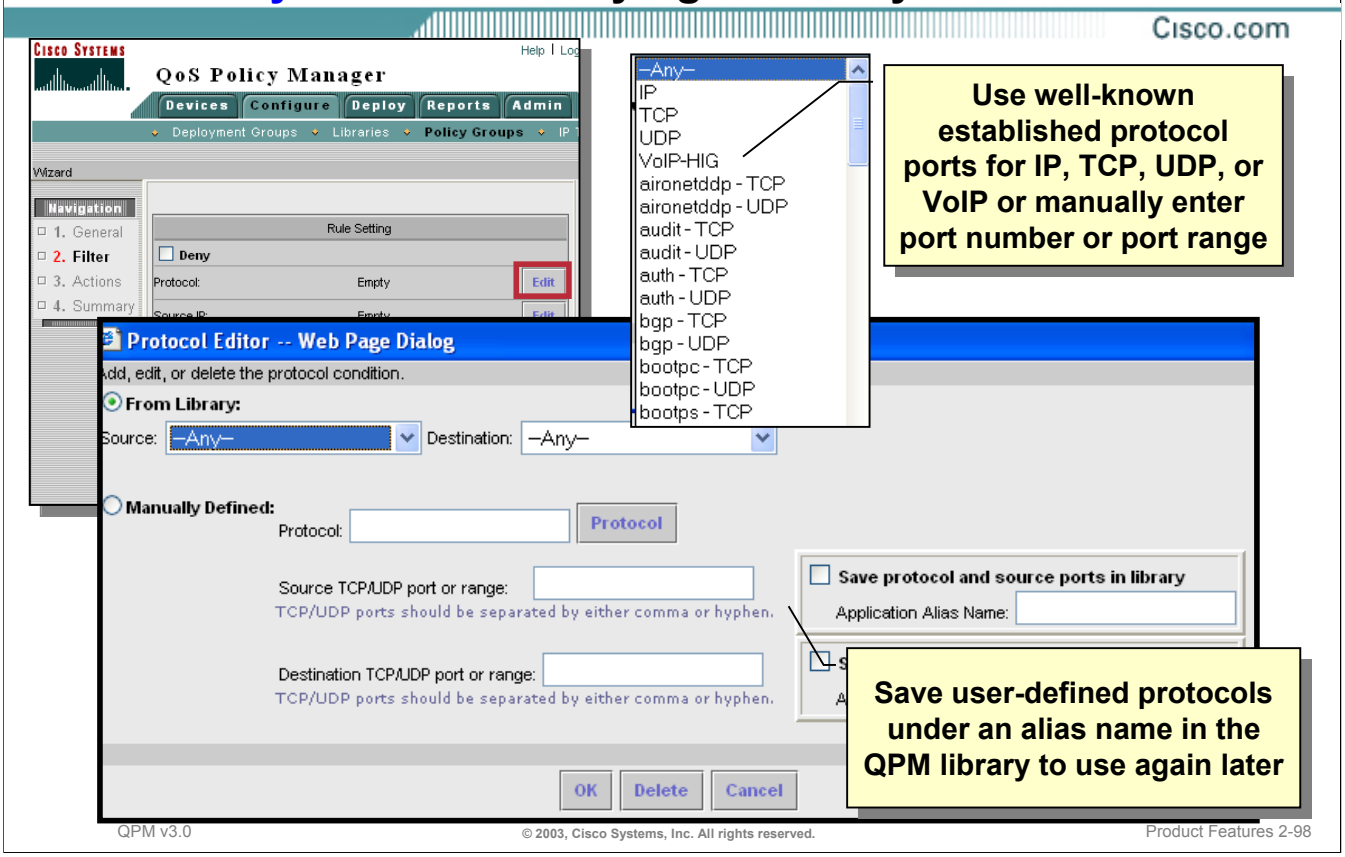
- Source IP or Destination IP address - IP aliases can be used and defined from the *Configure* > *Libraries* task bar or from the Rule Settings window.
- Source application or destination application protocol - Application aliases can be used and defined from the *Configure* > *Libraries* task bar or from the Rule Settings window.
- Service – an IP precedence or DSCP value.

Depending upon the QoS Properties and device constraints already defined for the policy group, the user 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. This is available for device types that support modular CLI and Class Based WFQ (CBWFQ) properties.
- IP RTP ports - Available for device types that support modular CLI and CBWFQ properties.
- CoS value
- MPLS value

Defining the In/Out Policies

The Policy Filter – Classifying Traffic by Protocol



The Policy Filter - Classifying Traffic by Protocol

To construct a policy filter based on the source and/or destination application protocol, select the *Edit* button in the *Protocol* row on the Rule Setting page.

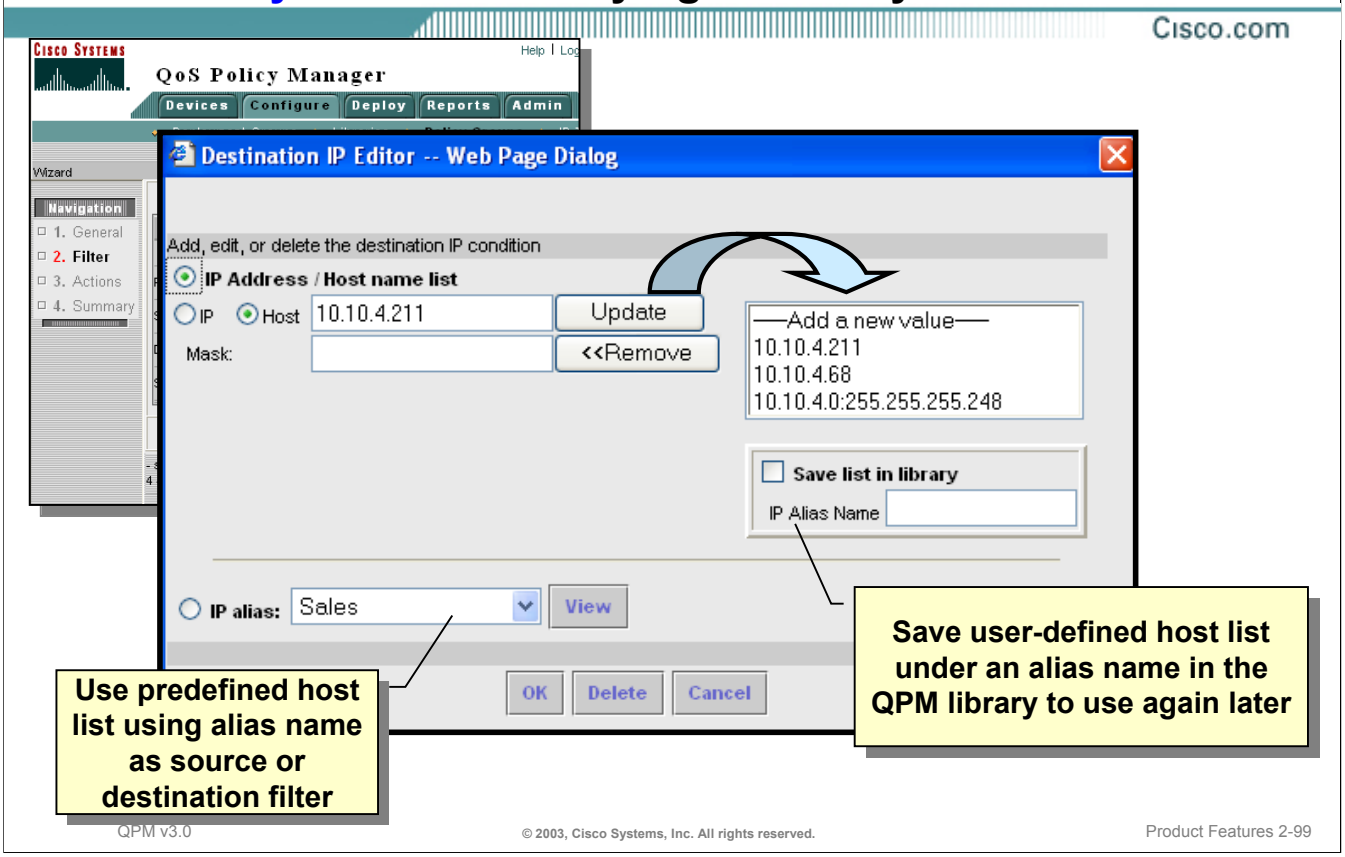
The application protocol can be manually defined by specifying the TCP or UDP protocol type and the source and/or destination TCP/UDP port number or range. If manually specified, the user can then save the definition in the QPM library for use later by providing an application alias name.

Alternatively, the user could select the application protocol from a list of well-known protocol ports or from an application alias already defined in the QPM library.

Tip: For a complete list of protocols and their port numbers, see the URL:
http://www.iana.org/assignments/port-numbers

Defining the In/Out Policies

The Policy Filter – Classifying Traffic by IP Address



The Policy Filter - Classifying Traffic by IP Address

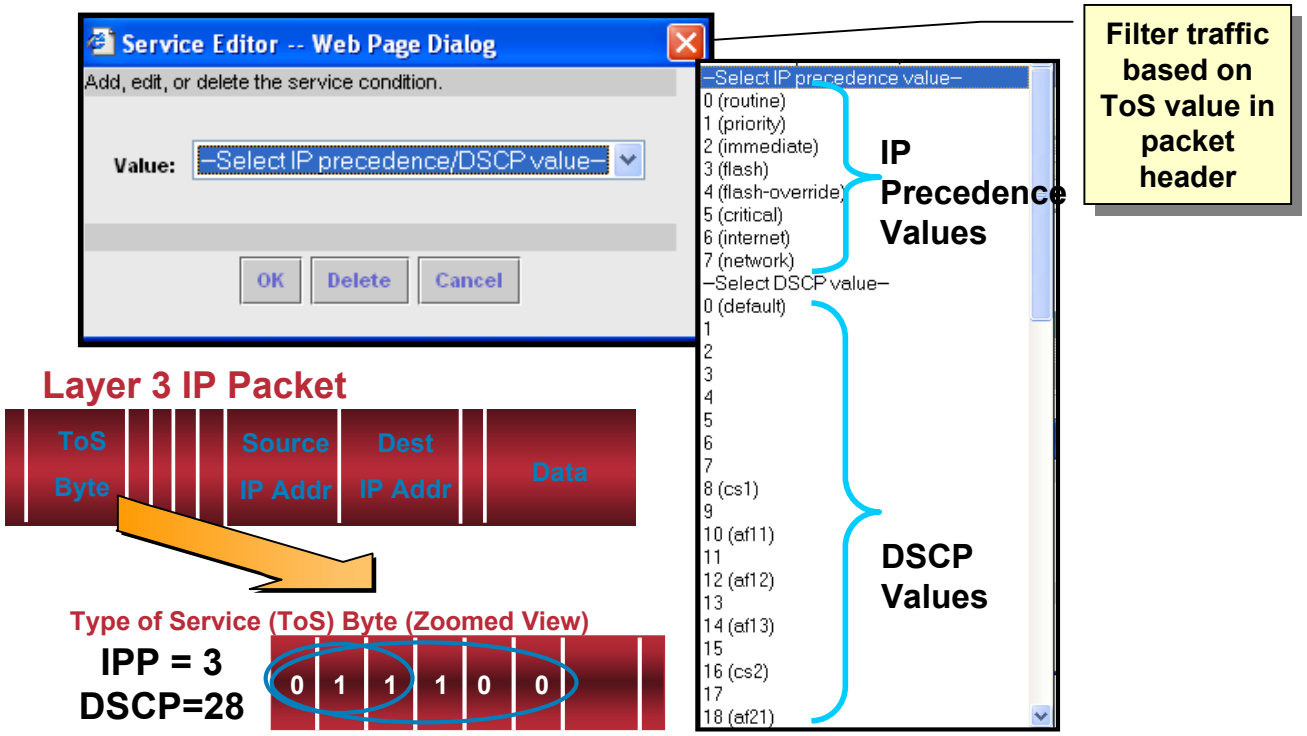
To construct a policy filter based on the source and/or destination IP address, select the *Edit* button in the *Source IP* or *Destination IP* row on the Rule Setting page.

The IP Address or Host Name can be manually defined. A subnet range can be manually defined by using the Mask field. If manually specified, the user can then save the definition in the QPM library for use later by providing an IP alias name.

Alternatively, the user could select the IP address or subnet range from an IP alias already defined in the QPM library.

Defining the In/Out Policies

The Policy Filter – Classifying Traffic by Service



The Policy Filter - Classifying Traffic by Service

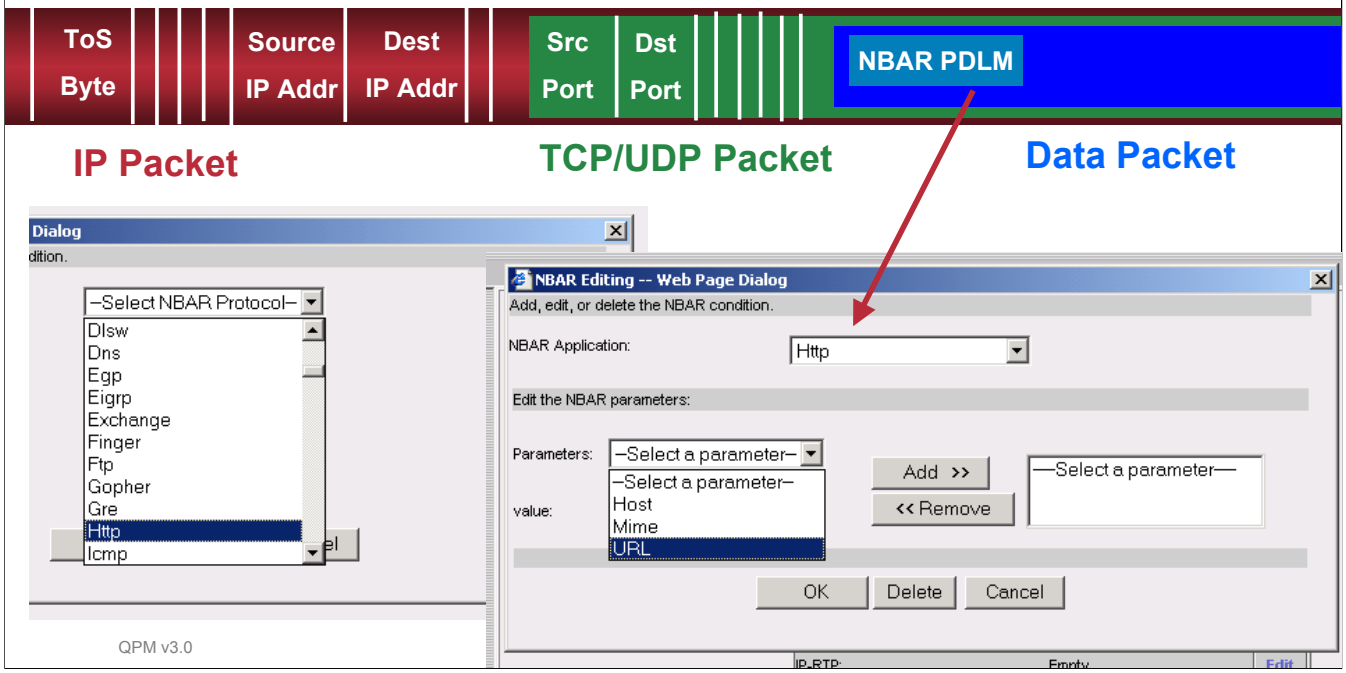
To construct a policy filter based on the type of service (ToS) defined in the header of a packet, select the *Edit* button in the *Service* row on the Rule Setting page. Using the pull-down menu, select from a list of IP precedence (IPP) values or DSCP values. IPP utilizes the first three bits of the ToS field in the packet header, providing values between 0-7, where as DSCP utilizes the first 6 bits of the ToS field, providing values between 0-63.

Defining the In/Out Policies

The Policy Filter – Classifying Traffic by Application (NBAR)

Cisco.com

NBAR configuration is done via simple dialogs and pop-up menus which are sensitive to the protocol type and its required arguments

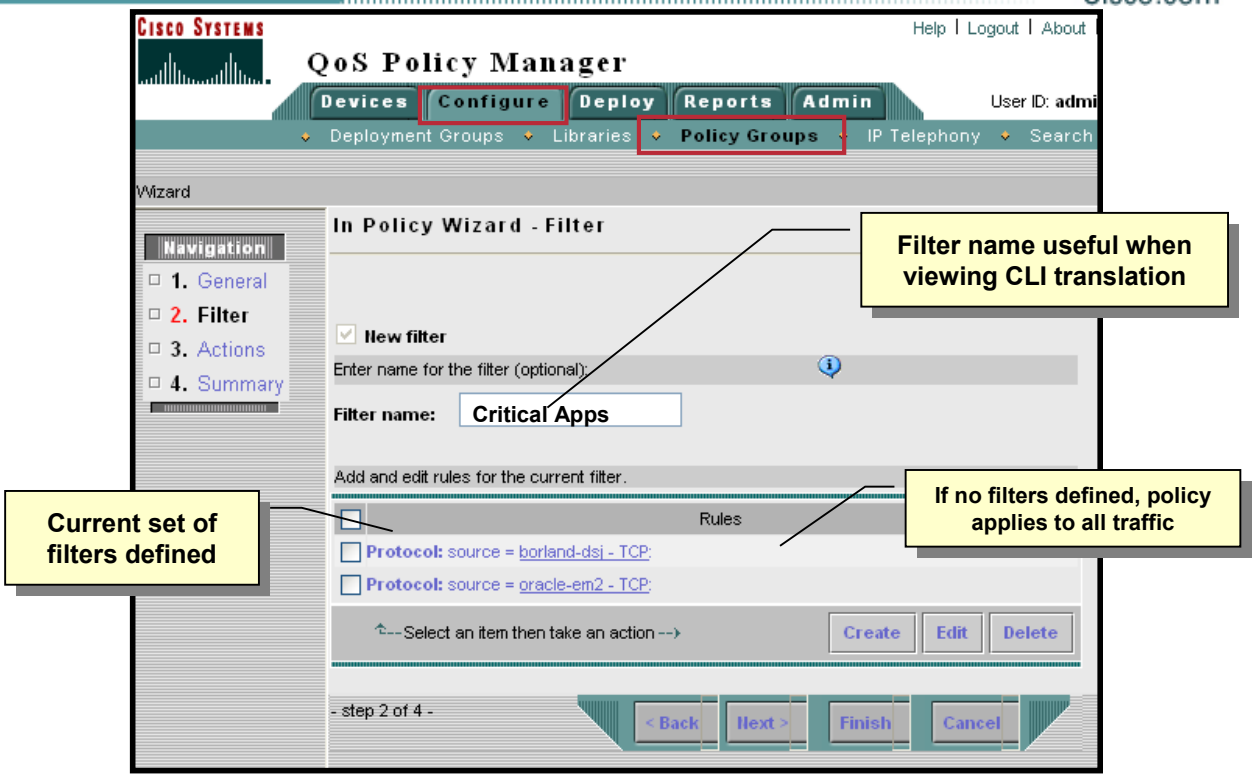


The Policy Filter - Classifying Traffic by Service

To construct a policy filter based on the type of service (ToS) defined in the header of a packet, select the *Edit* button in the *Service* row on the Rule Setting page. Using the pull-down menu, select from a list of IP precedence (IPP) values or DSCP values. IPP utilizes the first three bits of the ToS field in the packet header, providing values between 0-7, where as DSCP utilizes the first 6 bits of the ToS field, providing values between 0-63.

Defining the In/Out Policies

The Policy Filters Defined



The Policy Filters Defined

After a policy filter has been defined, it is listed under the Rules heading in the Filters Navigation window. To create additional filters, click the *Create* button. To modify/edit or delete a filter, check the box next to the filter and click the appropriate button.

Tip: Remember by providing a filter name, it helps the user identify the defined filter in the CLI translation.

After completing the filter definitions, click *Next*. If defining a QoS policy, the Policy Wizard - Actions page appears. If defining an Access Control policy, the Summary page appears.

Defining the In/Out Policies

The Policy Actions (QoS Policies Only)

Cisco.com

Marking
- Setting the IP Precedence or DSCP bits
- Select how to Trust the markings
- Setting Discard Eligibility bit for Frame Relay

Microflow Policing (Limiting on Switches)
- Limit and mark traffic that conforms to or exceeds specified rates

Policing (Limiting on Routers outbound interfaces)

Shaping (Generic, Distributed, Frame Relay Traffic Shaping)

Queuing

Congestion Avoidance
- Tail Drop
- WRED (refer to mappings defined in QoS Properties)

Actions depend upon QoS Properties and Device Constraints:

- **Class-Based QoS ...**
  - **Able to define multiple actions in a single policy**
- **All others ...**
  - **Define only a single action; all others are disabled**

The Policy Actions

The Policy Actions wizard helps to define the actions to be applied to traffic that matches the filter definition just defined. Note that not all of the actions may be available for selection; it will depend upon the device constraints and QoS properties of the policy group. The user can check the *Capabilities Report* for the Policy Group to determine which actions may be allowed.

Defining Policy Actions for QoS Monitoring

When using policies to monitor traffic for baselining, set the policy filter to recognize the application, and the policy action to take no action. QPM can monitor traffic based on the QoS policies that have been distributed to network interfaces using QPM. (Note that if the policy was not distributed by QPM, upload the policy to QPM and redeploy.)

The following QoS settings are ideal for baselining traffic and ensures that all traffic is transmitted without the policies affecting the traffic:

- QoS action: Policing.
- Set rate, burst rate, and exceed burst rate to 8; do not configure an excess rate.
- Set conformed, exceeded, and violated actions to *transmit*

Possible Policy Actions

- Marking—Defines a packet's relative importance, such as setting the IPP or DSCP bits in layer 3 of the packet header, the Trust level, and the Discard Eligibility bit in a frame relay packet. The markings can be used to identify and prioritize packets in subsequent policies, thus changing the packet's relative importance. Note: On Catalyst 6000 switches, the user also has the option of coloring by trust. In this way, you can choose to trust the IP precedence, CoS, or DSCP settings on packets that meet the policy's filter, while having different trust settings for other packets on the port.

  Note: Some versions of device software support complex coloring policies using committed access rate (CAR) classification. If creating a coloring policy on an interface that supports it, the user can define a complex marking action, rather than filling in the IPP or DSCP field.

The Policy Actions - continue

- Microflow Policing - Limits the input transmission rate of traffic, and marks packets. Limiting the bandwidth available for individual or aggregate flows is available on all Catalyst 6000 switches. The user can choose whether to limit per flow (Microflow), per device (aggregate) or across several interfaces in a device group (cross-interface). In addition, the user can specify that packets that match the filter but that exceed their designated rate are marked down, according to a pre-defined markdown table. In this way, the user can apply different markdown values for packets with different IP precedence or DSCP values, rather than applying a fixed markdown value for all traffic that meets the filter conditions. Refer to the on-line help for more information on setting the limiting parameters for Catalyst 6000 switches.
- Policing -Limits the rate of aggregate flows on a single interface or across interfaces. Limiting the bandwidth available to the traffic on routers is performed using committed access rate (CAR) limiting. CAR can be applied on the inbound, outbound, or both interfaces.
- Shaping – Shaping smoothes the flow of *outbound* traffic by limiting traffic. QPM generally uses Generic Traffic Shaping (GTS). On VIP interfaces, Distributed Traffic Shaping (dTS) is used. (On Frame Relay interfaces, the user can define Frame Relay Traffic Shaping as a QoS property.) Shaping policies buffer traffic flows to even out the transmission rate. Packets are not dropped until the buffer limits are reached. Incoming traffic flows can not be shaped.
- Queuing—Provides bandwidth guarantees and priority servicing for *outbound* traffic. Depending upon the type of QoS property defined for the interface (Priority Queuing, Custom Queuing, Class based QoS), the policy's queuing actions will vary.

  If the QoS Property for the interface was set to Priority Queuing, the policy action Priority will appear in the navigation window. It was when the QoS Property was set to Priority Queuing that the queue lengths were defined. Here we are defining the policy action. In other words, if a packet matches the filter condition, the packet will be placed in the selected queue (High, Medium, Normal, or Low).

  If the QoS Property for the interface was set to Custom Queuing, the policy action Custom Queue will appear in the navigation window. Packets that match the defined policy filter can allocate at least the specified amount of bandwidth. The ratio value must be in increments of 5, and the total allocation for all custom queue policies on the interface or device group must not exceed 95%. The remaining 5% is used for unfiltered traffic.

  If the QoS Property for the interface was set to Class-based QoS, the policy action CBWFQ will appear in the navigation window. CBWFQ combines the best characteristics of weighted fair queuing and custom queuing. CBWFQ lets you control the drop mechanism used for the packets that match the filter 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 IP precedence is not equal. In addition, packets that match the filter condition, can be allocated a percentage of the interface's bandwidth to the traffic flow. And finally, the Priority checkbox can be used to place the filtered traffic that is delay-sensitive, into a strict priority queue.
- Congestion Avoidance—Discards packets to avoid congestion using either Tail Drop or WRED algorithm.

QPM uses the command line interface (CLI) or modular CLI (also known as MQC) to implement QoS policies, depending on the device constraints and QoS properties. Policies implemented with modular CLI can contain multiple actions (Class-based QoS). In other cases, only one policy actions can be defined, all other actions are disabled in the wizard.

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.

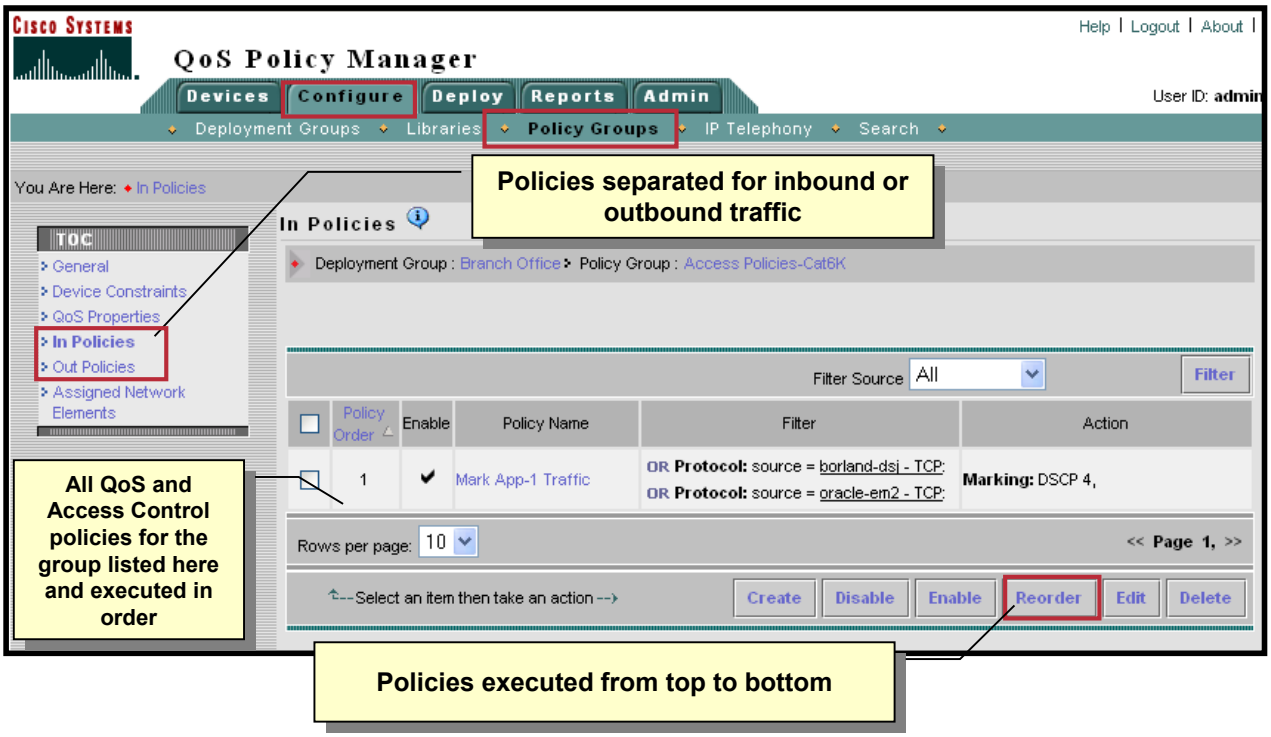
Defining the In/Out Policies
Policy Summary

Policy Summary

For completeness, after the filters and actions (if any) have been defined for the policy, review the policy definitions in the Summary page. The user can go back and revise definitions before completing the Policy Definition wizard.

Click *Finish* to complete the policy definition and then view all the policies defined for the entire policy group.

Defining the In/Out Policies
The Policies Defined

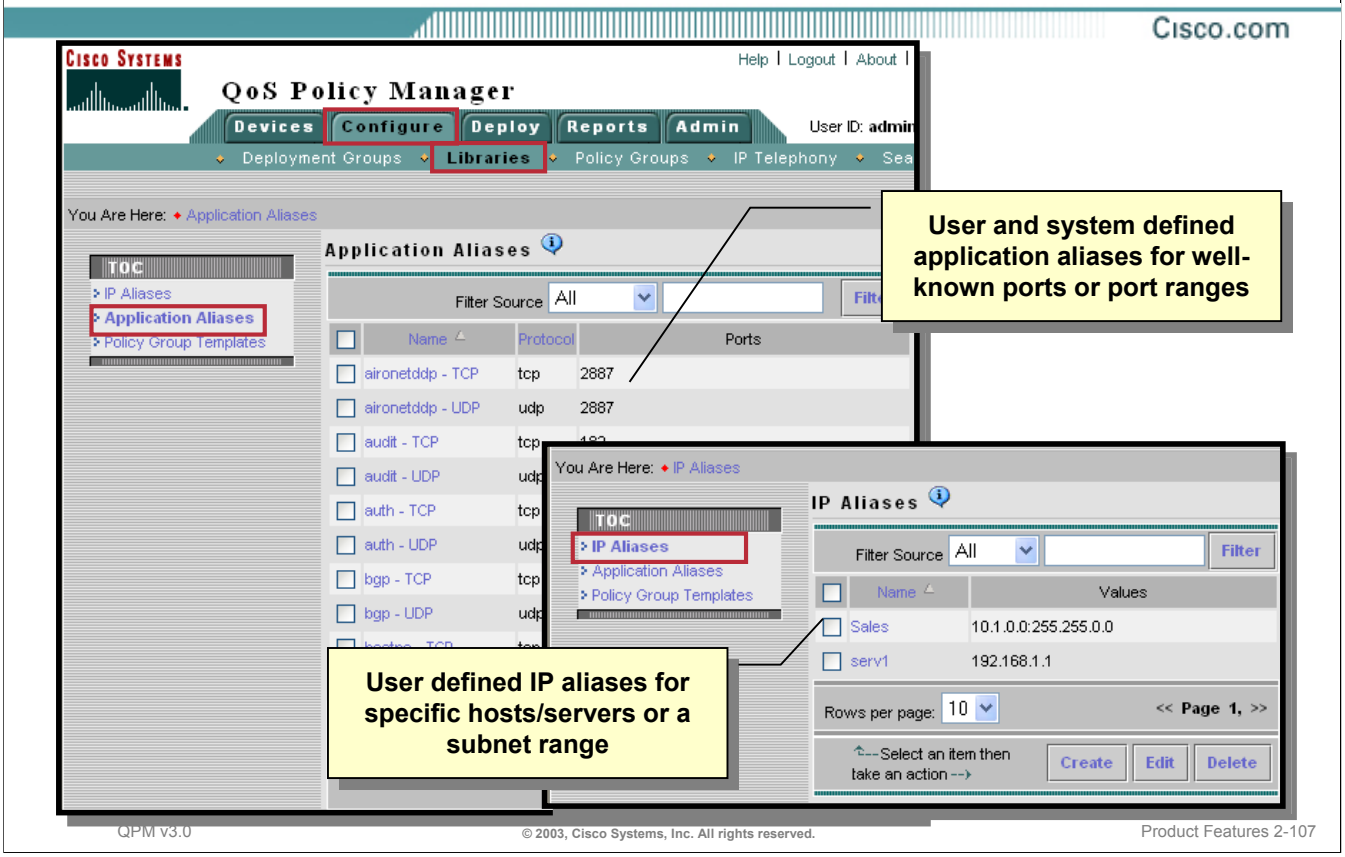


The Policies Defined

The individual policies within the policy group can be view, edited, disabled, enabled or deleted by displaying the In Policies or Out Policies page from the TOC navigation window.

Remember, if there is more than one policy defined, the device looks at the policies in order, until the first match is found, at which point it applies the policy and ignores remaining policies. When the device is configured with the policies, it scans policies in order, (illustrated top to bottom in QPM), and applies the first matching policy. However, for certain policies, a *Continue* statement is provided so that subsequent policies are examined after the previous policy is applied. For example, if you create a limiting policy that should also apply to the selected traffic, the limiting policy must appear after the coloring policy (or alternately, the limiting policy must also use Continue). (This example is reflected in the scenarios in Chapter 3.)

Defining the In/Out Policies
More on Aliases



More on Aliases

When defining the policy filters, the user may have manually defined IP address or application aliases. These aliases, as well as system defined aliases for well-known application protocols, can be viewed, edited, or deleted by selecting *Configure* > *Libraries* and selecting *IP Aliases* or *Application Aliases* from the TOC navigation menu.

Aliases can be used in policy definitions across all deployment groups. When the alias definition is changed, all policies that reference the definition are affected.

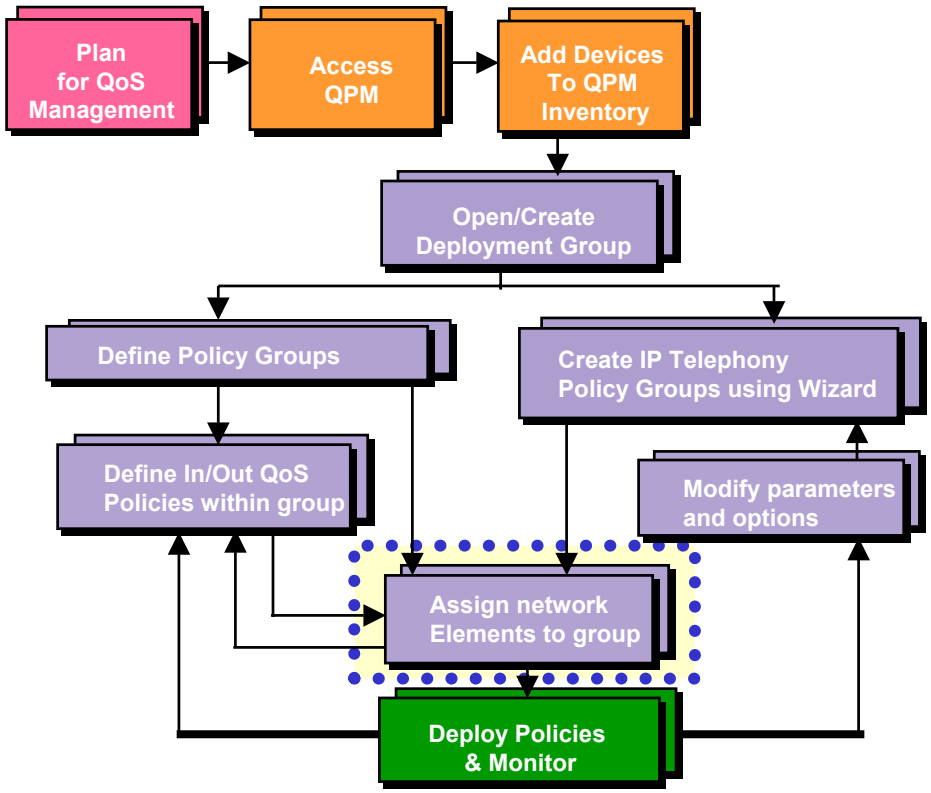
Also, if redeploying a historical job, QPM validates all alias definitions and their references before proceeding with the job.

Tip: For a complete list of application protocols and their port numbers, see the URL: **http://www.iana.org/assignments/port-numbers**

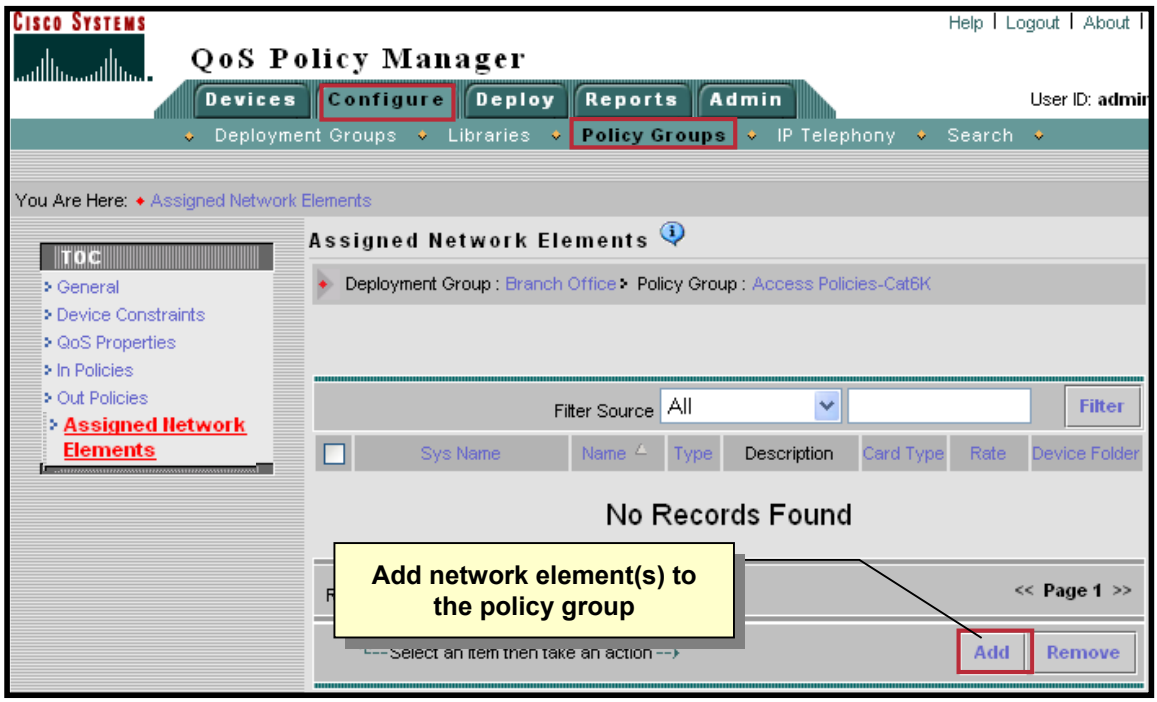
This page intentionally left blank.

Roadmap

Assign Network Elements



Assigning Network Elements



Assigning Network Elements

First, what is a Network Element? Policies are applied to network elements. QPM supports both physical and logical network elements. A physical network element physically exists on a device and can be read or accessed using SNMP and Telnet. Examples include device, interface, sub-interface, VLAN, DLCI, and VC. A logical network element is one that does not exist on a device, and its purpose is helping the user manage their network elements. An example is source-destination pairs.

After a policy group is created, and its device constraints and QoS Properties are defined, the user can either defined the individual policies for the group or assign network elements to the group and then define the individual policies. QPM will allow only those network elements in the device group that match the policy group's device constraint definitions.

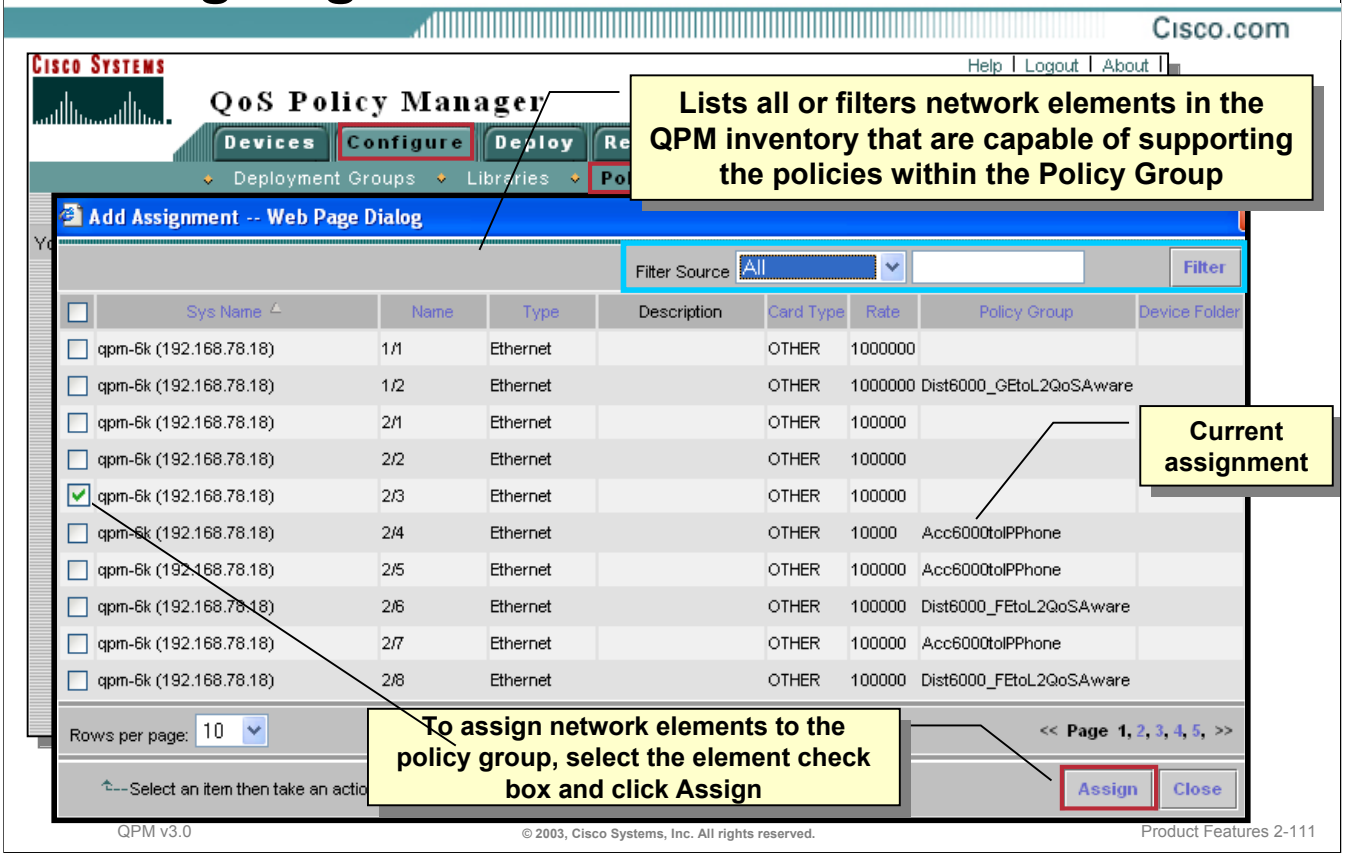
Once the network elements have been assigned to the group, the user can change the assignment or remove the network element assignments. When network elements are reassigned, QPM automatically removes the previous assignment and saves the new assignment.

Assigning network elements to policies can be performed from one of two areas:

- From the *Configure>Policy Group>Assigned Network Elements* page, illustrated above and on the next few pages
- Or from the *Devices>Manage>Device Table*, illustrated later

The Assigned Network Elements page displays the network elements that have already been assigned to the opened policy group. Initially, the policy group contains no network element assignments, as illustrated above by "*No Records Found*". To assign network elements to the policy group, click *Add*.

Assigning Network Elements



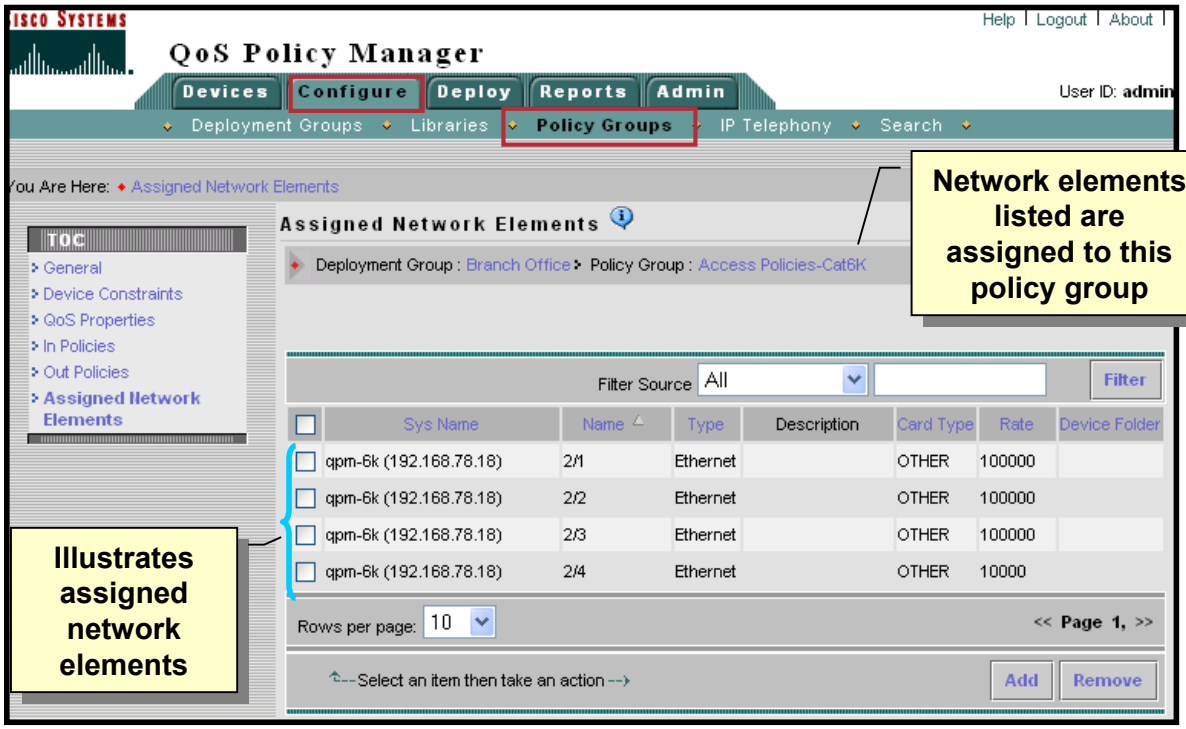
Assigning Network Elements

After selecting the *Add* button from the *Configure* > *Policy Groups* > *Assigned Network Elements* page, (this TOC appears only after you have opened a policy group page), a separate Add Assignment window appears. This window illustrates the network elements in the current device group that match the device constraints defined for the policy group. For example, if the device constraint is Ethernet interfaces, then only Ethernet interfaces on devices within the device group are displayed and are available for assignment.

The list of network elements within the device group that match the device constraints for the policy group could be large. If so, the user could filter the network elements by selecting a field (e.g. SysName, Type, Rate, etc.), enter a string to match, and then click the *Filter* button.

To assign the desired network elements to the opened policy group, check the box for the row containing the network element and then click *Assign*. The Assigned Network Elements page reappears, displaying all the network elements assigned to the policy group (refer to next illustration).

Assigning Network Elements

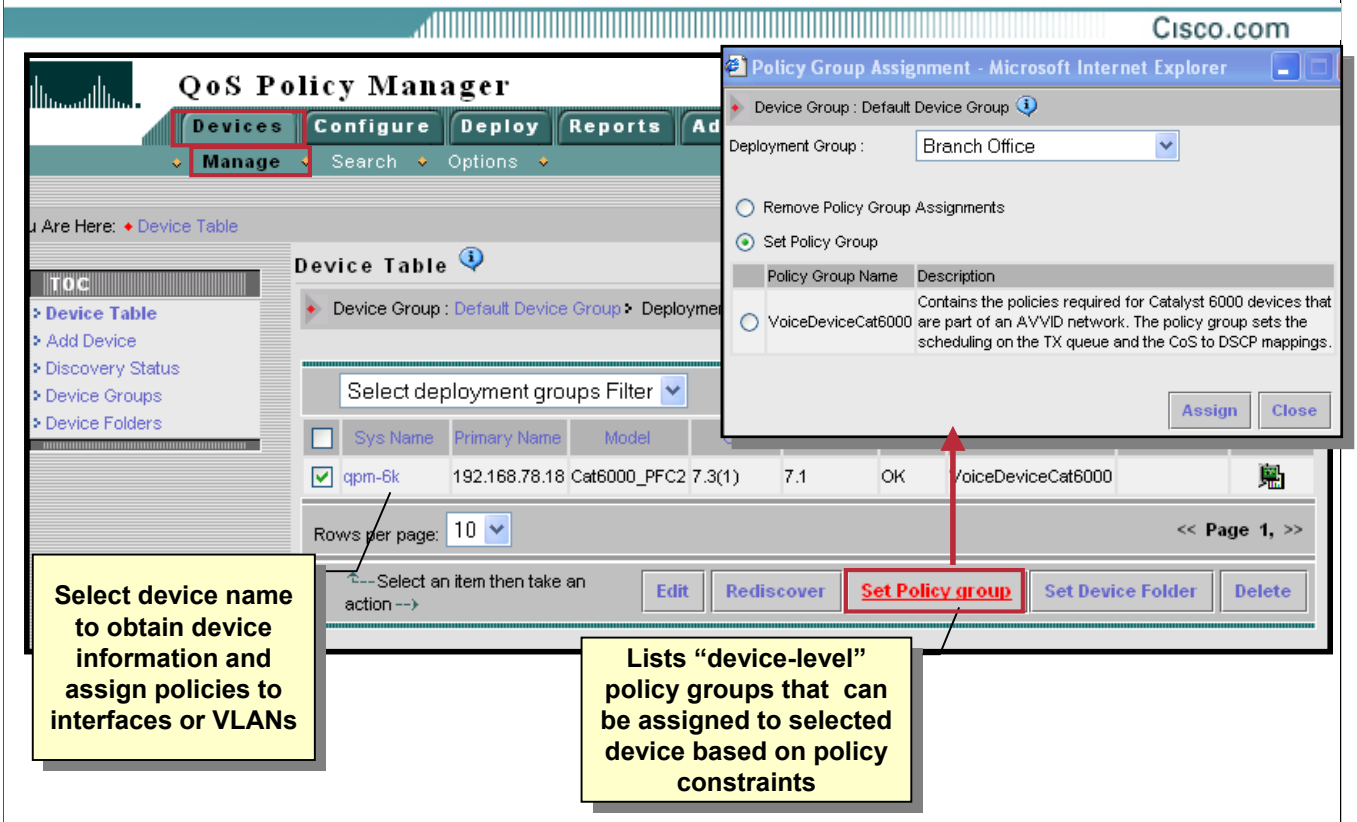


Assigning Network Elements

The Assigned Network Elements page illustrates all network elements currently assigned to the opened policy group. To remove network elements from the policy group assignment, select the assigned network elements in the Assigned Network Elements page, and click *Remove*.

The fields that appear in the Assigned Network Elements page depend on the type of assigned device or network element. Refer to on-line help within QPM for a brief description of the fields illustrated.

Assigning Network Elements
Alternative Method – Device Level Policies



Assigning Network Elements – Alternative Method

Network Elements can also be assigned to policy groups directly from the Device Table. Note that there are four types of network elements that can be assigned to policy groups:

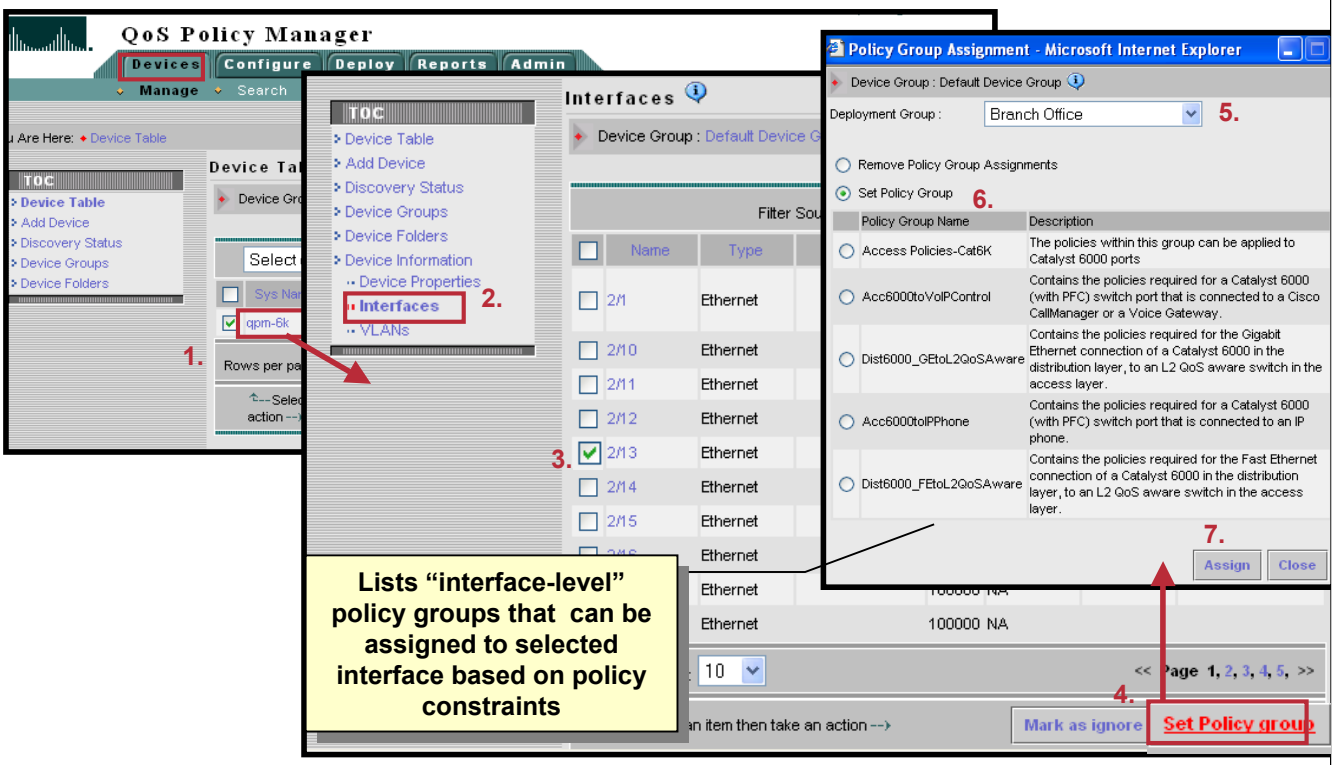
- Devices (illustrated above)
- Interfaces
- Interface sub-elements (e.g. VCs and DLCIs)
- Logical or user-supplied elements (VLANs and source-destination pairs)

The dialog window above can be used to assign, change, or remove *Devices* from a policy group. To get to this dialog window, select *Devices* > *Manage*. From the Device Table page that appears, select the check box next to the devices to add to or remove device from a policy group that supports device network elements, then click *Set Policy Group*.

QPM then displays a dialog window that lists the policy group names that could be assigned to the device based on the device constraints for the policy groups. From this window, the device could be assigned, reassigned, or removed from a policy group.

Tip: To remove a QoS configuration from a device, create an empty policy group, then reassign the device to this policy group and deploy the policy group.

Assigning Network Elements
Alternative Method – Interface/VLAN Level Policies



Assigning Network Elements – Alternative Method continue …

The previous page illustrated how to assign *device* network elements to policy groups. The following procedure describes how to assign, change or remove interfaces, interface sub-elements, and logical or user-supplied network elements from policy groups.

1. From the Device Table page, click on the device name to reveal the Interface selection in the TOC or alternatively, click the *Interfaces* icon in the table row of a device that contains the network element or elements that you want to assign. In either case, the Interfaces page appears.
2. To 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 to assign to or remove from a policy group, then click *Set Policy Group*. The Policy Group Assignment dialog box opens.
    b) The available Policy Groups that can be assigned to or removed from the selected interface are illustrated and based upon the device constraints defined for the policy group.
3. To assign, remove, or change sub-elements (e.g. Virtual Circuits or DLCIs) of an interface to a Policy Groups:
    a) From the Interface Properties page, Select any sub-element 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.
    b) The available Policy Groups that can be assigned to or removed from the selected sub-elements are illustrated and based upon the device constraints defined for the policy group.

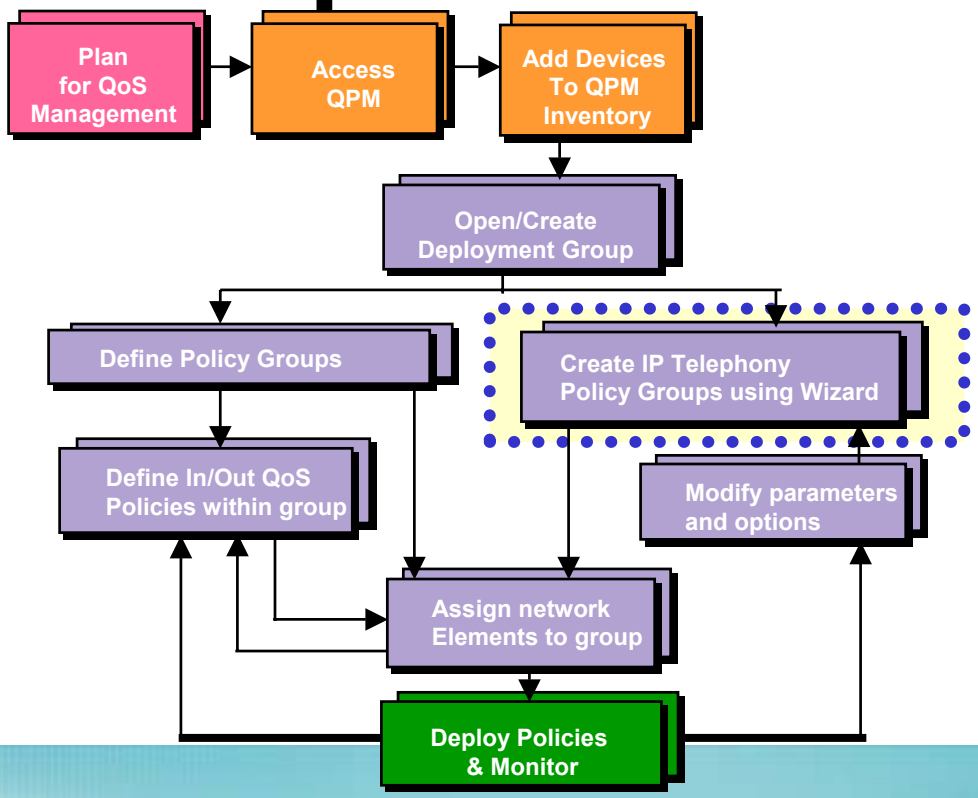
Assigning Network Elements – Alternative Method continue …

4. To assign, remove, or 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 to assign, then click *Set Policy Group*. The Policy Group Assignment dialog box opens.
    c) The available Policy Groups that can be assigned to or removed from the selected source-destination pairs or VLANs are illustrated and based upon the device constraints defined for the policy group.

This page intentionally left blank.

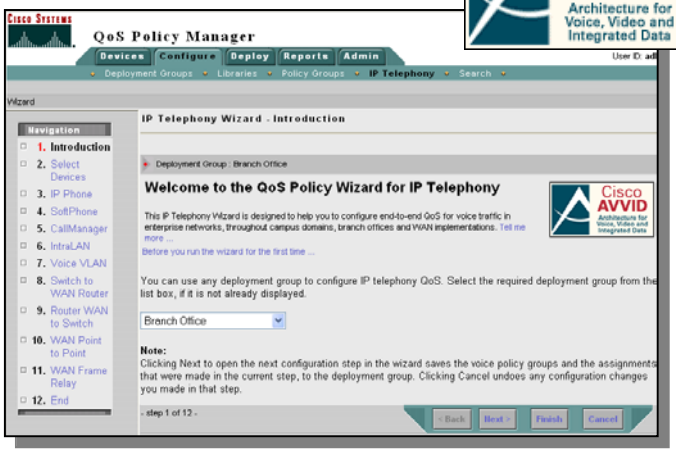
Roadmap

Create IP Telephony Policy Groups



QPM Support for IP Telephony

- **End-to-end QoS for IP Telephony**
- **Automated Wizard**
- **Use predefined QoS IP Telephony templates**
  - **Follows the AVVID recommendations**
  - **Customize templates**



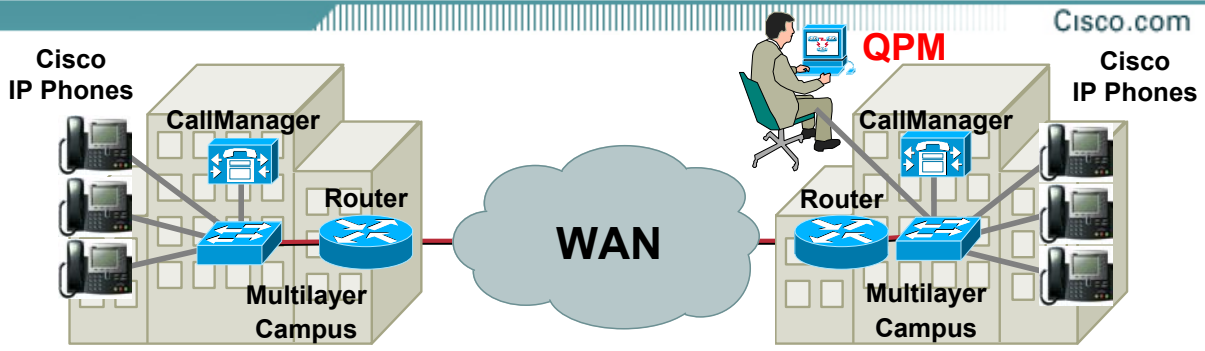
QPM Support for IP Telephony

Using a 12 step wizard, QPM will guide the user through all the steps required to configure QoS for IP Telephony end-to-end. From the access switch connecting IP phones to the core device, QPM will identify the network points (device interfaces) where QoS needs to be configured for IP telephony, and then, select and assign the appropriate QoS policies for each interface on the voice path.

QPM provides predefined QoS policy groups for the various network points along the voice path. These policy groups are templates that are stored in the QPM templates library and can be used “as-is” or customized.

Note: The QoS policies and properties are defined according to the Cisco IP Telephony Design Guide recommendations. (Refer to Chapter 5 to locate this document on-line.)

QPM Support for IP Telephony



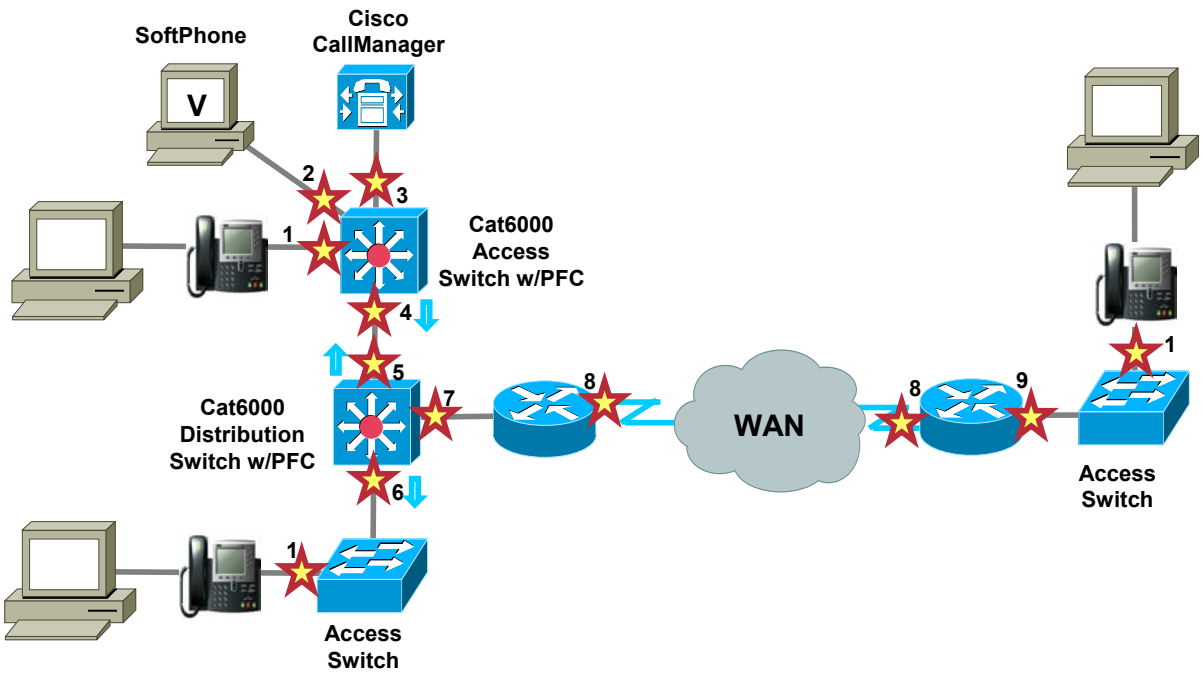
Identify traffic flows	Establish/mark service classes	Enforce	
• Subnet / IP address • UDP port range • IP ToS marking • Trust settings • RSVP policy control • VLAN • RTP payload type	Voice → Gold	• CBWFQ • LLQ • IP RTP Priority • RSVP for campus and WAN devices • Cat 6K 1P2Q2T	• CRTP • Link Fragmentation and Interleaving (LFI) • Enhanced FRTS with FRF.12 & FR Fair queue & FR Voice bandwidth

QPM Support for IP Telephony

The illustration above reflects the ways in which QPM identifies voice traffic (i.e. by IP addresses, port ranges, IP header type of service (ToS) bits, VLAN, etc.). Once the QoS policy has identified the traffic through the policy filters, the policy actions marks the packets for the appropriate service class. Then at each device interface, along the voice path, various QoS mechanisms can be enforced to provide adequate response time through the network.

QPM Support for IP Telephony
Identifying QoS Network Points

Cisco.com



Identifying QoS Network Points

Using the sample network above, the important network points that require QoS configuration statements are highlighted and described below.

1. Incoming voice traffic coming from an IP phone into an access switch
2. Incoming voice traffic coming from a SoftPhone into an access switch
3. Incoming voice control traffic coming from a Cisco CallManager server into an access switch
4. Uplink traffic coming from a Layer 3 QoS aware access switch (with PFC) going to a distribution switch (with PFC)
5. Downlink traffic coming from a Layer 3 QoS aware distribution switch (with PFC) going to an access switch (with PFC)
6. Downlink traffic coming from a Layer 3 QoS aware distribution switch (with PFC) going to an layer 2 access switch (with PFC)
7. Distribution switch outbound traffic to WAN router
8. WAN interface
9. Branch WAN router to Layer 2 access switch

QoS policy group templates (configuration settings) exist in the QPM library for each of these network points. The templates can be used “as-is” or customized to suit the network environment. All that the user needs 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.

Shortly, we will discuss how to manually set a *device role* to define the network point for a device.

Create IP Telephony Policy Groups
Getting Started

Getting Started

To launch the QoS Policy Wizard for IP Telephony networks, simply select *Configure* > *IP Telephony*.

Before using the wizard, however, verify the following prerequisites:

- All devices in the network have been added or imported into the QPM inventory. If the IP Telephony wizard is opened before the devices have been added or imported, no devices will be displayed.
- In addition, ensure that all voice VLANs have been configured on all the relevant ports of the devices to enable the wizard to attach QoS properties to these VLANs.

From the Introduction page, select a deployment group to configure IP Telephony QoS. After completing the IP Telephony wizard, QPM creates voice policy groups from the voice policy group templates which are provided by QPM in the Policy Group Templates library based on the network points requiring QoS settings for voice. Your deployment group may also contain previously created policy groups containing data policies. 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.

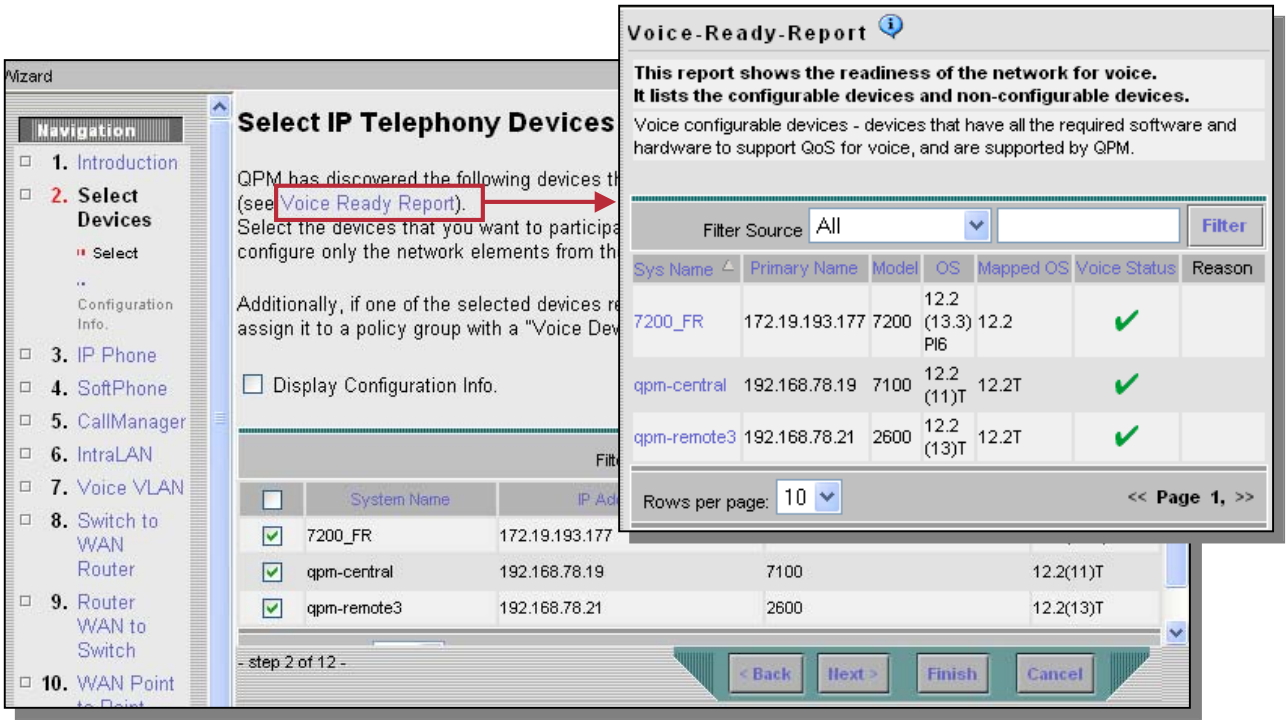
Device Roles

QPM allows the user to import files which contain device role information about devices. 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, the can manually override it in the Device Properties page.

To configure Device Roles, go to the Device Table (*Devices* > *Manage*), and select the device. The *Device Properties* task will appear in the navigation menu.

Create IP Telephony Policy Groups
Getting Started – Selecting Devices

Cisco.com



Getting Started - Selecting Devices

The second step of the wizard is to select the devices that might require QoS configuration. QPM lists the devices that support IP Telephony.

After all the devices have been added, check the readiness of the devices for voice QoS, by running the *Voice Ready* report. The Voice Ready report, illustrated above, shows all the devices in the current device group, and whether or not they support voice QoS.

The Voice Ready report can be generated in two ways:

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

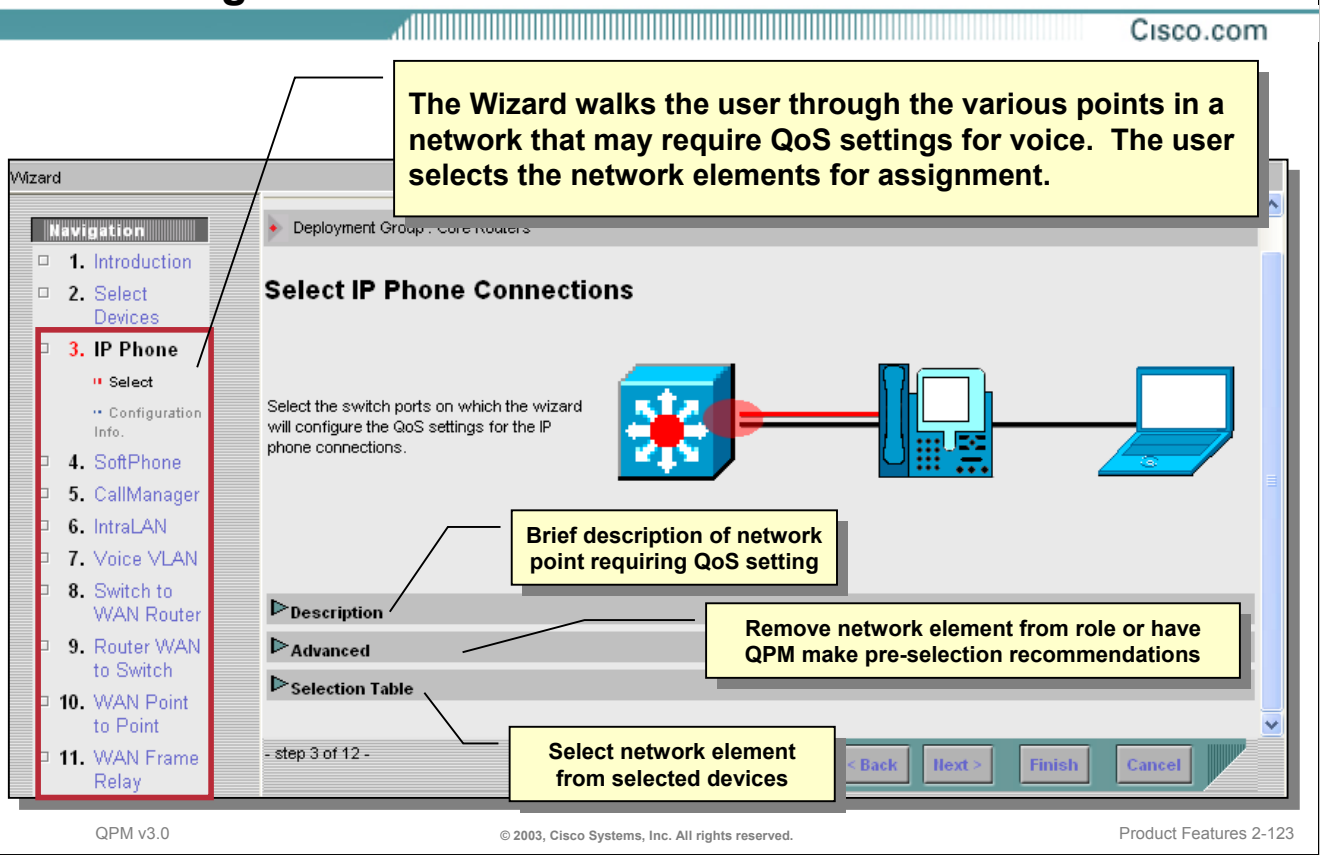
In addition, some devices require global device configuration. For example:

- On Catalyst 6000 switches, the QoS for IP telephony configuration requires adding VoIP control traffic to the second-queue-first-threshold of the 2Q2T queuing scheme of the Catalyst 6000. It also requires adding the VoIP RTP traffic (CoS = 5) to the second-queue-second-threshold, or to the priority queue in the 1P2Q2T queuing scheme.
- On Catalyst 4000 switches, the QoS for IP telephony configuration requires adding VoIP control and VoIP RTP traffic to the highest priority queue.

The wizard will assign those devices that require global configuration to the appropriate voice policy groups with the "Voice Device" voice role.

Tip: It is recommended to select the Display Configuration Info checkbox to view the assignment of network elements requiring device configuration as you proceed through the wizard.

Create IP Telephony Policy Groups
Selecting the Network Points



Selecting the Network Points

The remaining steps in the IP Telephony wizard walks the user through each of the 9 network points, identified earlier, in the network that may require QoS settings for VoIP traffic. Remember that by manually defining the device role in the Device Properties page or by importing the information using a text file, the IP Telephony wizard can limit the list of devices for selection during each step.

At each step, the wizard presents a brief description of the network point, advanced options for removing existing network elements from the role or having QPM make pre-selection recommendations, and finally, a list of only those interfaces on which the relevant QoS settings can be configured.

Refer to QoS for Voice Traffic scenario in Chapter 3 for a complete walk-through using the IP Telephony wizard.

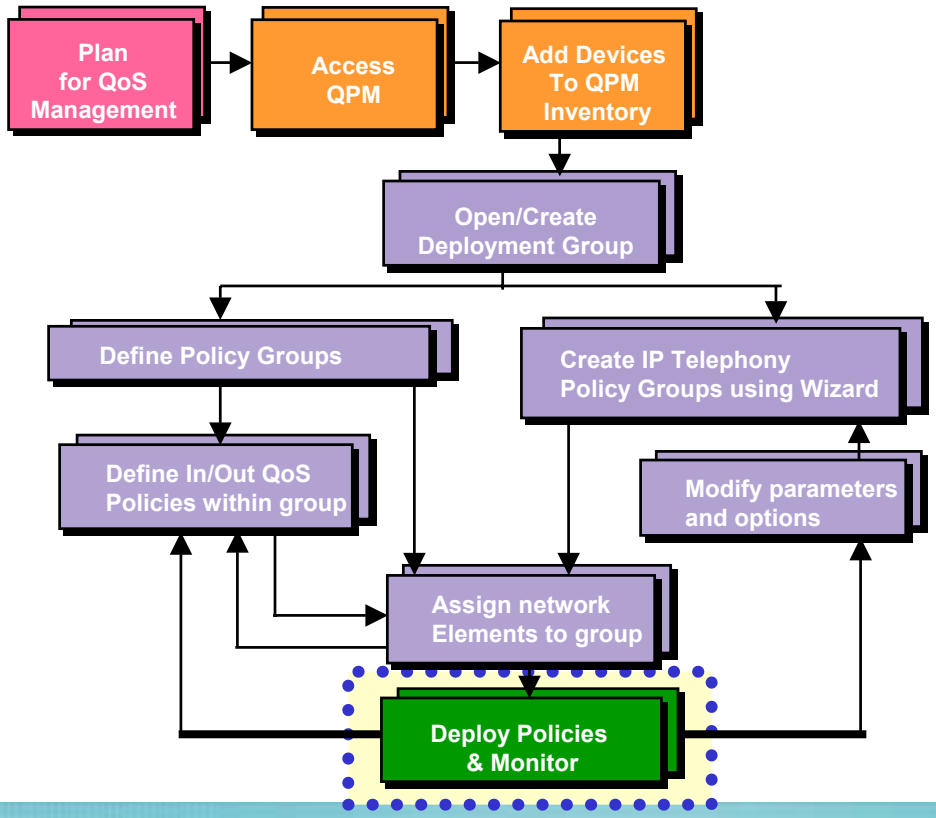
Create IP Telephony Policy Groups
End of Wizard

End of IP Telephony Wizard

In the final step, the IP Telephony Wizard adds the QoS policies and network element assignments to the selected deployment group. At this point, the user can choose to deploy the QoS polices saved in the deployment group using the Deployment Wizard. This topic is discussed next.

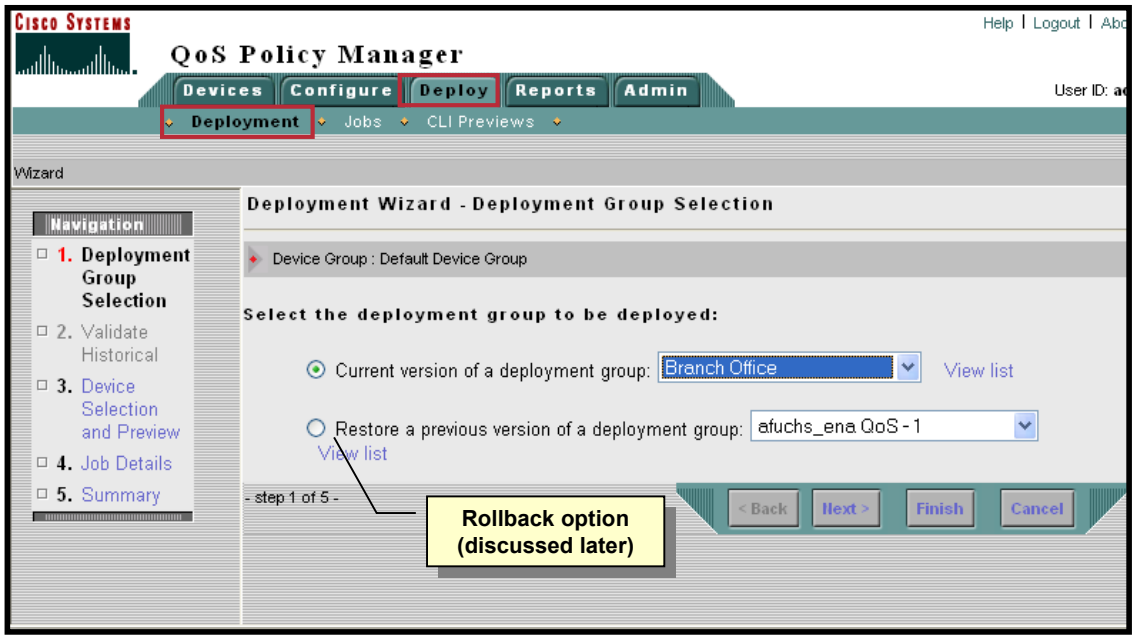
Roadmap

Deploy & Monitor Policies



Policy Deployment
Selecting the Deployment Group

Cisco.com



Selecting the Deployment Group

To deploy the policy groups to the assigned network elements use the 5-step Deployment Wizard. Start the Deployment Wizard by selecting *Deploy* > *Deployment*.

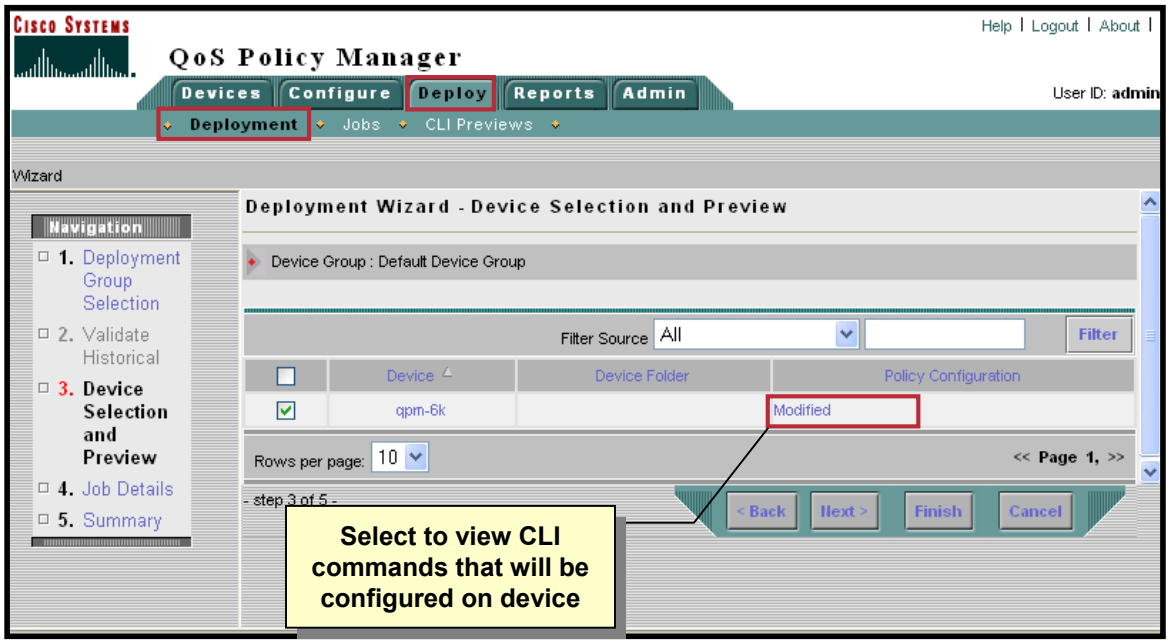
The first step in the Deployment Wizard is to select the deployment group. Remember that a QPM deployment group contains policy group definitions, with all their associated policies and library components, such as IP aliases and application aliases, and the assignment of policies to network elements.

From this page, the deployment group can be selected from the pull-down menu. Later, it will be discussed on how to rollback a QoS configuration using the Restore option from this page. Note: The second step, *Validate Historical*, is only available if the Restore option is check. This step is used to validate the policies, the network elements assigned to the policy group, and aliases used in the deployment group.

Note: If deployment was activated from the IP Telephony Wizard, the Deployment Group Selection page, does not display. In this case, the Device Selection and Preview page automatically appears.

Policy Deployment
Selecting the Devices

Cisco.com



Selecting the Devices

Once the deployment group has been selected, the devices that require their configuration to be modified to will be listed. Thus, the next step is for the user to select and preview the devices requiring configuration changes.

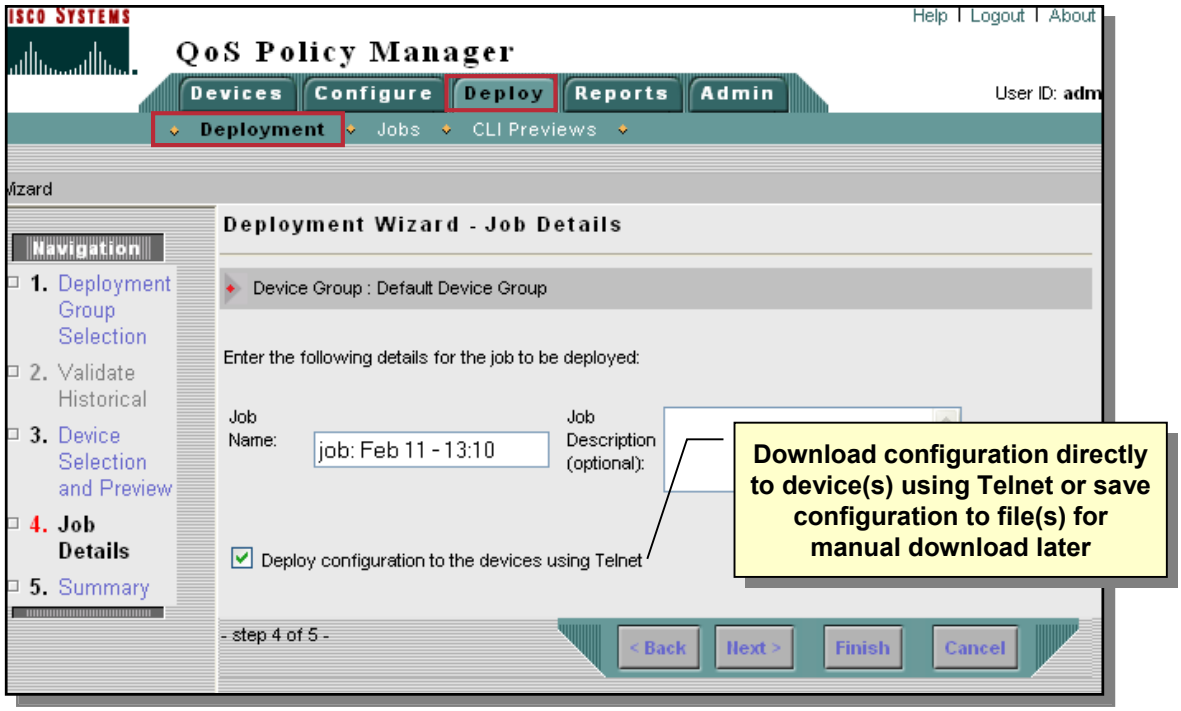
The user can deploy an entire deployment group, or they can specify a subset of devices within a selected deployment group to which QPM will deploy the appropriate QoS policies by marking the checkbox next to the device. By default, all devices requiring configuration changes will have the checkbox marked. Each deployment event is called a "job".

From this page, the user can also preview the CLI commands that will be configured on their devices prior to deployment. To preview the CLI configuration commands for a device, click its *Policy Configuration* link in the table. A CLI 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)

(The CLI Preview window will be discussed later in this tutorial.)

Policy Deployment
Configuring the Job



Configuring the Job

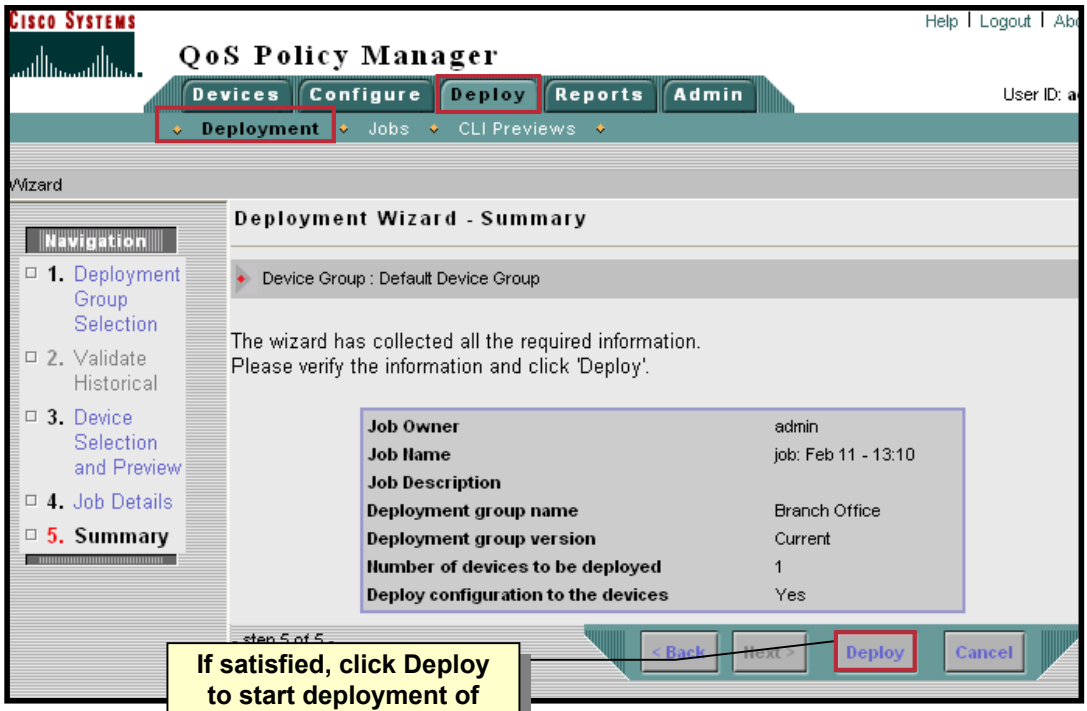
One of the last steps prior to deployment is to define the job by providing a Job Name and optionally a description.

The user also can elect to deploy the configuration directly to the devices using Telnet. This option triggers actual deployment of the deployment group to the devices. QPM can also deploy 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 a hard disk. When required, the user can download these files as a single zip file to their desktop, by clicking the *Files* icon in the Job History report which can be generated from the *Deploy* > *Jobs* task bar.

Remember that if using Telnet to deploy the QoS configuration, the user can choose to use a Secure Shell (*SSH*) connection to the device. Refer back to setting the *Device Group Properties* page in the Getting Started section of this workflow to enable the SSH feature.

Policy Deployment
Job Summary and Deployment

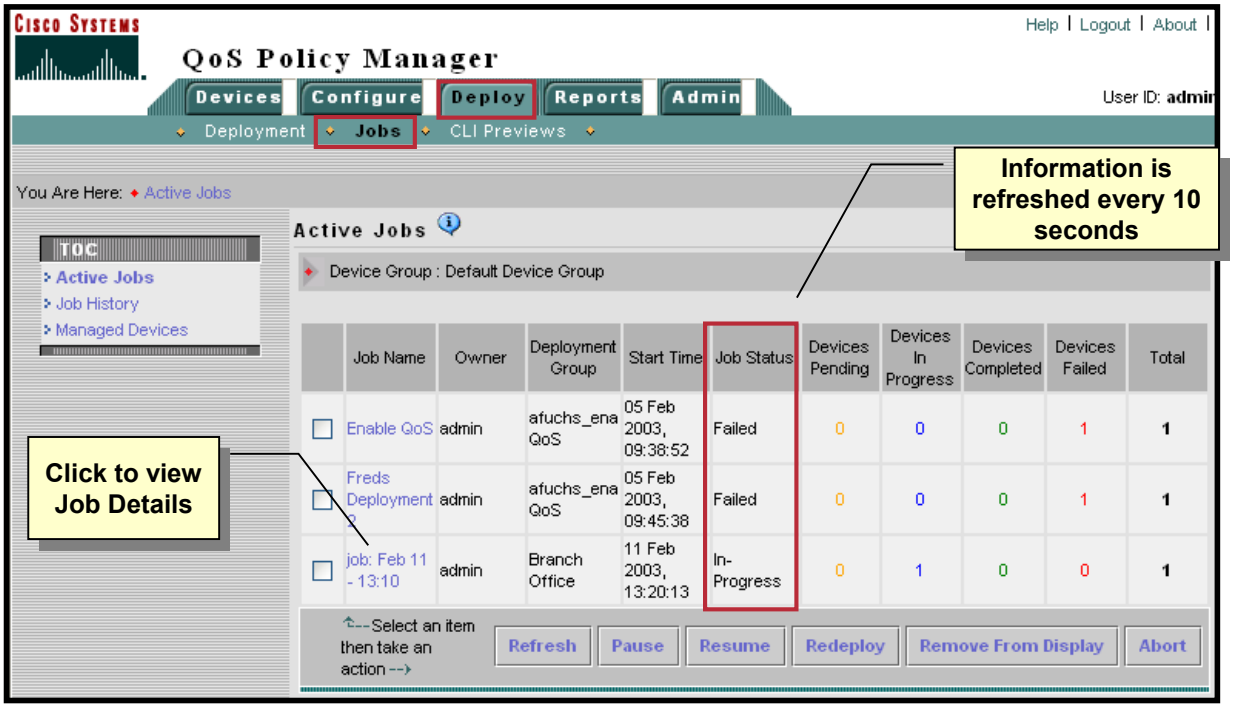
Cisco.com



Job Summary and Deployment

The last step before the actual deployment process begins is to review all the data collected through the Deployment Wizard for verification. If satisfied with the job information that is displayed, the user can deploy the deployment group. Depending upon the option to use or not to use Telnet, QPM sends the configuration commands directly to the network devices or builds configuration files on the QPM server when selecting the *Deploy* button. The *Active Jobs* page appears next, allowing the user to view the deployment process.

Policy Deployment
Active Jobs



Active Jobs

The status of a job can be viewed during deployment using the Active Jobs page which appears after the user clicks *Deploy* and can also be viewed by selecting *Deploy* > *Jobs*. The Active Jobs page provides a dynamic view of all the active deployments and their status.

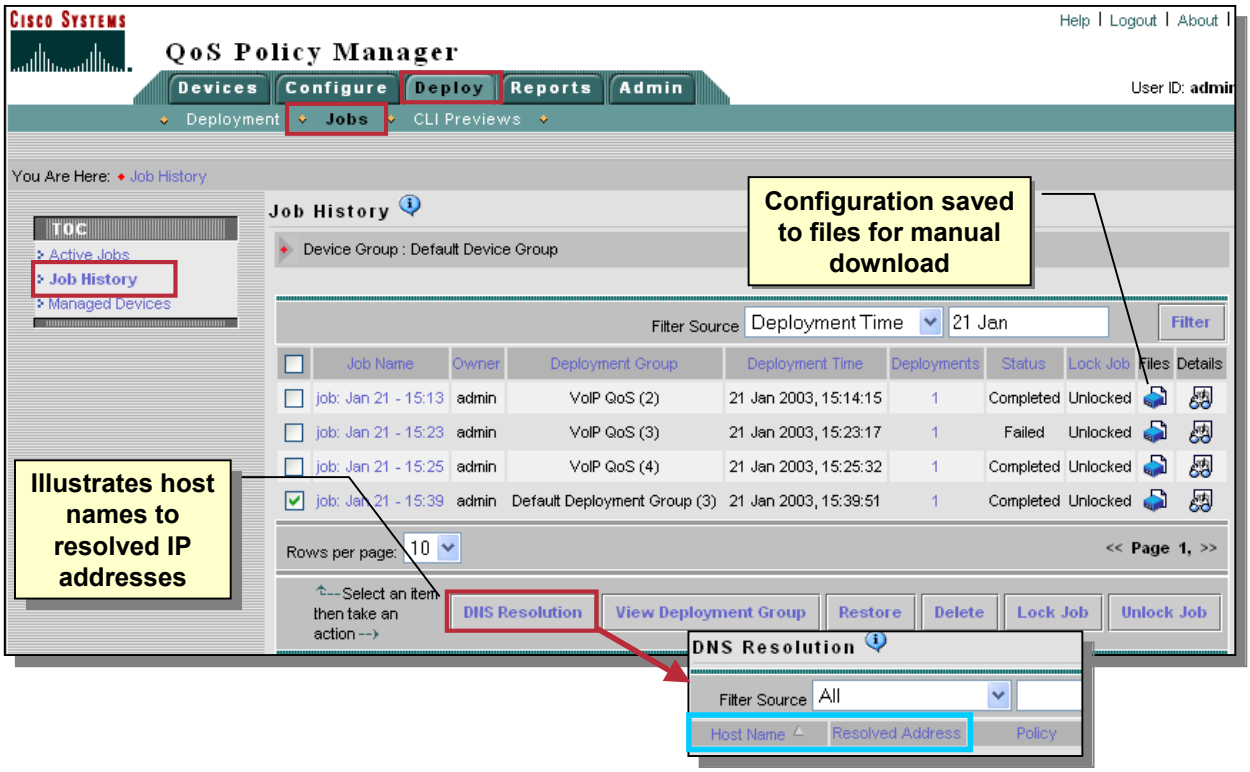
For each deployment job, the start time of its configuration, its status, and a summary of the number of devices deployed according to their status, are displayed. The status of a job deployment or a device deployment might be Pending, In Progress, Completed, or Failed. A job deployment may also have 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.

Note: The page is automatically refreshed every ten seconds. To force a refresh manually, click *Refresh*.

Policy Deployment
Job History Report



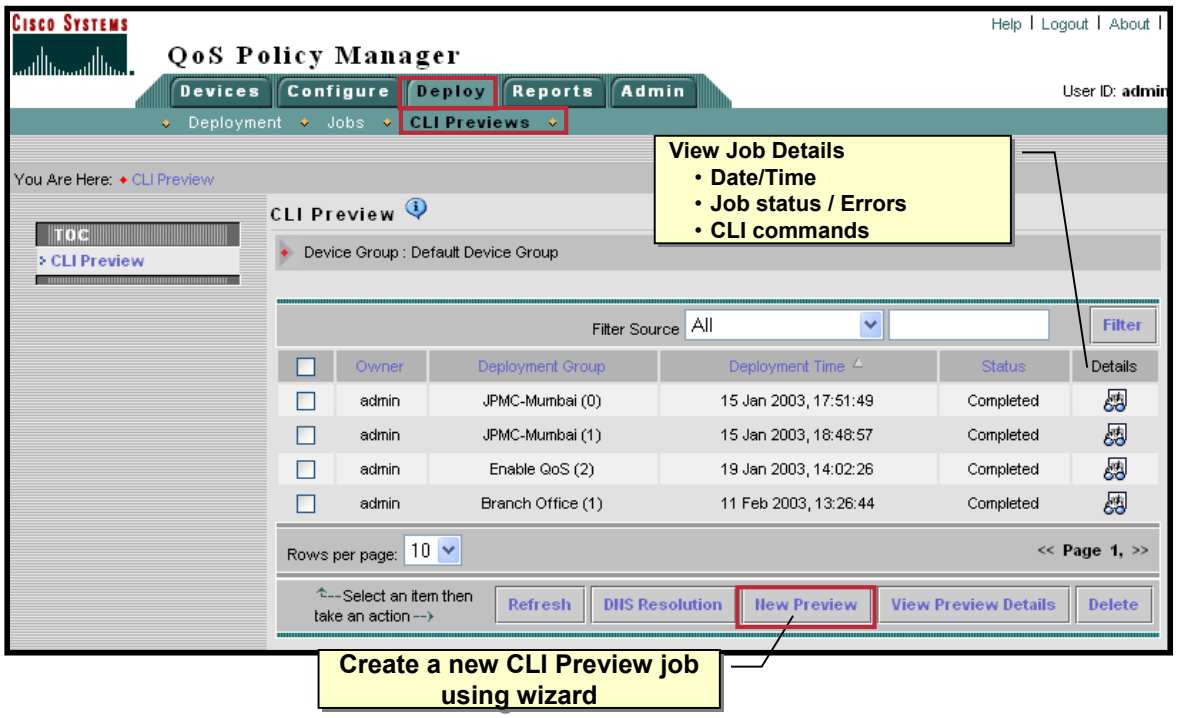
Job History Report

The Job History report provides information on jobs submitted for a deployment group and its status. Details about the status of a job can be also viewed by selecting the *Details* icon.

As mentioned earlier, if the QoS configuration is sent to configuration files instead of directly to the devices using Telnet, the device configuration files can be viewed from this report.

Another helpful task is the DNS Resolution feature. When creating a policy definition which includes a host address, a host name may be used instead of the IP address. QPM will resolve the newly-added host names to their IP addresses, to update any changes in the network. From the Job History report, the user 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. To view the results of a DNS host name resolution check, select the job using the checkbox and then, click *DNS Resolution*. The DNS Resolution page appears,displaying a list of IP addresses to which the host names were resolved, for the selected job.

Policy Deployment
CLI Preview



CLI Preview

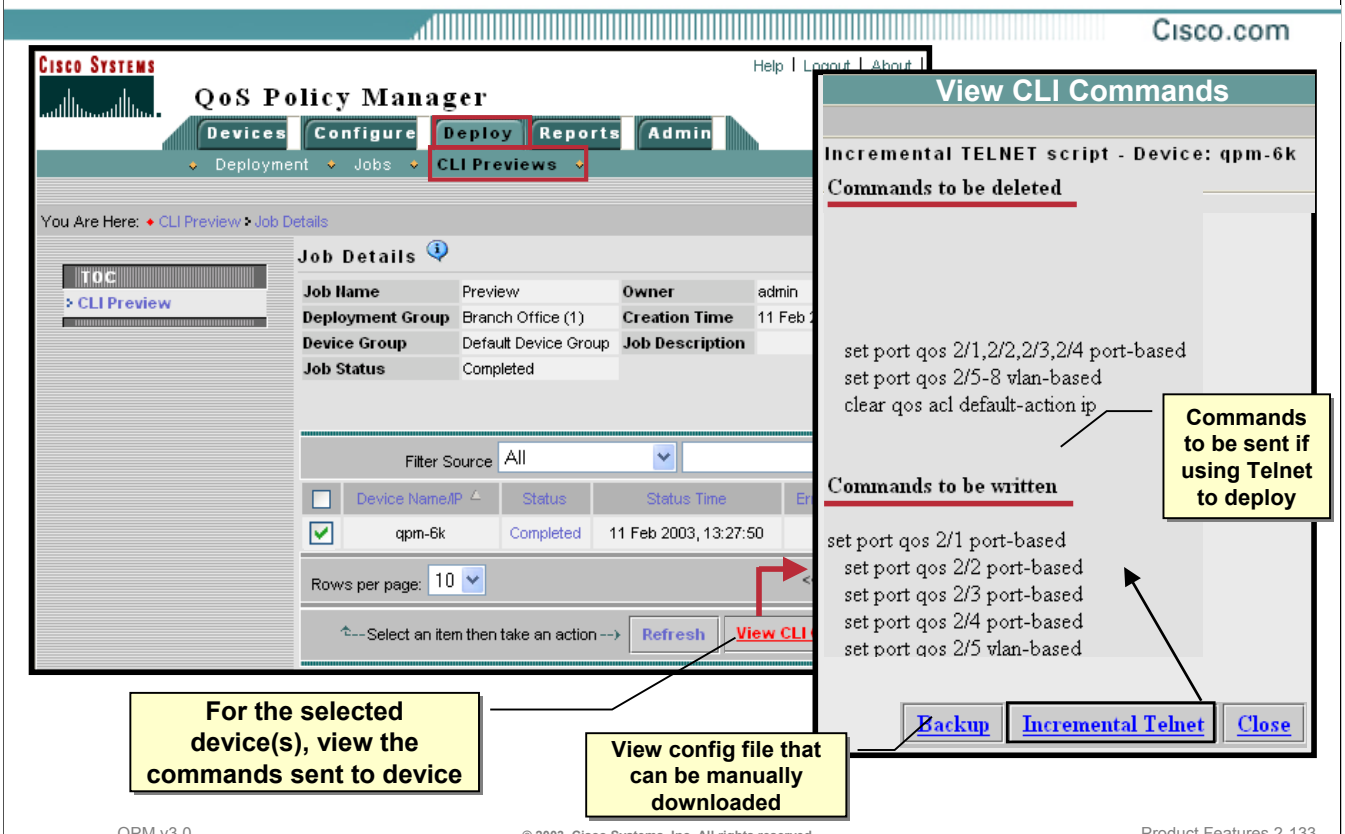
To view, in advance, the CLI commands that will be sent to the devices upon deployment, the user can create a CLI Preview job to view the commands for the current deployment group. CLI previews are determined by querying the devices for their existing configuration and then calculating the incremental changes.

By selecting *Deploy* > *CLI Preview* and then clicking the *New Preview* button, the user can activate a CLI Preview job in which CLI commands are generated for all or selected devices in a deployment group.

In addition, QPM provides other ways in which the CLI commands can be viewed:

- In Step 3 in the Deployment Wizard, the user can preview the CLI commands that will be configured on a single device, prior to deployment.
- In the Policy Translation page, the user can view the CLI configuration of policies for a device.

Policy Deployment
CLI Preview

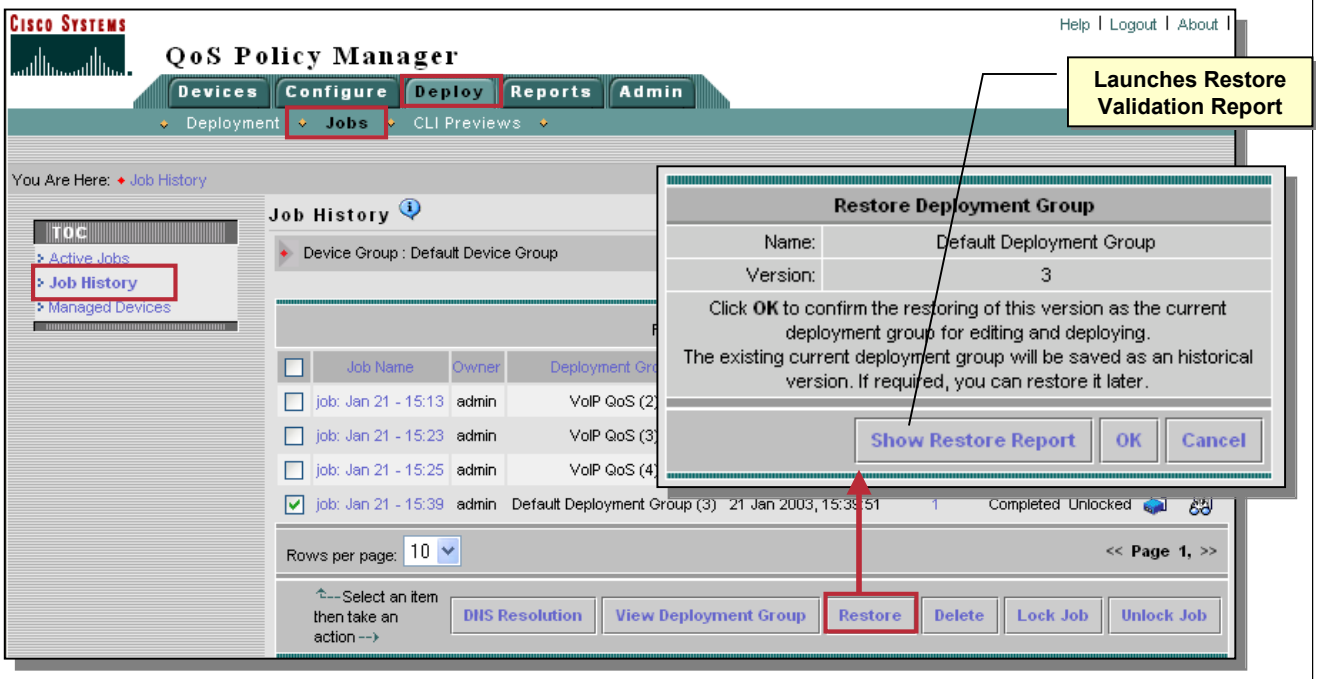


CLI Preview

After running a CLI Preview job, the results can be viewed when completed by clicking the *View CLI Commands* button. Remember that the CLI previews are determined by querying the devices for their existing configuration and then calculating the incremental changes. Therefore, the user can view the commands in the configuration that will be deleted and the new commands that will be written to the device configuration.

If deploying directly to the device using Telnet, view any incremental Telnet script commands that will be written. Alternatively, view the Backup ShowRun configuration commands.

Policy Deployment
Restore Historical Deployment Group



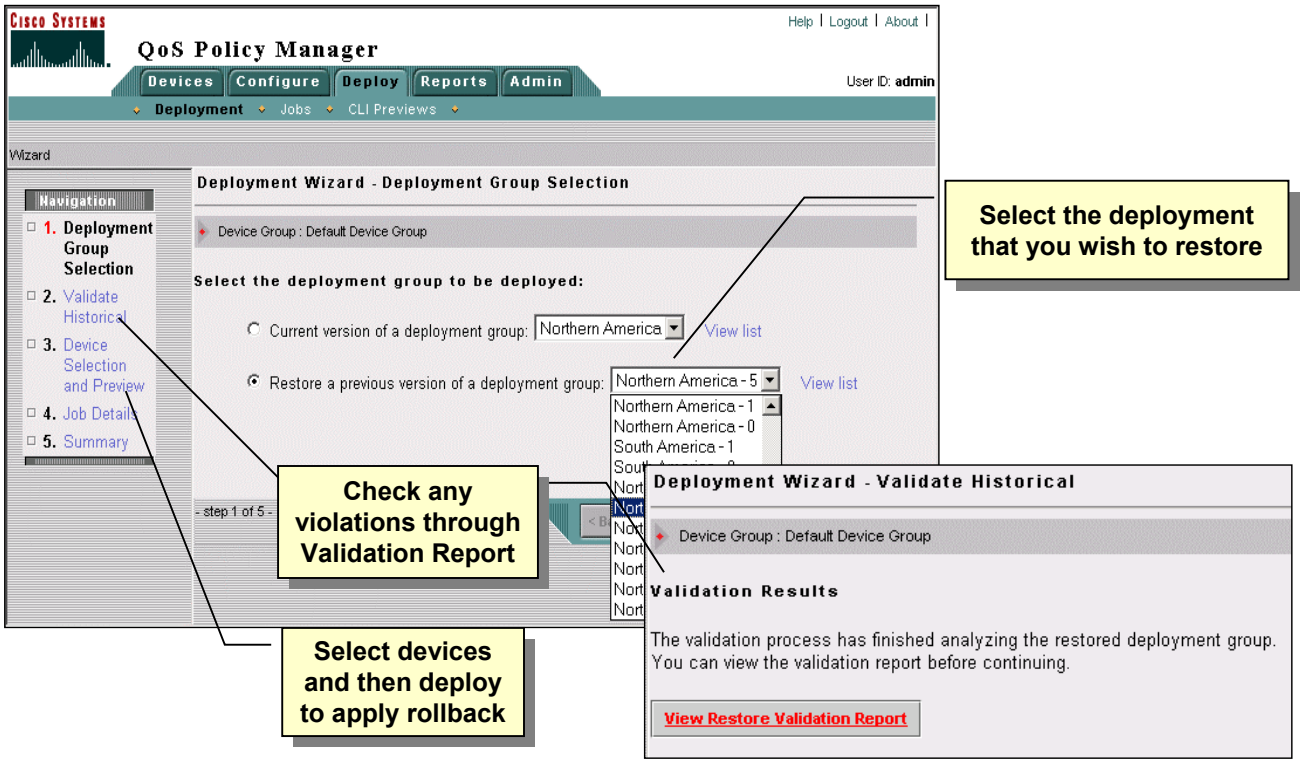
Restore Historical Deployment Group

QPM allows the user 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. Note, a historical version of a deployment group can be viewed without restoring.

To view a table of historical deployment jobs and all their details, use the *Job History* report found by selecting *Deploy* > *Jobs*. Here, the user can select the *Restore* button. Validation checks are automatically done on the deployment group. If the restore process detects any validation violations, the results will be written to a validation report for viewing. Violations may occur due to changes in aliases, assigned network elements, or changes to the device. (Refer to next page for more information.)

Note: A user can view a history of all the deployment group restore operations, from the *Reports* > *Restore* page.

Policy Deployment
Deploy Historical Deployment Group

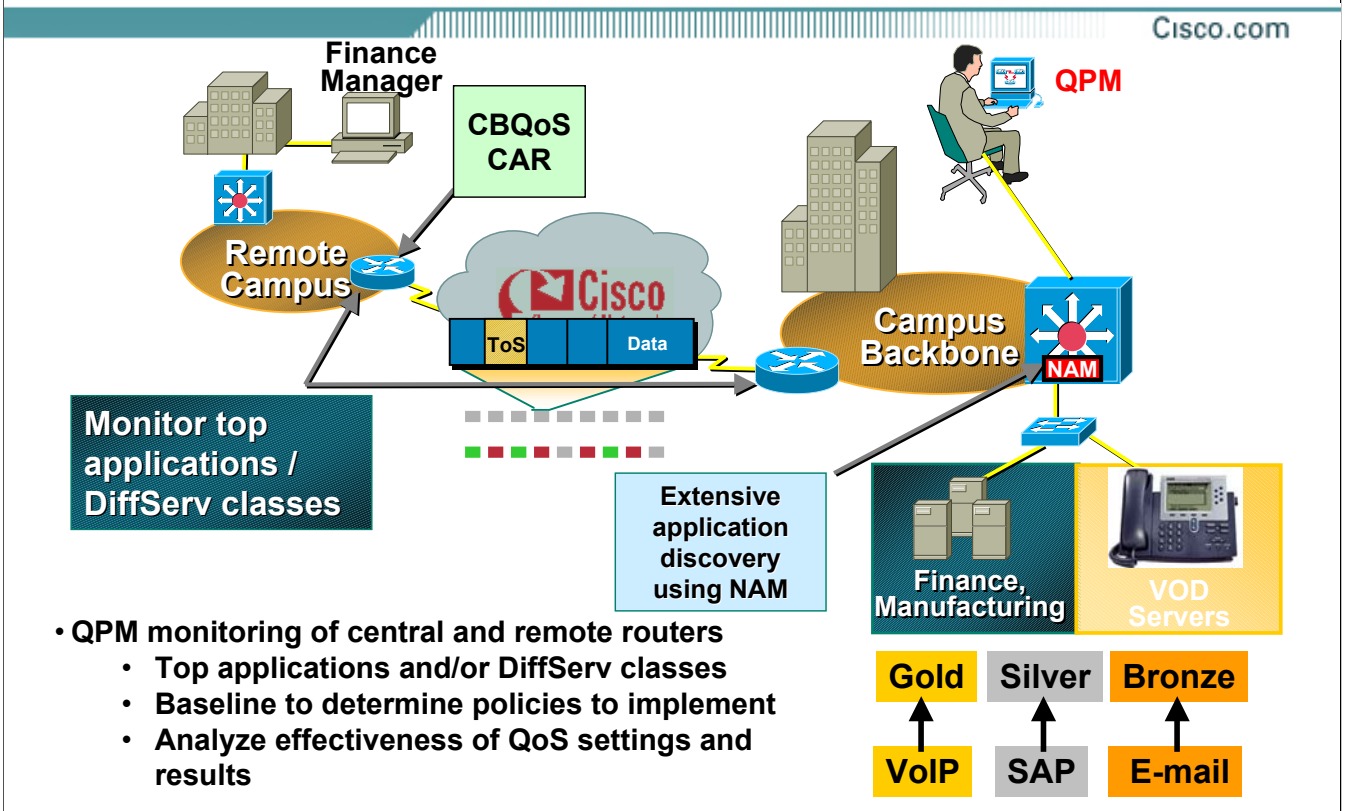


Deploy Historical Deployment Group

To deploy the restored deployment group, follow the steps of the Deployment wizard and select the option to restore a previous version of a deployment group. The next step in the Deployment wizard is to validate the historical version. Again, the system does the following checks and automatically provides a restore validation 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.

QoS Monitoring and Analysis using QPM
Overview



- QPM monitoring of central and remote routers
  - Top applications and/or DiffServ classes
  - Baseline to determine policies to implement
  - Analyze effectiveness of QoS settings and results

QoS Monitoring and Analysis using QPM

QoS monitoring and analysis using QPM, can be performed throughout the lifecycle of network management.

Earlier in the planning phase of the workflow, QPM could be used to perform a baseline analysis to determine how traffic was flowing on the network. This is performed by having QPM deploy QoS policies that filter or classify traffic, but does not perform any policy action except allow the traffic to pass through. Based on the analysis of the baseline, network administrator will have more confidence in the QoS mechanism chosen for deployment.

After deployment of actual QoS mechanisms, such as limiting, shaping, queuing or dropping, network administrators can then use QPM to analyze the effect of implementing QoS mechanisms in the network. Network administrators can use QPM to pull the policy statistics from the device MIBs and generate reports to assess the effectiveness of the QoS policies and possibly plan for policy changes.

(In order for QPM to monitor QoS policies, the policies need to be deployed by QPM and consist of either Class-Based or CAR QoS policy types.)

QoS Monitoring and Analysis using QPM
Features

Cisco.com

- **Leverages Cisco intelligent infrastructure**
  - **Class-Based QoS (CBQoS) MIB used for Modular QoS defined policies (IOS 12.2, 12.2T, 12.1E)**
  - **CAR MIB used for non-Modular QoS defined policies (IOS 11.1cc, 12.0, 12.1, 12.2, 12.2T)**
- **Real-time and historical line graphs and bar charts**
- **View traffic statistics before and after QoS actions:**
  - **Packets/bit rate matching policy and specific filter**
    - **includes NBAR application filters**
  - **Attempted (before QoS action)**
  - **Succeeded (after QoS action)**
  - **Dropped traffic**
- **View QoS action statistics**
  - **WRED, Policing, Traffic Shaping, Queuing**
- **Export of raw data to file/database for advanced analysis**

QoS Monitoring and Analysis using QPM

Remember that QPM can only monitor Class-Based QoS (i.e. CBWFQ) and CAR QoS type policies that are deployed to the network by QPM.

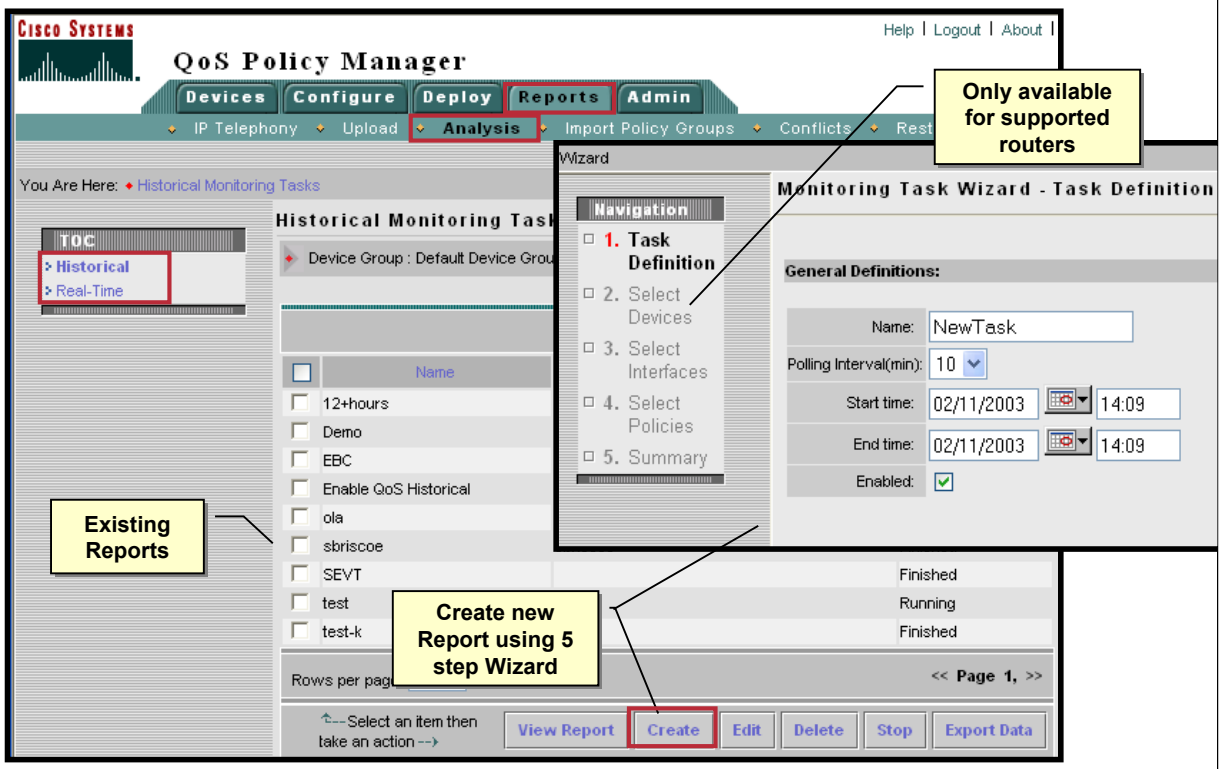
QPM can perform two types of analysis: Historical and Real-Time. Both historical and real-time QoS monitoring reports display the similar types of QoS monitoring data.

- Historical analysis monitors traffic for all QPM policies on one or more interfaces, polling on a regular basis and storing the gathered data. The data is gathered between a start and end time that is defined and displayed in historical monitoring reports. A network administrator 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. Network administrators 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.

The type of statistics reported in the reports are:

- 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).
- A breakdown of the traffic that matched each of the policy's filters. For example, see if traffic from one application is using too much of the bandwidth allocated to its traffic class.
- 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 (limiting), and Traffic Shaping.

QoS Monitoring and Analysis using QPM
Configuring QoS Analysis

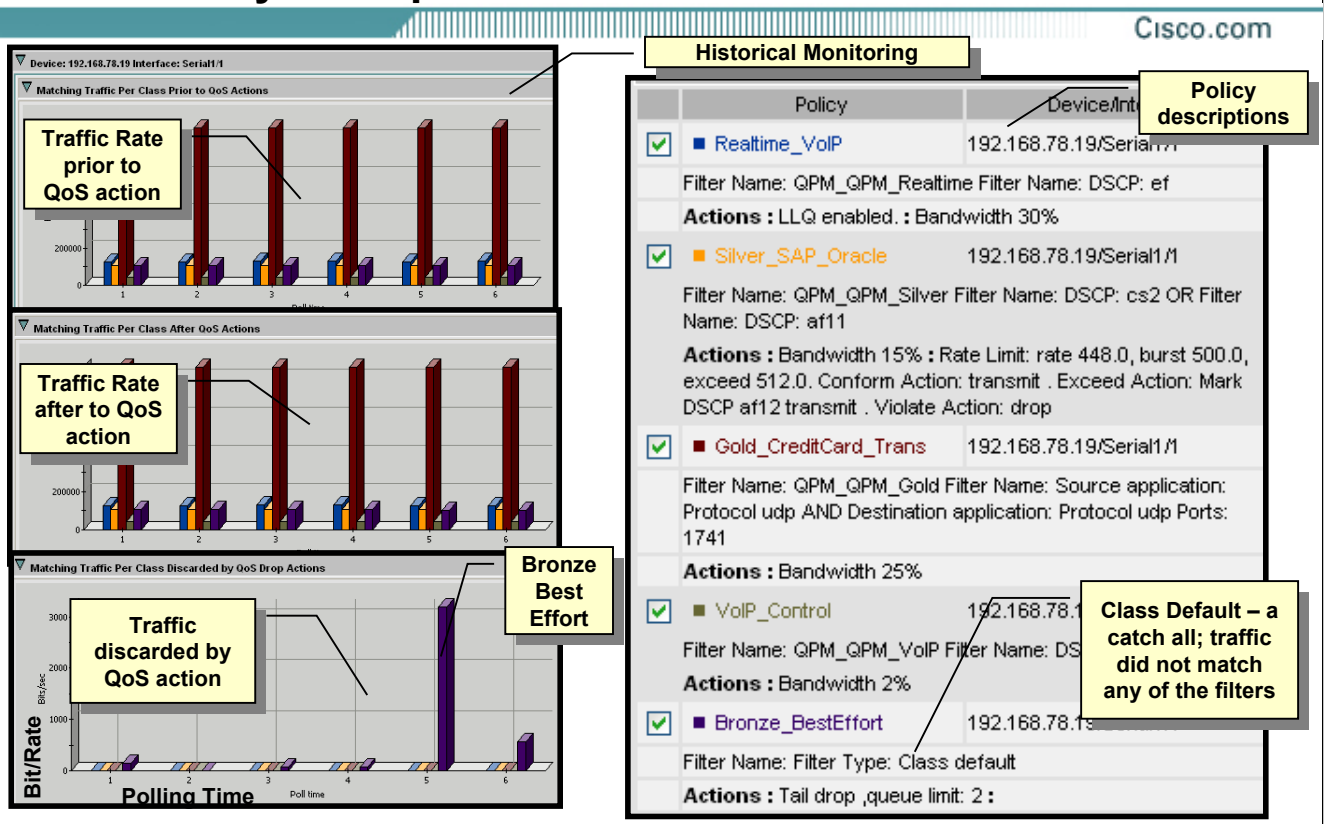


QoS Monitoring and Analysis using QPM

The QoS analysis will show how the important traffic classes on your network are flowing. Each traffic classes is monitored by a named policy configured on a supported IOS device. This information can be used to design QoS that better meets the needs of the network. As mentioned, you can perform a QoS analysis using either historical or real-time data. To do this, follow the steps below:

1. Create a QoS monitoring task using the 5-step Monitoring Task Wizard. From QPM, select *Reports* > *Analysis* and then select either *Historical* or *Real-Time* from the TOC menu. Previously defined reports are listed. To create a new QoS monitoring task, click *Create*. Enter a name and polling interval. If running a historical task, enter the monitoring start and end times.
2. QPM then lists the routers in the QPM inventory and in the active device group that support traffic monitoring. (Only devices that belong to the active device group are available for selection. Use *Devices* > *Manage* > *Device Groups* to change the active device group, if ACS is used for user/device authorization.)
3. Then select the interfaces on the device that should be monitored. Remember that real-time monitoring can monitor only one interface continuously, whereas, historical monitoring can monitor one or more interfaces for a defined timeframe. Also, only interfaces on which QoS is configured that QPM can monitor appear in the list.
4. And finally, select the QoS policies that should be monitored on each interface.

QoS Monitoring and Analysis using QPM
QoS Analysis Reports



QoS Monitoring and Analysis using QPM

Historical QoS monitoring reports are available after the QoS analysis task has polled data from the router three times (which depends on the start time and polling interval defined). But the data is most useful if the tasks runs for a significant period of time because the results are more reliable after the data has been polled a number of times. To view a report, select the report from the *Reports* > *Analysis* page and click the *View Report* button.

Real-time QoS monitoring reports are available and displayed immediately after defining the QoS analysis task.

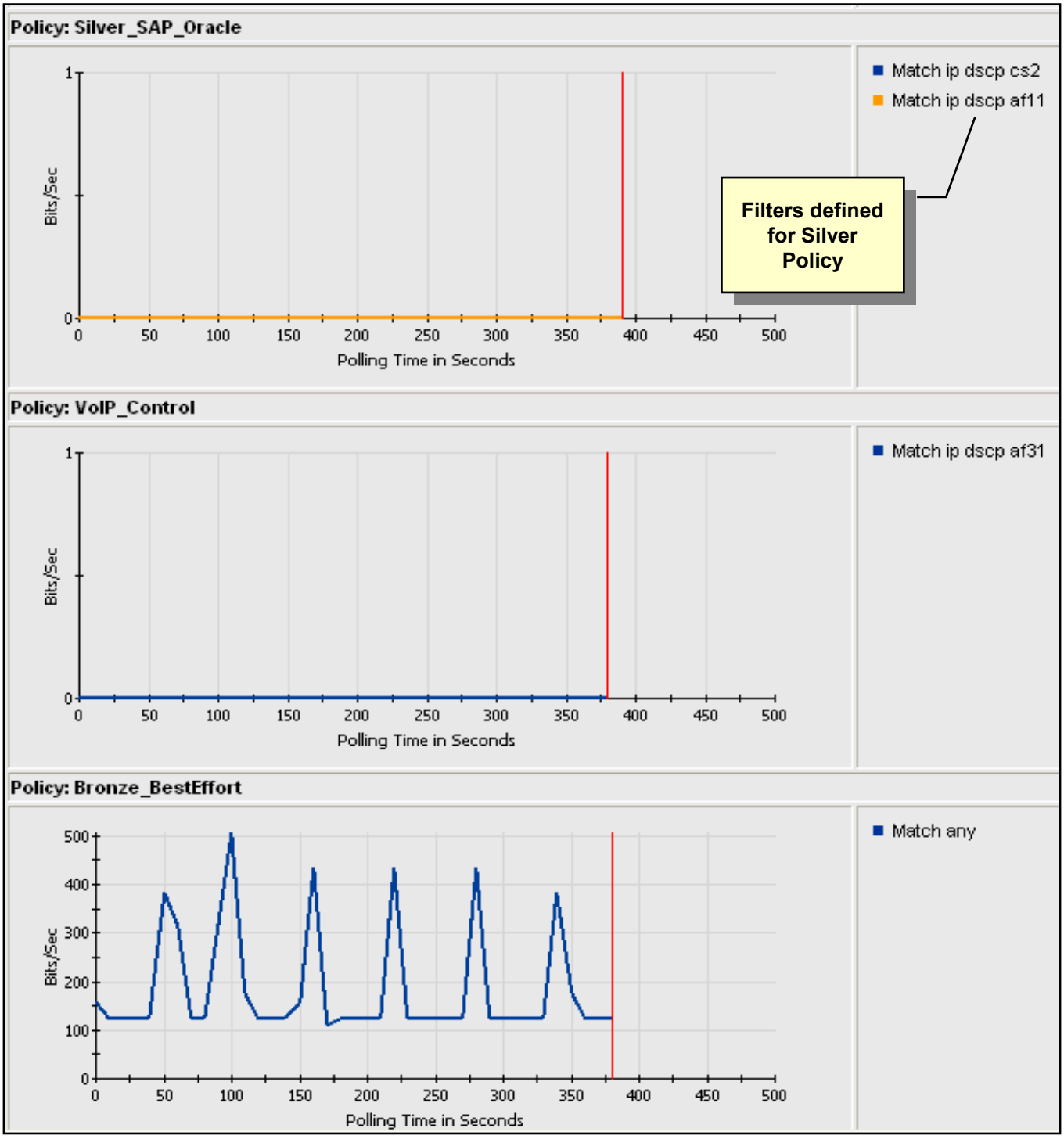
The reports are divided into 3 areas: Policies, Filters, and Actions.

- The Policy section, illustrated above, shows how much traffic matched the policies and whether it was transmitted or dropped.
- The Filters section, illustrated on the next page, shows how matching traffic was distributed among the policy filter conditions.
- The Actions section, illustrated on upcoming page, shows the policy actions that were taken on matching traffic.

The report layout can be customized. Refer to the on-line help for more information.

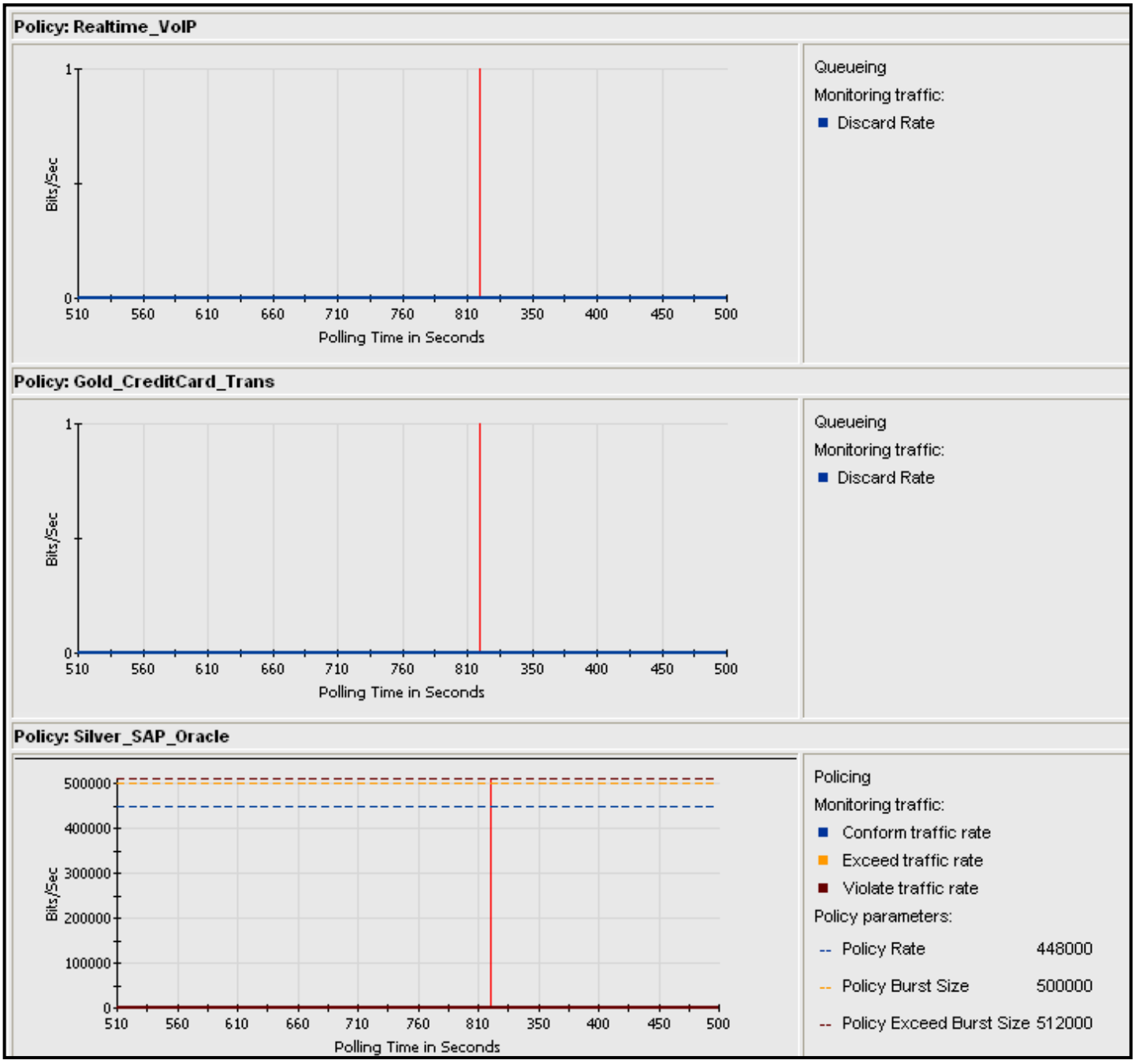
Real-Time Monitoring Task

This graph illustrates the Filters section of the report. It illustrates how matching traffic was distributed among the policy filter conditions.



Real-Time Monitoring Task

This graph illustrates the Actions section of the report. It illustrates the actions that were taken on matching traffic. In this case, no traffic was discarded.



This page intentionally left blank.

Congratulations!

We hope that this chapter has helped you to understand how QPM can a valuable part of your network management toolkit.

Continue on with Chapter 3 to learn more about QPM by looking at various QoS scenarios.

Cisco Systems

Chapter 3

Scenarios

QoS Policy Manager (QPM) v3.0

Chapter 3 Scenarios

Cisco.com

QPM Scenarios

1. Limiting Bandwidth on Non-Critical Applications
2. Prioritizing Traffic
3. Providing QoS for Voice Traffic

Chapter 3 Objectives

In this chapter, we will explore three QoS scenarios that illustrate the use of several QPM features discussed in the previous chapter. These scenarios will help you to understand how to achieve specific networking QoS objectives using Cisco IOS and CatOS features. You will then learn how to use QPM to create policies and deploy them to your devices.

In general, QoS can help solve bandwidth and time sensitivity problems. In these scenarios, you will explore how to limit and guarantee bandwidth to specific traffic types. Prioritization of traffic will allow you to obtain better response time for time sensitive applications and voice traffic.

Note that some applications can benefit more from QoS techniques than other applications. The benefits you might get from QoS are dependent not only on the applications you use, but on the networking hardware and bandwidth available to you.

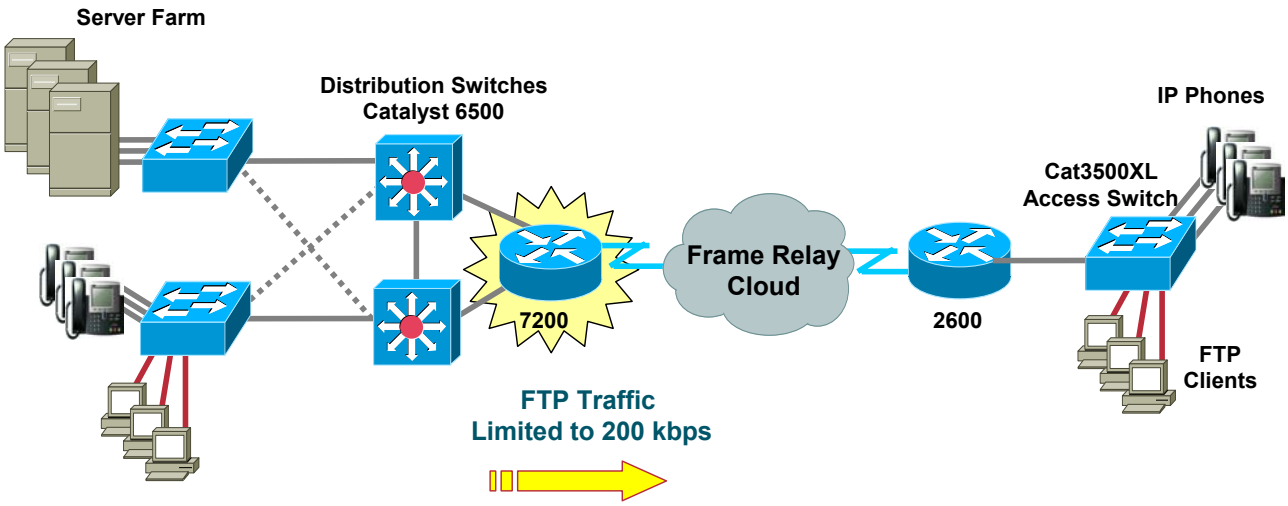
Before we begin, it is important to note that there are numerous designs for addressing the QoS requirements in these scenarios and there may be more than one solution. Now, let's describe the first scenario.

Scenario 1

Limiting Bandwidth on Non-Critical Applications

Scenario 1
Limiting Bandwidth on Non-Critical Applications

Cisco.com



QPM v3.0

Scenarios 3-4

Scenario 1 - Limiting Bandwidth

If the network has insufficient bandwidth, either due to the lines being leased or the devices installed, you need to protect your critical applications running across the WAN from being delayed by large amounts of non-critical application traffic. QoS mechanisms can help you limit the bandwidth for non-critical applications (perhaps FTP file transfers), so that critical applications have a greater amount of bandwidth available to them.

Limiting bandwidth lets you set a limit on specific types of traffic. You may wish to put a cap on the bandwidth available to specific traffic to ensure that the remainder of the bandwidth is available to other kinds of traffic. You can create traffic shaping policies or traffic limiting policies on an interface to manage how much of the bandwidth should be allocated to a specific traffic flow. You can set your policies based on a variety of traffic characteristics, including the type of traffic, its source, destination, and/or IP precedence settings (traffic coloring). Shaping differs from limiting in that shaping attempts to throttle traffic when it reaches the rate limits. The router buffers some of the traffic bursts. Only when the buffer is full are packets dropped. Whereas, limiting policies drop all packets that exceed the defined rate limit.

For this scenario, we will create a policy that limits FTP traffic to 200 K bits/sec across the WAN. If FTP traffic does not fill 200 KB/sec, other kinds of traffic can use the unused bandwidth. Packets could be dropped or buffered to shape the traffic if the traffic bursts exceed the limit. In this scenario, we will limit or drop non-conforming packets on the outbound WAN interface.

Scenario 1
Getting Started

QPM v3.0 Scenarios 3-5

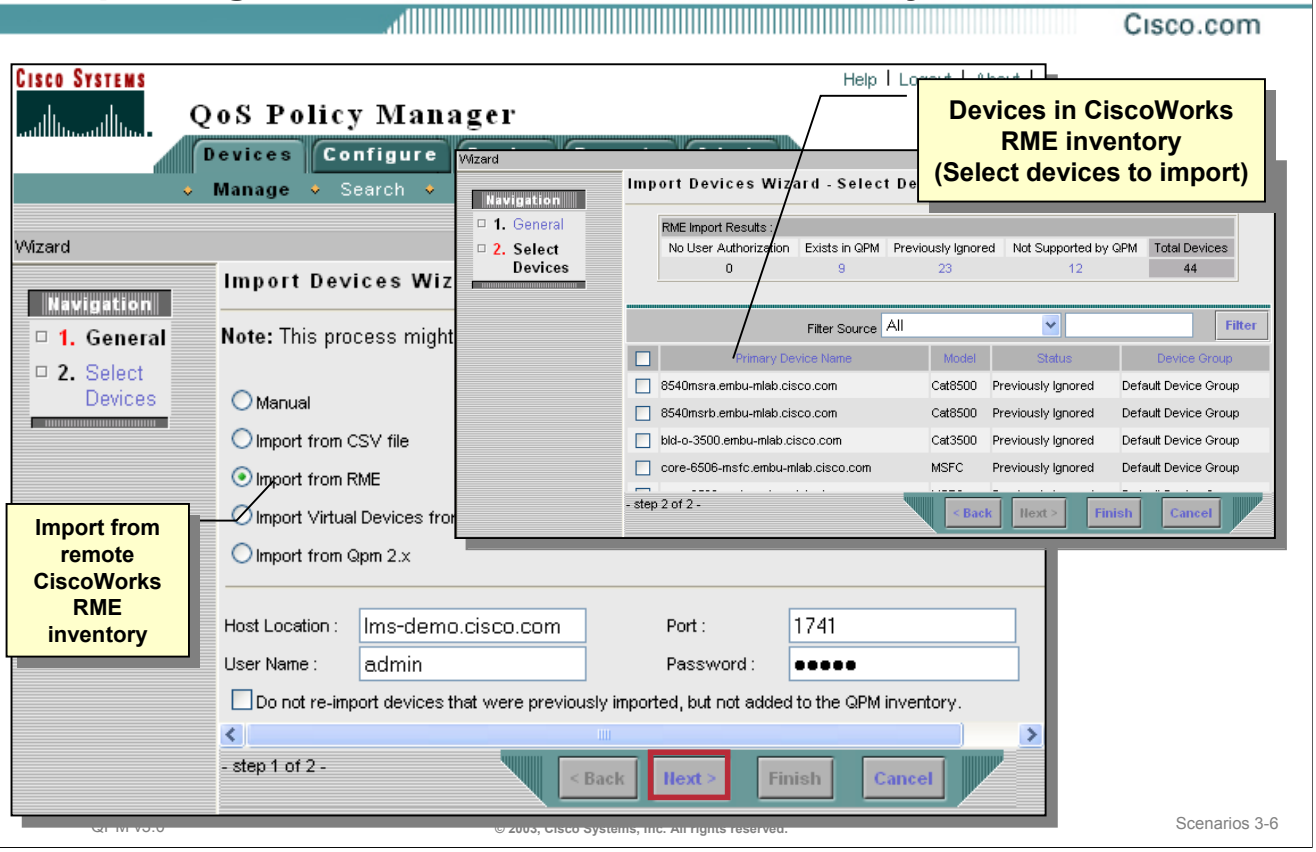
Getting Started

Getting started writing QoS policies with QPM is easy. First, launch QPM from the CiscoWorks desktop. From a supported web browser access the CiscoWorks server that is hosting the QPM application.

To perform this task, follow the steps below:

1. Ensure that your client workstation and web browser meets the specified client requirements outlined in Chapter 4 of this tutorial.
2. Enter the URL **http**://<*CiscoWorks server*>:**1741**
3. Login to the CiscoWorks server. The default administrator login is *admin*. (The default administrator password is set during installation)
4. Open the QoS Policy Management drawer in the navigation pane on the left.
5. Click *QPM*. A new browser window is launched.

Scenario 1
Importing the Devices into QPM Inventory



Importing Device from RME to the QPM Inventory

To manage the QoS configuration on a device or any of its elements with QPM, you must first add it to the QPM 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, the devices must be running and accessible on the network before they can be added to the inventory.

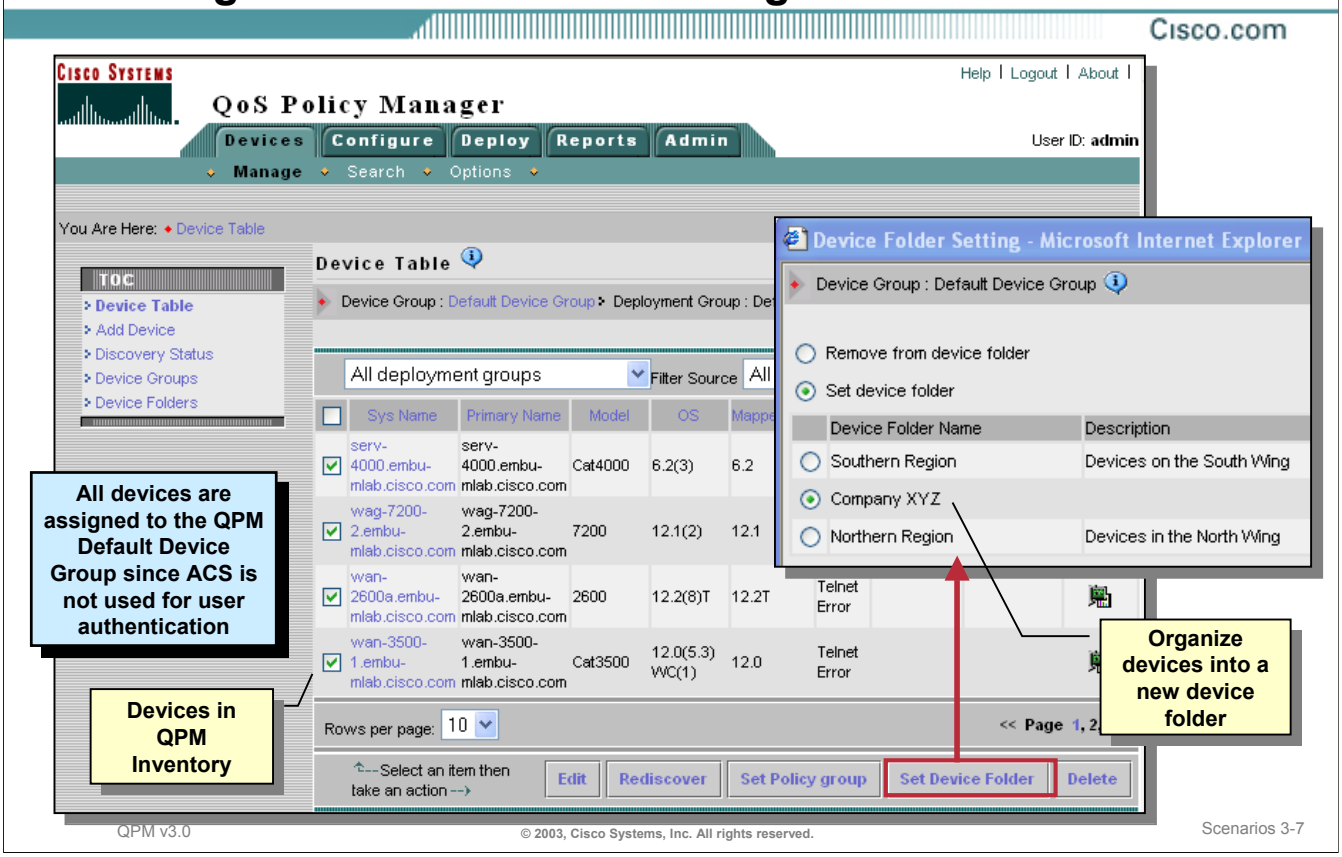
You can only add a device to the inventory if you have sufficient access permissions to it. Remember, you can use Cisco Secure Access Control Server (ACS) or the CiscoWorks Common Services (CCS) for user authorization. These scenarios assume CCS user authorization for the devices in the device group.

To add devices from CiscoWorks Resource Manager Essentials (RME) to QPM using the Import feature, follow these steps:

1. From QPM, select *Devices* > *Manage*.
2. From the TOC navigation pane, select *Add Device*.
3. First, select the *Import from RME* radio button and then enter login information about the RME server, such as: IP address or hostname, installed service port number (by default RME is installed using TCP port 1741), and the administrator's login name and password.

   Check the "Do not re-import …" checkbox if you do not want a device that is already in the QPM inventory to be re-imported; thus possibly changing some device attributes that were configured. Also, check the box if you already ignored a device from a previous import session and still do not want to import the device.
4. Click *Next* to then select the devices in RME to import.
5. QPM provides a summary of the devices in RME that were already imported, previously ignored during an earlier import session, or not supported by QPM. A list of available devices for import are listed. Place a checkmark next to the devices you wish to import. Note, if the list is large, there may be multiple pages of devices for selection. Click *Finish* to begin the import process.

Scenario 1
Viewing the Device Table / Setting the Device Folder



Viewing the Device Table / Setting the Device Folder

After you have added devices to QPM, the devices in the QPM inventory can be viewed using the Device Table. (Remember that there may be multiple pages in the table for viewing. By default, only 10 devices are displayed per page, but this is configurable and all devices can be viewed on a single page and scrolled for viewing.) If not displayed already, select *Devices* > *Manage* > *Device Table*.

In these scenarios, the user authentication method employed is the local CiscoWorks server. Since ACS is not being used, all devices are placed into the *Default Device Group* created by QPM. (If ACS was used for user authentication, the device groups in ACS are imported into QPM and the devices are placed into the same device groups that are in ACS.)

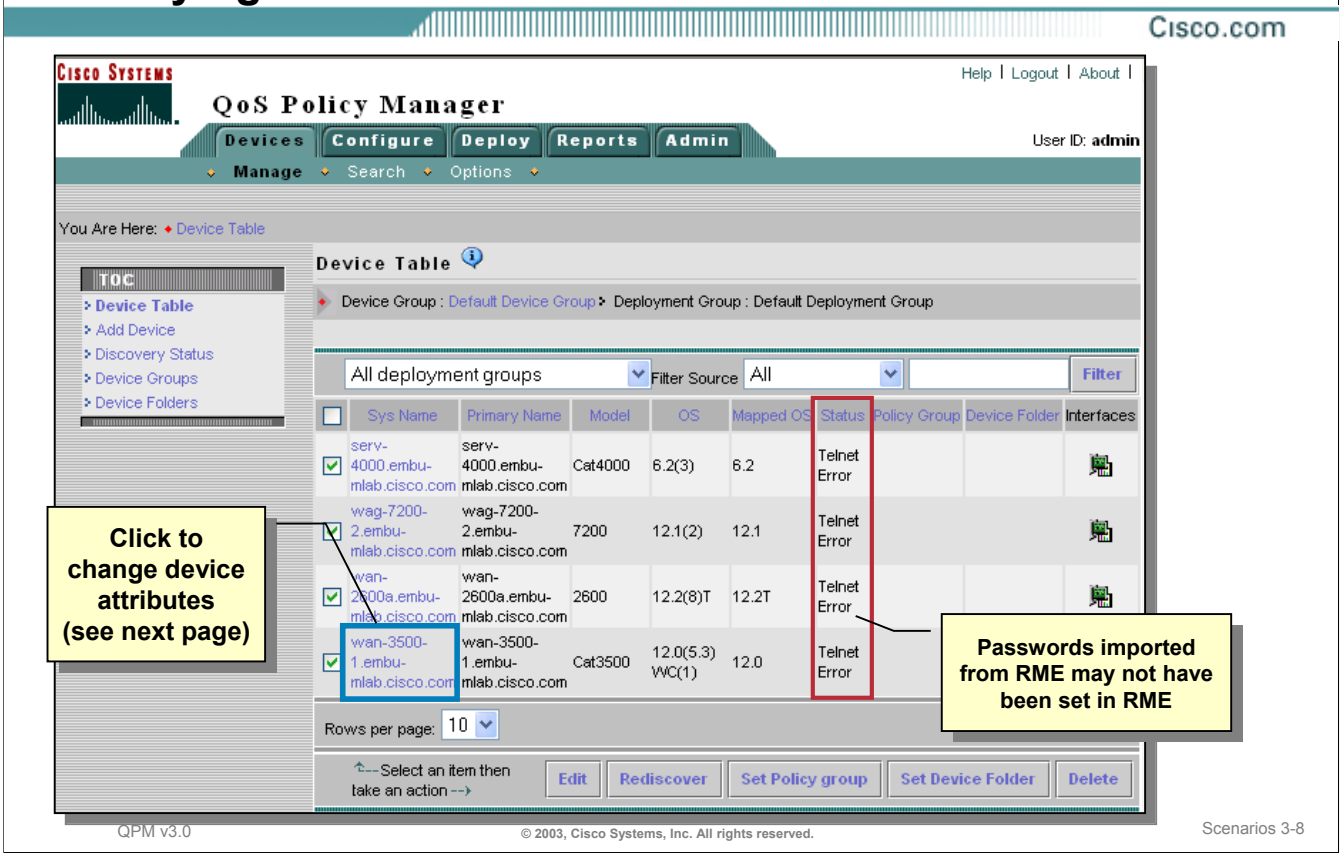
Since this QPM server is used to manage multiple organizations, the devices just imported will be placed into a new device folder for ease of administration. A new device folder, called Company XYZ, will be created.

To create a new device folder, assign the devices to the folder, and view the Device Table, follow these steps:

1. Create a new device folder by selecting the tab *Devices* > *Manage* and then the link *Device Folders* in the TOC. Click the *Create* button, enter a name and description for the new folder, and click *Save*.
2. The devices can then be moved to the new device folder by opening the Device Table and selecting them. Select *Device Table* from the TOC navigation pane. Check the devices to move to the new folder, and click on the *Set Device Folder* button.
3. Check the *Set device folder* radio button and the desired folder name to move the devices to from the list of device folders, and then, click *OK*.

(Device folder names can be used later to filter devices from a long list of devices in the inventory.)

Scenario 1
Verifying Device Attributes



Verifying Device Attributes

As just seen, the devices that are in the QPM inventory can be viewed along with their attributes and interfaces using the *Device Table* in QPM.

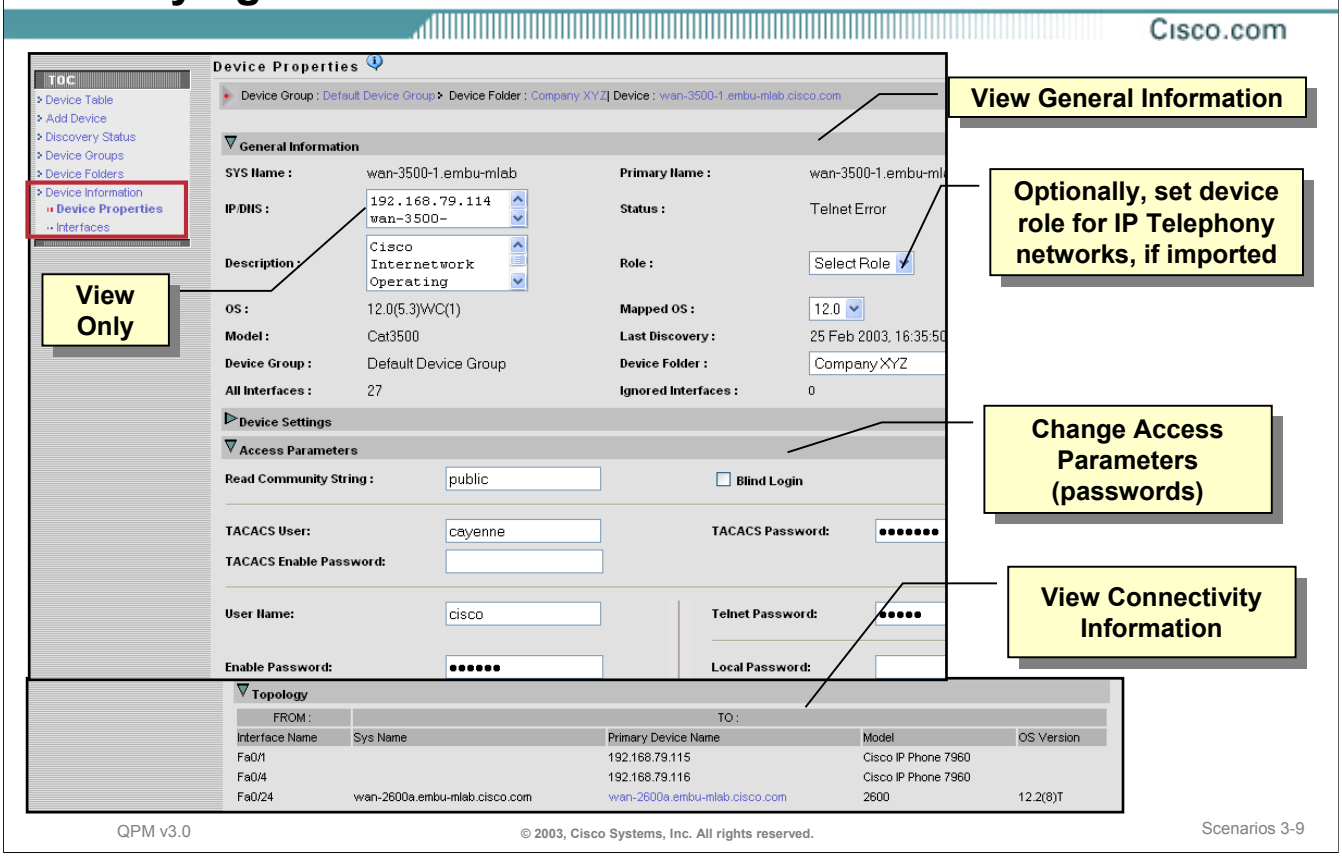
After a device is added, manually or imported, the passwords (i.e. Telnet, TACACS+, and SNMP read community string) for the device are verified and the attributes are gathered, if possible. If the passwords are incorrect, the Status column in the Device Table will indicate the potential problem.

Note, that if devices are imported from RME, the passwords are also imported and if the passwords change in RME, QPM and RME can be synchronized using a task located under the QPM *Admin* tab.

As illustrated in the Device Table, QPM uses the device model type and operating system (OS) version number to load device capabilities into the inventory. All subversions of a certain version are translated or mapped to a major version, unless QPM explicitly supports the minor version.

To change any attributes for a device, click on the device name in the Sys Name column, or check the devices to edit and click the *Edit* button. Let's look at these attributes now.

Scenario 1
Verifying Device Attributes



QPM v3.0 Scenarios 3-9

Verifying Device Attributes

To verify or modify some attributes of a device, select the device name from the Device Table. Notice that additional entries, such as *Device Properties* and *Interfaces*, will appear in the TOC navigation pane when the Device Properties window appears.

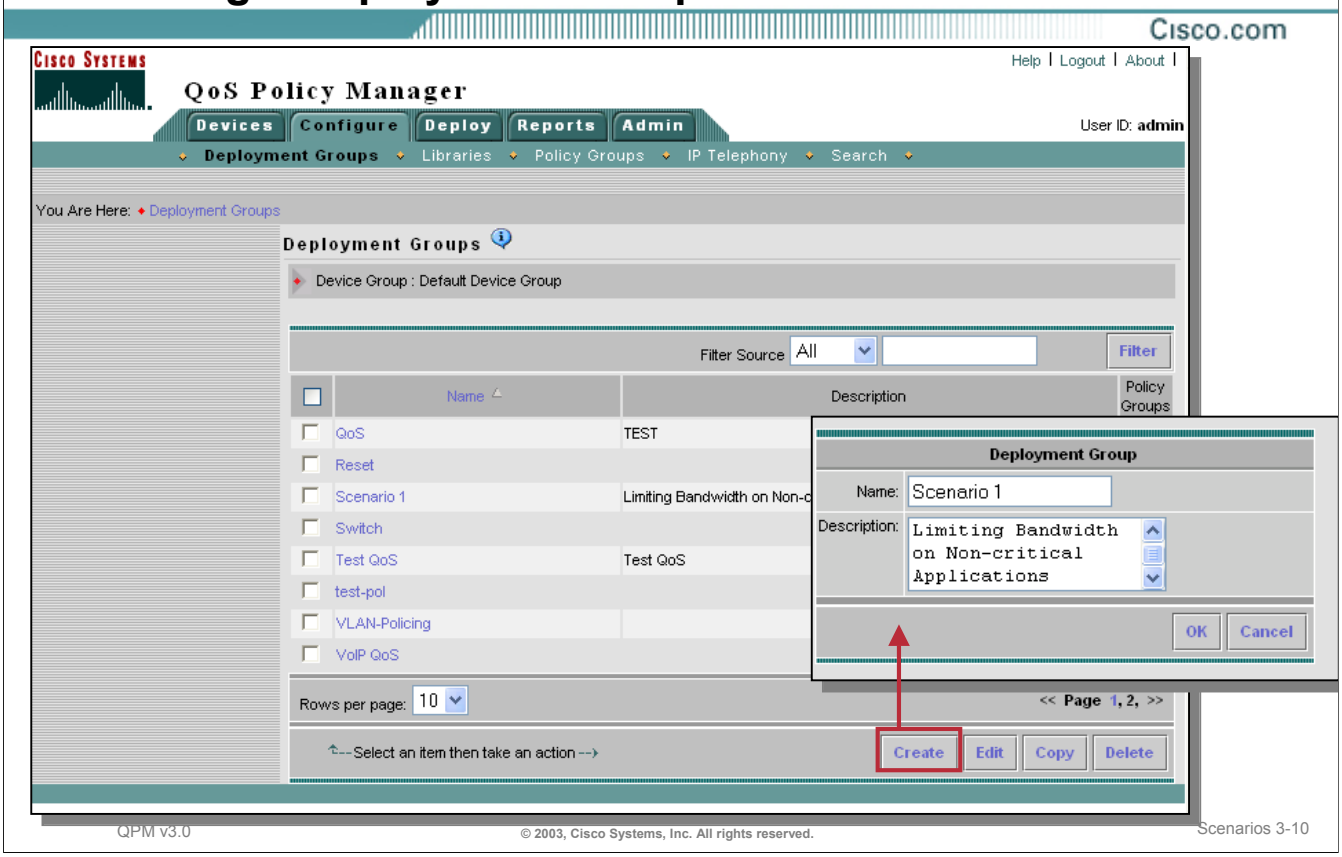
The Device Properties window is broken down into separate sections: General Information, Device Settings, Access Parameters, ACL Ranges, and Topology. Each of these sections are described below:

- *General Information* – Device attributes such as Sys Name, IP address, IOS version number, and device type can be viewed from this section. Notice that some fields are editable.

  If multiple IP addresses have been defined on the device, these addresses can be viewed (but not modified) in the IP/DNS field.

  (Though not needed for this scenario, the *device role* for the device can be set by selecting the appropriate device role from the pull-down menu. A device role is a device property that specifies the network point (refer to Chapter 2) for a device in the AVVID network. As seen in Scenario 3, a device role might identify a device as a campus access, campus distribution, or WAN aggregation point. Device roles are used by the IP Telephony wizard to help automatically identify which interfaces should be assigned to which policies. To import device roles using a text file, select *Device > Options.)*
- *Device Settings* – Provides options to allow users to write to memory, create access control policies, and enable NBAR port mappings.
- *Access Parameters* - If the device passwords (SNMP read community string, TACACS, Telnet, local or enable passwords) need changing, go to this section.
- *ACL Ranges* – Use this section to define ACL ranges used to translate QPM policies to CLI command. Note that only extended ACLs are supported in QPM.
- *Topology* – Use this section to easily view neighboring Cisco devices and which interfaces they are connected to if the Cisco Discovery Protocol is supported and enabled on the devices.

Scenario 1
Creating a Deployment Group



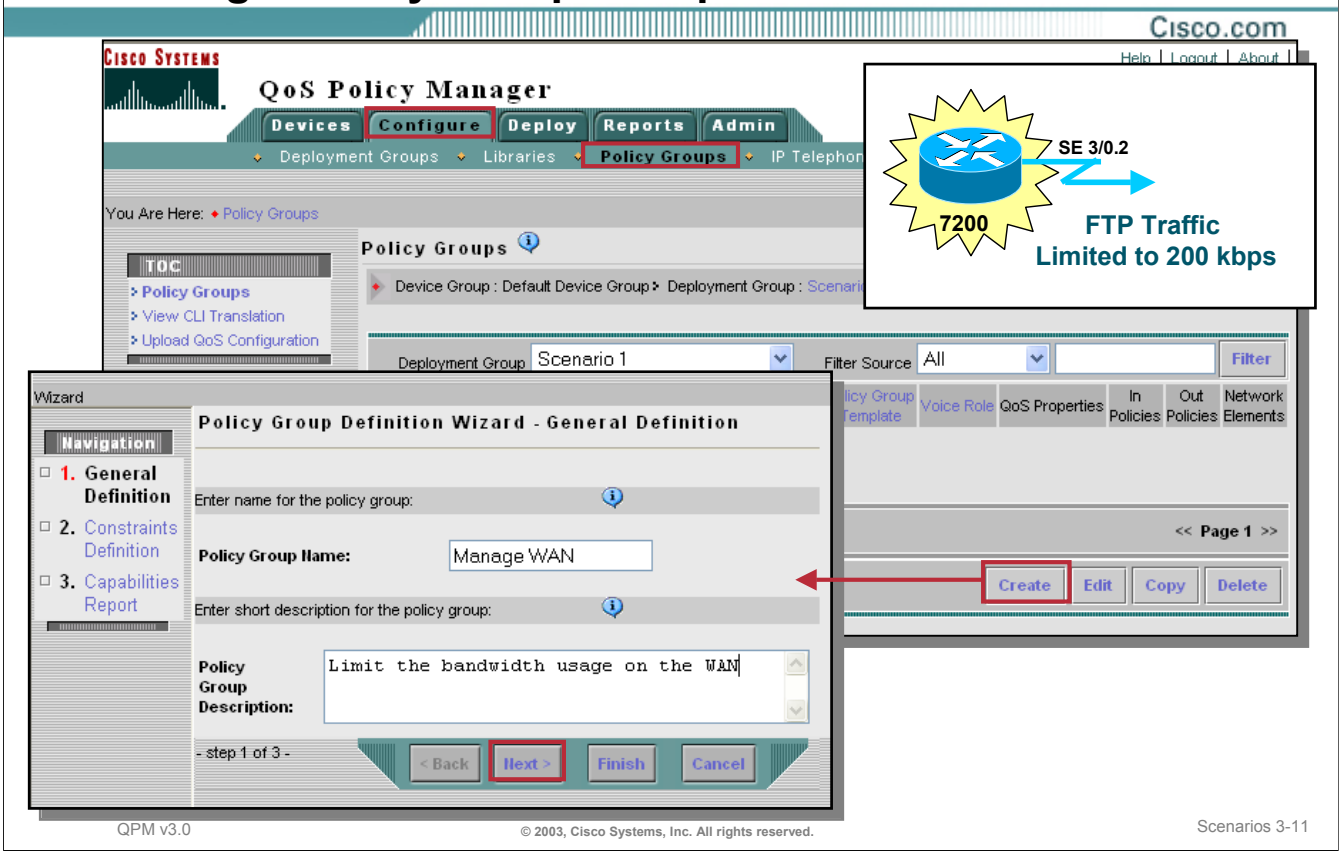
Creating a Deployment Group

Since ACS is not used for user authorization in these scenarios, there exists only the single QPM Default Device Group. All devices will belong to this group and it is, by default, defined as the active device group. Deployment groups can now be created for the active device group. Let's create a deployment group, define a policy group, and define the QoS policies that will be used to limit the WAN bandwidth for FTP. To create a new deployment group, follow these steps:

1. Select *Configure* > *Deployment* Groups. A list of deployment groups previously defined for the active device group are listed.
2. Click the *Create* button to define a new deployment group.
3. Enter a name and description for the new deployment group. Click *OK* when done.
4. The new deployment group should appear in the list. Policy groups can now be defined for the deployment group by either selecting the *Policy Groups* icon in the row associated for that deployment group or by following the step illustrated next.

TIP: Remember that the deployment group can contain multiple policy groups; each of these policy groups can contain multiple QoS policies assigned to the network elements in the device group. You can create and manage multiple deployment groups for phased deployment, or for testing what-if scenarios.

Scenario 1
Creating a Policy Group – Step 1



QPM v3.0 Scenarios 3-11

Creating a Policy Group – Step 1

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. Thus, QPM lets you define only QoS properties and policies that are supported by the device constraints specified for the policy group.

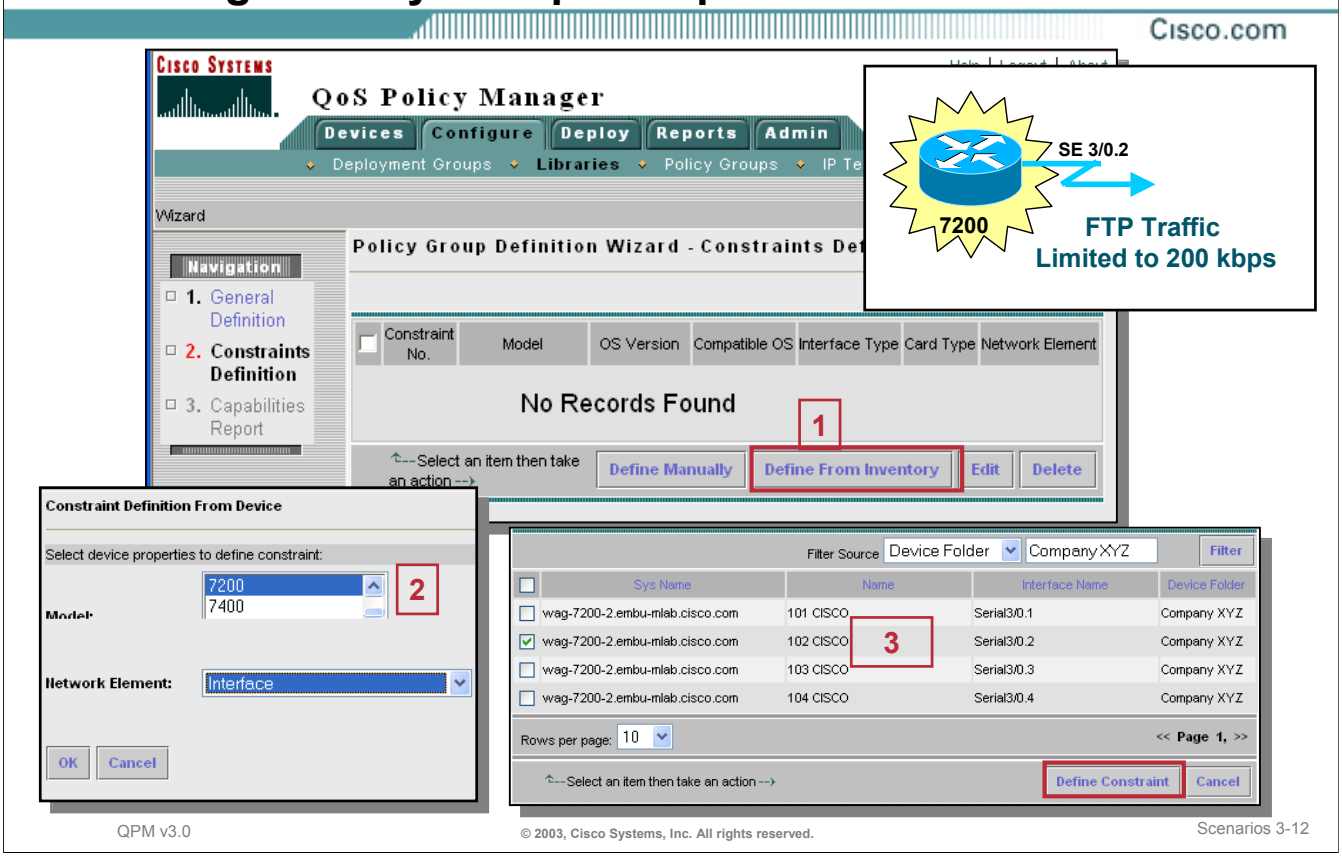
The general setup for a policy group consists of 3 steps:

- Providing a policy group name and description
- Defining the constraints for the group
- Viewing the capabilities for the group

To create a new policy group, follow these steps:

1. Select *Configure* > *Policy Groups*. (Or from the previous illustration, select the *Policy Group* icon from the list of deployment groups.)
2. If not correctly set, select a Deployment Group from the pull-down menu to define where this policy group is to be saved. A list of previously defined policy groups and their settings for the selected development group are listed.
3. To create a new policy group, select the *Create* button.
4. Enter a name and short description for the policy group.
5. Click *Next* to define the device constraints for the policy group.

Scenario 1
Creating a Policy Group – Step 2



Creating a Policy Group – Step 2

The second step to creating a new policy group is to define the constraints for the group. 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. Constraints can be defined by device model, OS type and version, interface type, card type, and network element type (device, interface, sub-interface, and so on). You can define multiple device constraints in a policy group, but they must all be for the same network element type.

To define the device constraints for the policy group, follow the steps below:

1. After entering a name and short description for the policy group, proceed to the next step, *Constraints Definition*, in the navigation menu. Select either *Define Manually* or *Define From Inventory* to specify a new device constraint. If you choose *Define From Inventory*, then only those device models, OS types and versions, and interfaces that exist in the QPM inventory will be available for selection.
2. Select the device model constraint (e.g. 2600, 4500, 7200, etc.). In this scenario, the only device that will be monitoring and limiting the non-critical traffic bandwidth usage is the Cisco 7200. Therefore, select only 7200 device models.
3. Select the network element constraint (e.g. device, VLAN, interface, DLCI, etc.). In this scenario, all policies will be assigned to interfaces. *Note that you cannot change the network element type after it has been defined for the first device constraint in the policy group*.
4. If defining the device constraint from the devices in the inventory, a list of devices in the inventory that match the device model and network element is displayed. Select the device and interface matching the one in the scenario (i.e. wag-7200 Serial 3/0.2). From this selection, QPM can determine the OS version, interface type, and card type constraints.
5. Click the *Define Constraint* button when finished.

Scenario 1
Creating a Policy Group – Step 3

Creating a Policy Group – Step 3

After you have defined the device constraints for the policies within the policy group, view the Capabilities Report. The Capabilities Report displays the QoS capabilities that can be supported for the policy group (common capabilities listed under the capabilities summary column) and for each device constraint defined. In this scenario, only one device constraint was defined, but if the policy is going to be applied to multiple devices with different attributes then multiple device constraints would need to be defined. If you have defined two device constraints based on two different device model numbers in the previous step, then both device models must support the QoS feature in order for the policies within the group to contain that QoS feature.

To view the Capabilities Report for a policy group, follow either of these steps:

1. Select the *Capabilities Report* from the navigation menu after defining the device constraints, as illustrated above.
2. Or, from *Configure* > *Policy Groups*, select a policy group for editing, then click on *Device Constraints* from the navigation window. Select the *Capabilities Report* button at the bottom of the window.

Scenario 1
Define the QoS Properties for the Policy Group

Cisco.com

Defining the QoS Properties for the Policy Group

After defining the general information for the policy group, the QoS Properties for the policy group should be reviewed and modified, if needed. The QoS Property settings, as well as the device constraints, will affect which QoS features will be available when you are ready to define the inbound and outbound policies. A policy group's QoS properties and mappings apply to *all flows* passing through the interface. Whereas, the action of a QoS policy only applies to the traffic matching the filters defined.

Note: QoS properties include scheduling properties (queuing technique), 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.

To review the QoS Properties for the policy group, follow these steps:

1. If not already at the Policy Group main navigation menu, then select *Configure* > *Policy Groups*, select the deployment group, select the checkbox next to the name of the policy group, and then click *Edit*.
2. From the navigation menu for a selected policy group, select *QoS Properties*. The current settings are displayed.
3. For this scenario, there is no need to change the QoS Properties. We will leave the queuing technique at the interfaces default to the scheduling method already defined for the device and all other QoS properties, such as compressed RTP, RSVP, etc., are not needed for this scenario.

Scenario 1
Defining the Outbound Policies – Step 1

Cisco.com

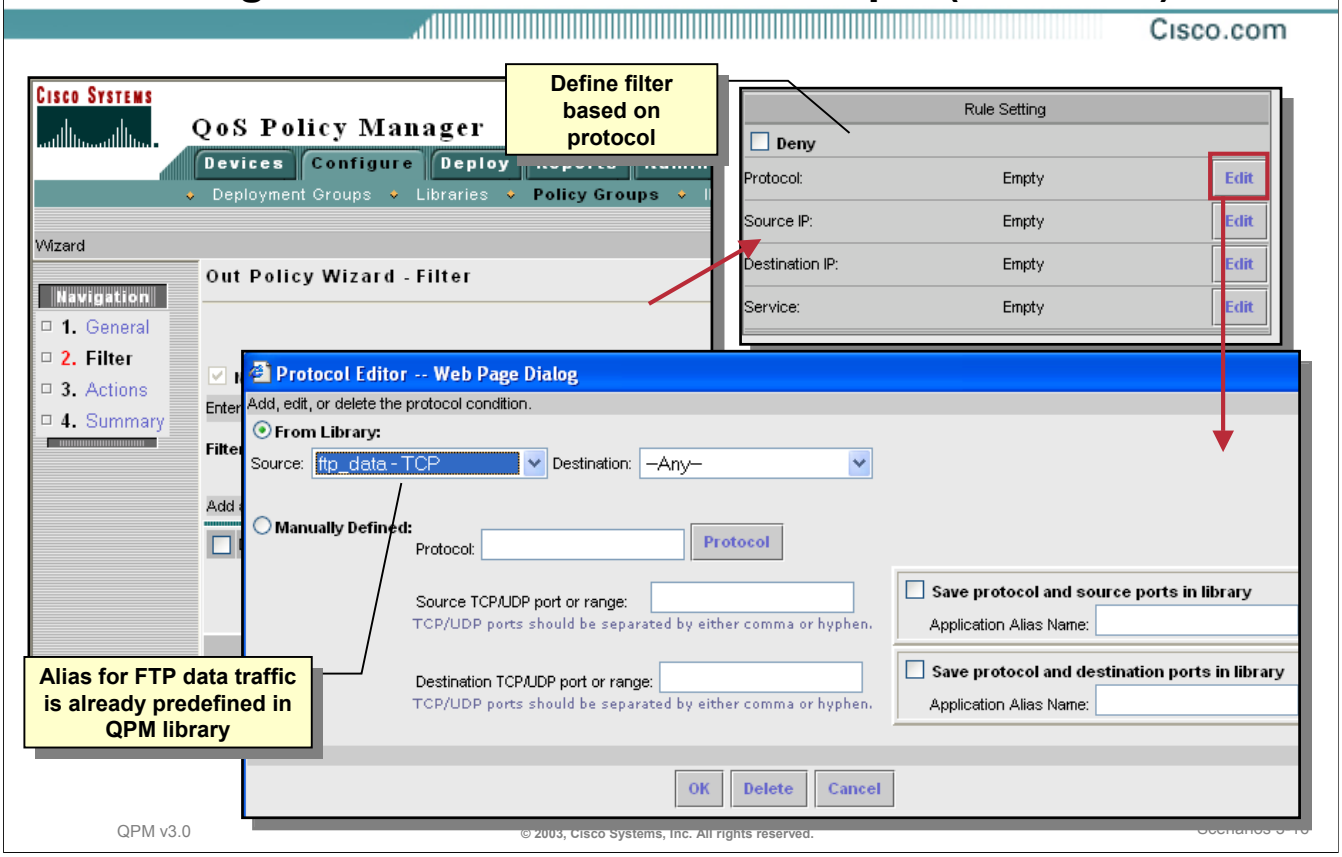
Defining the Outbound Policies – Step 1

Reflecting back to Chapter 2 and the workflow for using QPM, we are now ready to define the limiting policy on the outbound WAN interface of the Cisco 7200. The policy will restrict FTP traffic to 200 Kbps. If exceeded, the traffic will be dropped. To define the policy, follow these steps:

1. From the navigation window for the selected policy group, select *Out Policies*. A list of current outbound policies will be displayed, if any exist.
2. Click the *Create* button to define a new policy. A 4-step wizard appears.
3. Enter a name for the new policy (e.g. Limit FTP Traffic) and a short description.
4. Set the type of policy to QoS Policy. (QoS policies define an action to be taken; whereas, Access Control policies either permit or deny traffic matching a filter.)
5. Click *Next* to define the policy filter.

Scenario 1

Defining the Outbound Policies – Step 2 (The Filter)



Defining the Outbound Policies – Step 2 (The Filter)

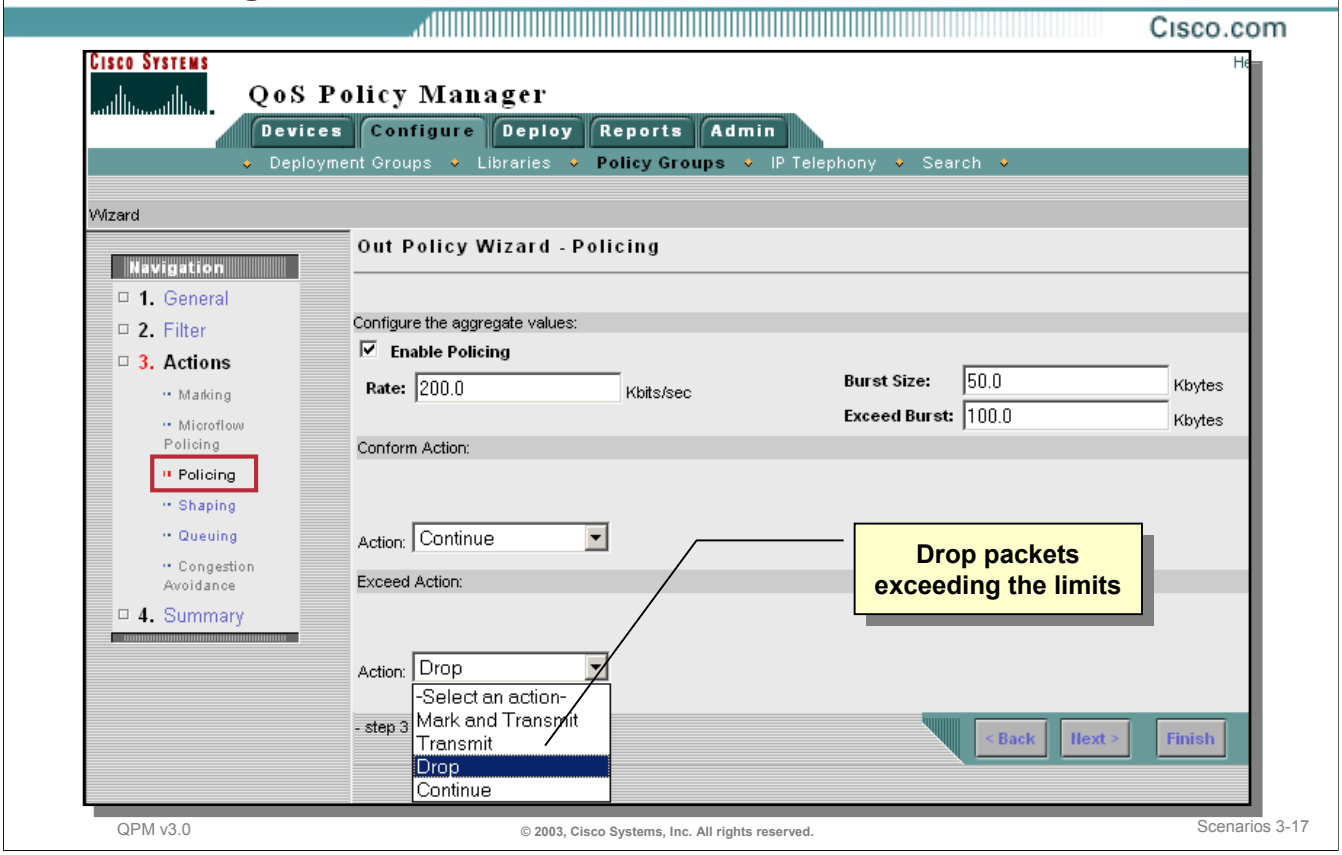
Next define the filter for the policy. All outbound traffic matching the filter will be subjected to the policy action, defined next.

1. The wizard should have proceeded to the Out Policy Wizard - Filter page.
2. Select the radio button, *Create a new filter*. (The other radio button, *Class Default*, defines a catch all policy for packets that do not match the filters.)
3. Optionally, provide a filter name. This is helpful for viewing CLI translations later.
4. Click the *Create* button at the bottom to define the filter.
5. Configure the filter to look for all FTP-Data traffic. In the Rule Settings window, edit the Protocol filter definition.
6. QPM has a large library of well-known protocol definitions. From the Source pull-down menu, select *ftp_data –TCP*. This will match all ftp-data. Click *OK* when done.

Note, you may also want to filter by the Source IP address if you want to only limit traffic let's say from the server farm. If so, also edit the Source IP filter definition in the Rule Settings window.

Scenario 1

Defining the Outbound Policies – Step 3 (The Action)

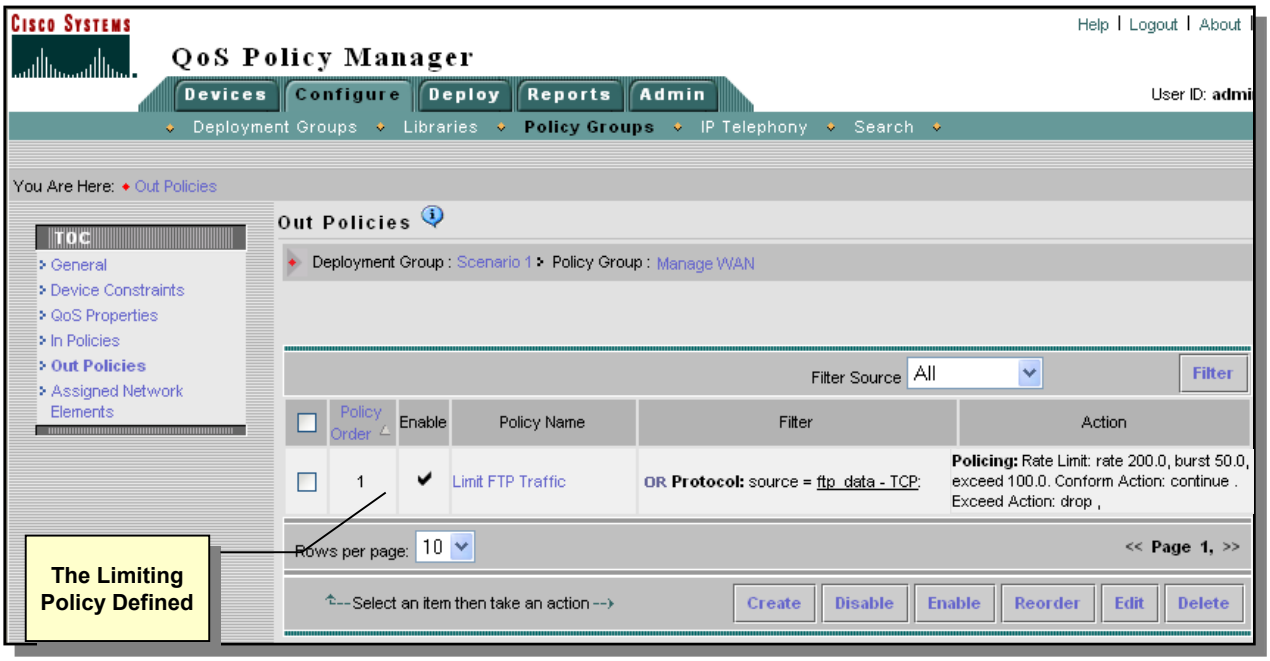


Defining the Outbound Policies – Step 3 (The Action)

Finally define the action to be applied. All outbound traffic matching the filter will be subjected to this policy action.

1. The wizard should have proceeded to the Out Policy Wizard - *Actions* page. Depending upon the results of the Capabilities Report (limited by the device constraints defined) and the QoS Property settings for the policy group, only some actions will be available for selection. QPM helps you determine what is a valid action depending upon these settings.
2. In this scenario, we will police (or limit) traffic matching the filter ftp_data. Select the Policing action from the navigation window to define the values.
3. Check the *Enable Policing* checkbox.
4. Set the rate to 200 Kbps.
5. Set the burst size to 50 Kbytes. Burst size is 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.
6. Set the exceed burst to 100 Kbytes. The exceed burst is 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.
7. Set the Conform Action to *Continue*. Those packets that conform to this rate, will continue to the next policy, if any.
8. Set the Exceed Action to *Drop*. Those packets exceeding this rate, will be dropped. (Scenario #2 will modify this policy to queue the traffic instead of dropping the packets.)
9. Click *Next* or *Finish* when done.

Scenario 1
The Policy Defined



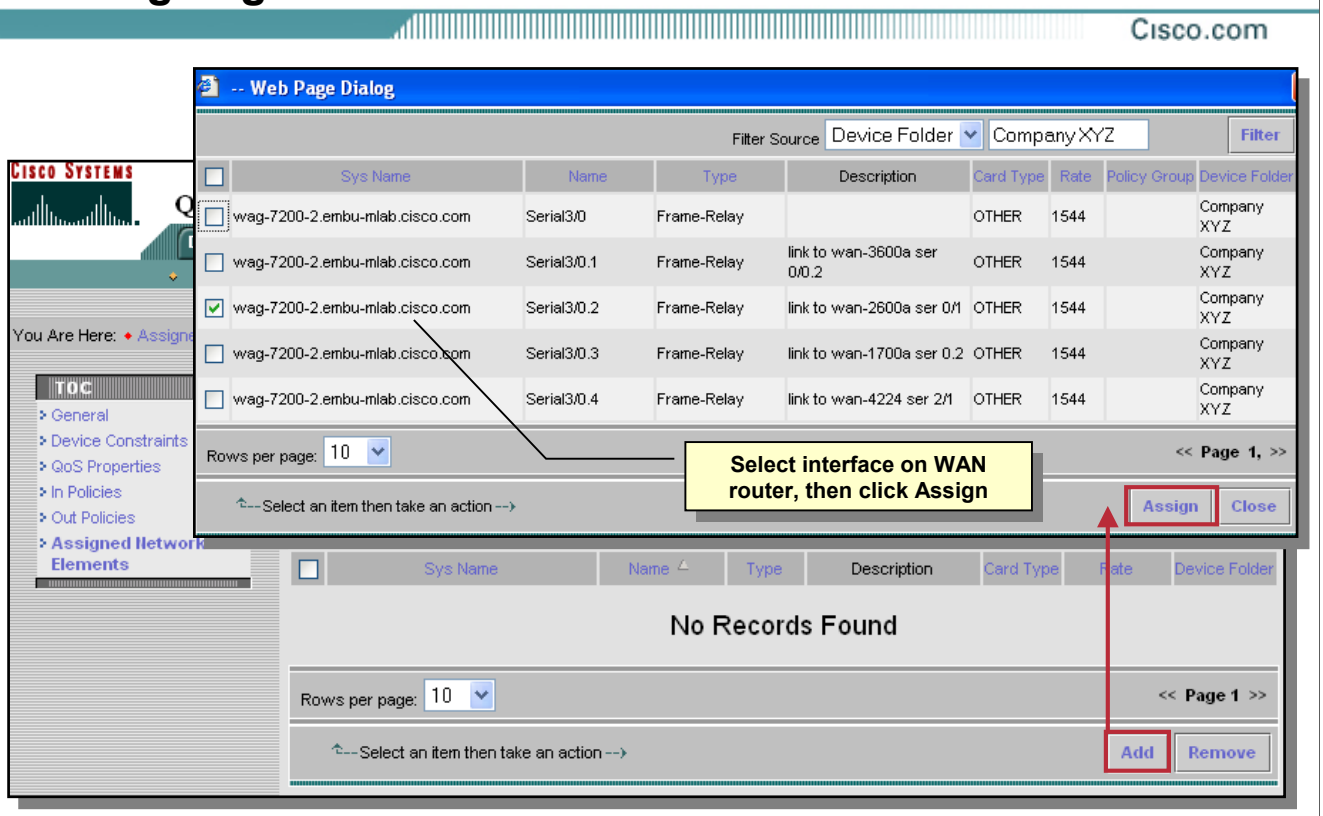
The Policy Defined

After the filters and actions have been defined and reviewed, the policy is saved in the selected Policy Group. In this scenario, a summary of the policy just defined is listed in the table for the Out Policies. Review the filter and action definitions to ensure that it meets your intentions. If not, select the checkbox next to the policy to change and click the *Edit* button.

Ensure that the policy is enabled. Policies can be disabled and enabled by selecting the checkbox next to the policy and clicking the *Disable* or *Enable* button.

(In the next scenario, we will define multiple policies in the group. When multiple policies exist, the order of the policies is important. The device will process the policies from top to bottom.)

Scenario 1
Assigning Network Elements



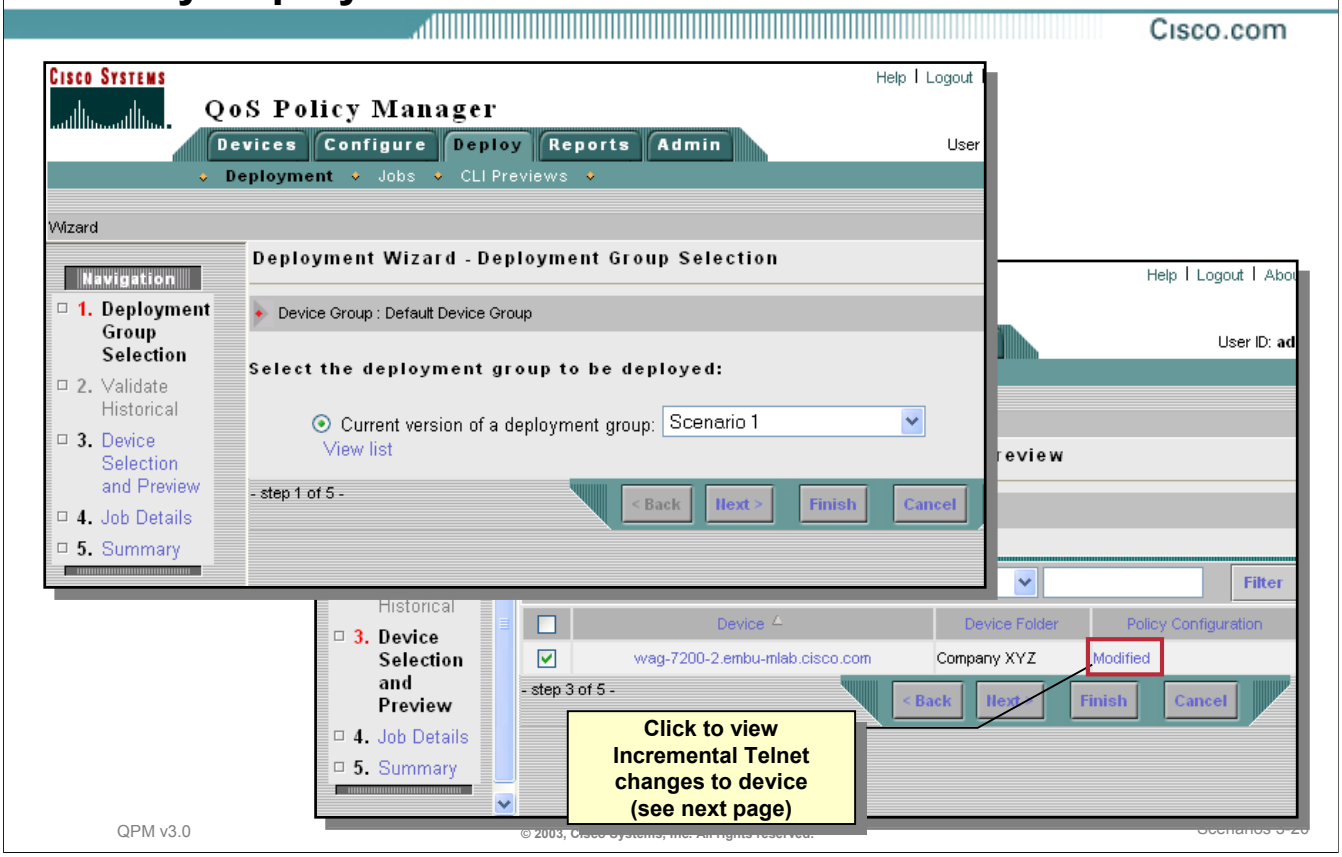
Assigning Network Elements

Network elements are the devices, interfaces, VLANs or DLCIs that the policies will be assigned to. The type of network elements that are available for selection are restricted by the device constraints defined earlier for the policy group. Assigning the network elements could be conducted before or after defining the QoS policies in the group even though it is illustrated as the last entry in the TOC window.

To assign the network elements to the policy group, follow these steps:

1. From the TOC window for the selected policy group, select *Assigned Network Elements*. In our scenario, no network elements (interfaces) have been assigned to the policy group.
2. To assign the Cisco 7200 Serial3/0.2 interface to this policy group, click the *Add* button.
3. QPM will display a list of network elements that match the device constraints for the policy group. Check the box next to the Cisco 7200 Serial3/0.2 interface and then click the *Assign* button to add this interface to the policy group.
4. The interface will now appear in the list of Assigned Network Elements.

Scenario 1
Policy Deployment

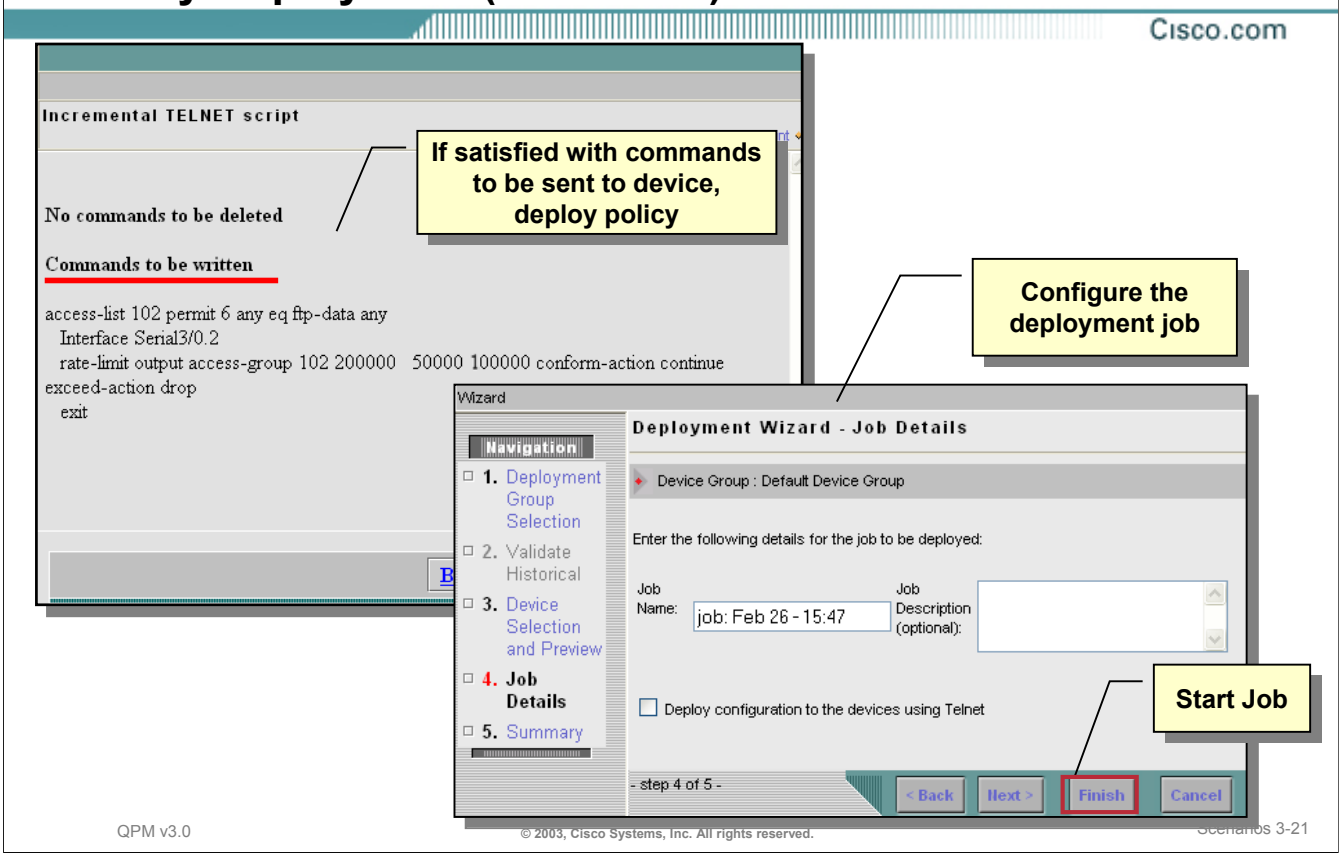


Policy Deployment

Reflecting back to Chapter 2 and the workflow for using QPM, we are now ready to deploy the policies in the deployment group. Follow these steps to deploy your policy to limit FTP traffic on the WAN interface:

1. From the main tabs in QPM, select *Deploy* > *Deployment*. The 5-step Deployment Wizard appears.
2. Select the deployment group to be deployed by selecting the radio button, "*Current version of a deployment group*", and then select the deployment group name from the pull-down menu. (The other radio button can be used to restore policies based on historical copies of the deployment process.)
3. Click *Next* to proceed to the next step in the Deployment Wizard, which is selecting the devices to deploy the policies to.
4. Only the devices whose network elements were assigned to the policy group are listed for selection. Ensure that the checkbox next to the Cisco 7200 device is checked.
5. In the table, select the *Modified* link in the Policy Configuration column to preview the Incremental Telnet command that will be sent to the device. (Refer to next illustration.)

Scenario 1
Policy Deployment (continued)



Policy Deployment (continued)

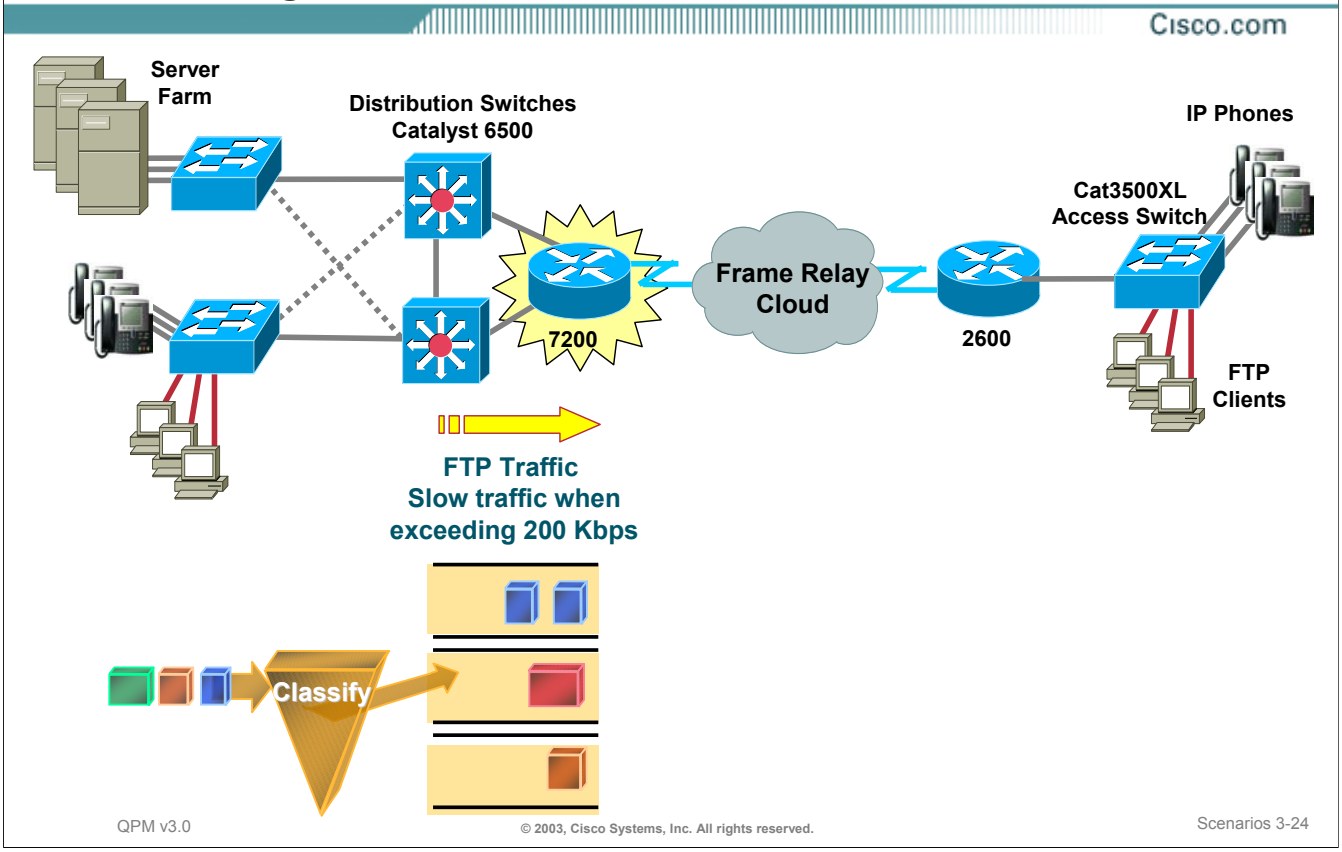
6. Review the commands that would be written (or deleted) to (or from) the selected device.
7. If satisfied with the configuration changes, close the window.
8. From the Device Selection window, click *Next* to build the job. The Job Details window appears.
9. Enter a meaningful Job name (or accept the default name) and optionally a short description.
10. To deploy the configuration using Telnet, mark the checkbox. In this scenario, we will not send the changes to the devices, but simply build a device configuration file that can be downloaded manually to the device later. To build new device configuration file, leave the box unchecked.
11. Click *Finish* to start the deployment job.
12. When needed, you can download the device configuration file(s) as a single zip file to your desktop, by clicking the *Files* icon in the Job History report.

This page intentionally left blank.

Scenario 2

Prioritizing Traffic

Scenario 2
Prioritizing Traffic



Scenario 2 - Prioritizing Traffic

In the previous scenario, FTP traffic was limited to 200Kbps across the WAN. If the FTP traffic exceeded this limit, the packets were dropped.

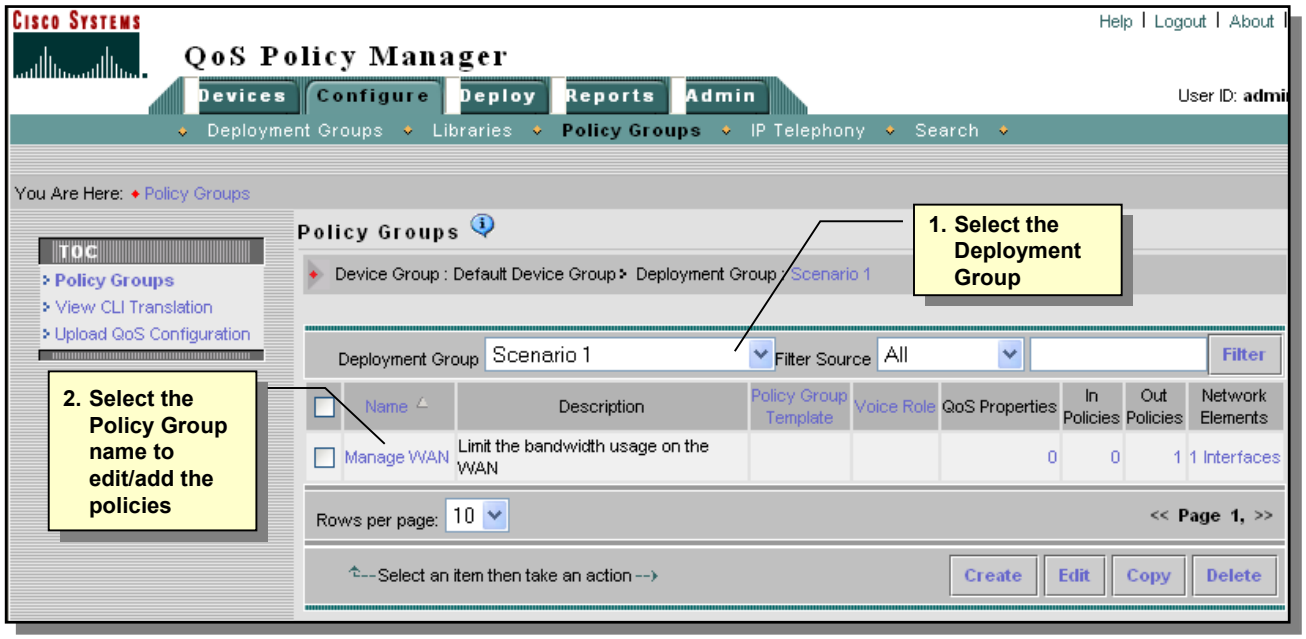
Now let's modify this policy to queue the packets exceeding this rate by first marking the packets exceeding the rate, using Advanced Coloring available with CAR (Committed Access Rate) which is available in IOS release 11.1cc, 12.0, or later, and then queuing the marked packets for transmission if bandwidth is available.

The traffic filter will remain the same - all FTP traffic (TCP 20). However, the policy's action will change. Instead of automatically dropping packets after exceeding 200 Kbps, now color the packets which exceed this threshold. On the outbound WAN interface, packets which exceed the threshold will be placed in a low priority queue. All other traffic will be placed in a normal priority queue. Therefore, FTP data coming from the server which exceeds 200 Kbps will not be dropped; it will be delayed. Two policies will be needed to define this requirement.

For this scenario, we will need to first define a queue on the serial interface of WAN 7200 router. We will used Priority Queuing as the queuing mechanism.

Scenario 2
Changing the Policy Group

Cisco.com



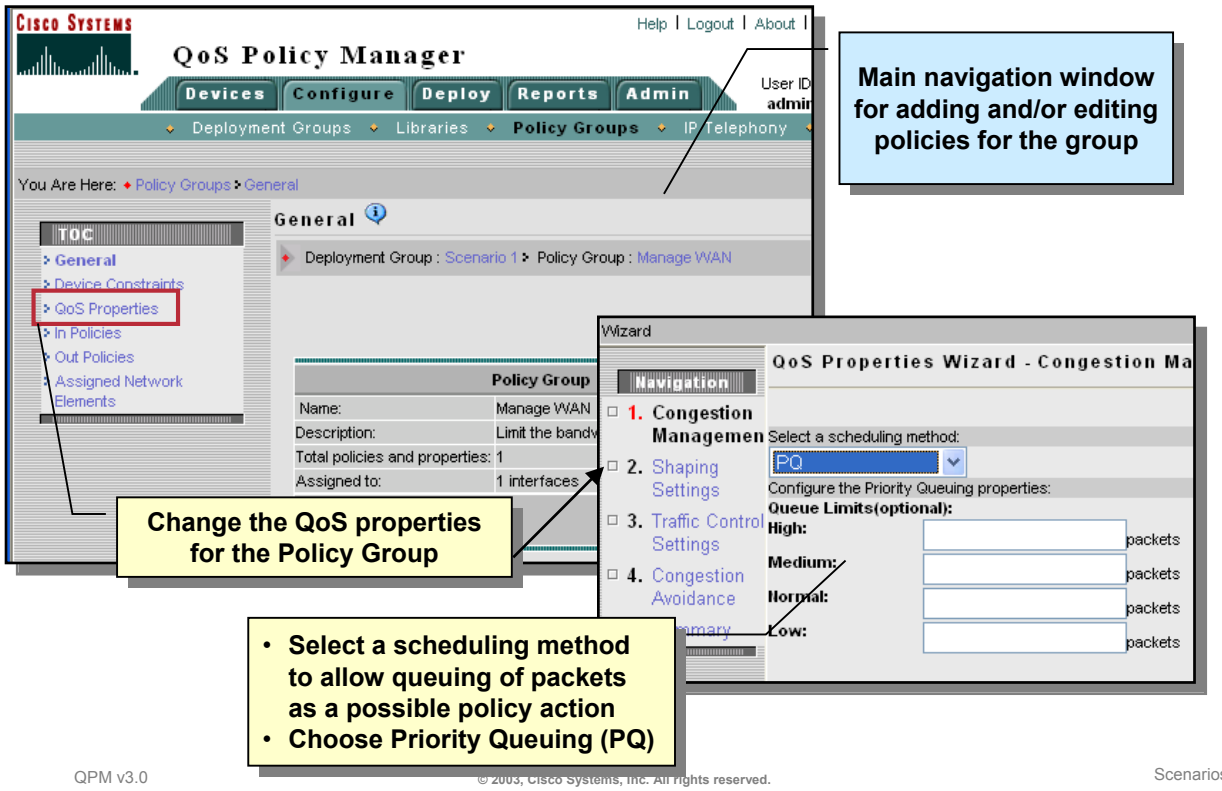
Changing the Policy Group

To implement this policy change, we will need to modify the existing policy so that it colors the packets and does not drop them. In addition, a second policy will filter the colored packets and place them into a low priority queue.

To add the new policy and edit the existing policy within the policy group, follow these steps:

1. From QPM, select *Configure* > *Policy Groups* from the main tabs.
2. Using the pull-down menu, located and select the newly created Deployment Group that you are working with. The policy group that was created in the previous scenario should be listed.
3. We will now edit the policy group. Click on the policy group name to make changes to it.

Scenario 2
Editing the Policy Group – QoS Properties



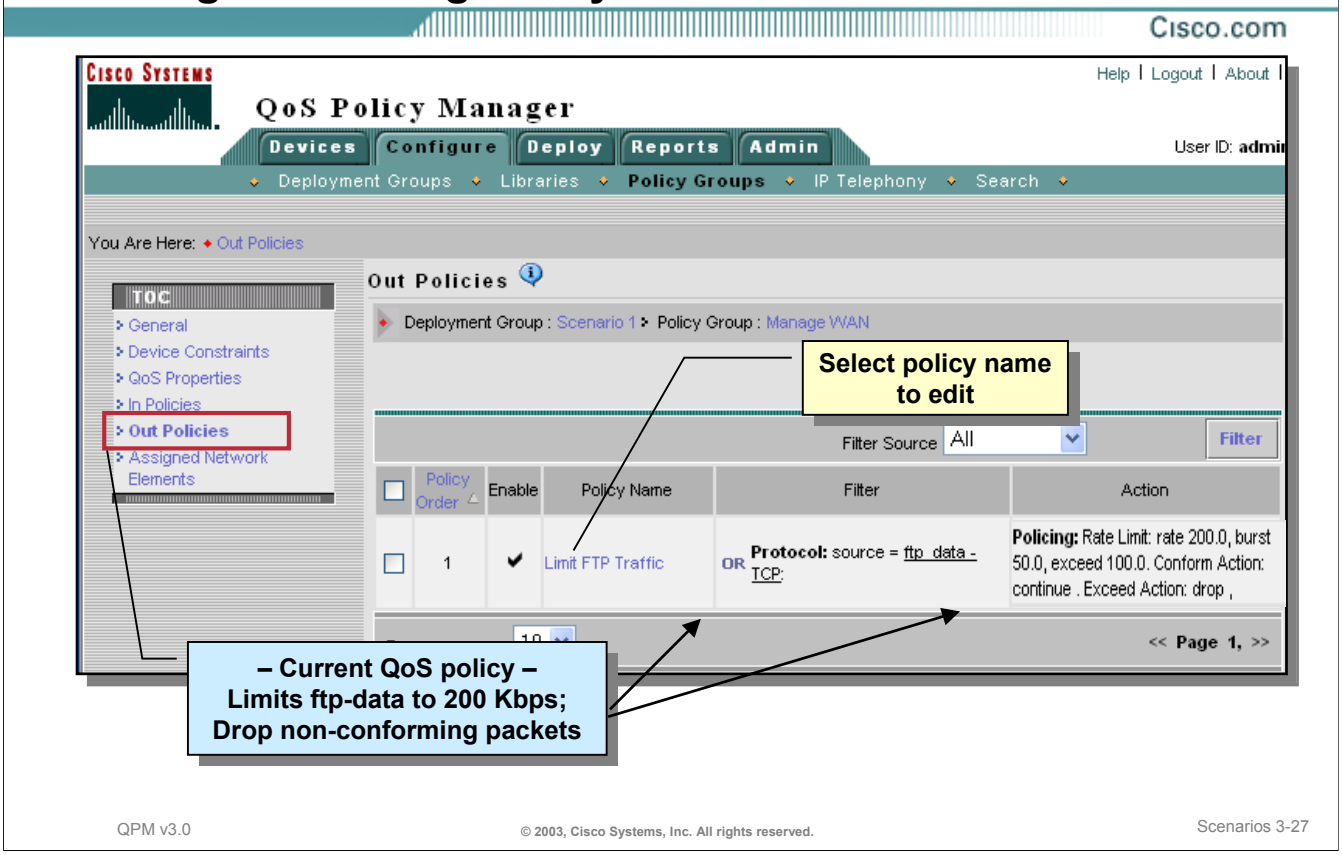
Editing the Policy Group – QoS Properties

Before we add a new policy and edit the existing one, we will first modify the QoS Properties for the policy group by changing the scheduling method. This in done in order for the policy group to have policies that provide queuing for congestion management.

Follow the steps below to set the scheduling method to Priority Queuing:

1. After selecting the policy group for editing, select *QoS Properties* from the TOC navigation sub-menu.
2. Click the *Edit* button to use the wizard to change the QoS Properties.
3. From the *Congestion Management* step in the wizard, change the scheduling method to *PQ* (Priority Queuing).
4. Optionally, you can set the maximum packets per queue.
5. None of the other QoS Properties require changing. Click *Finish* to review the QoS Property settings and begin changing the individual policies within the group.

Scenario 2
Editing an Existing Policy

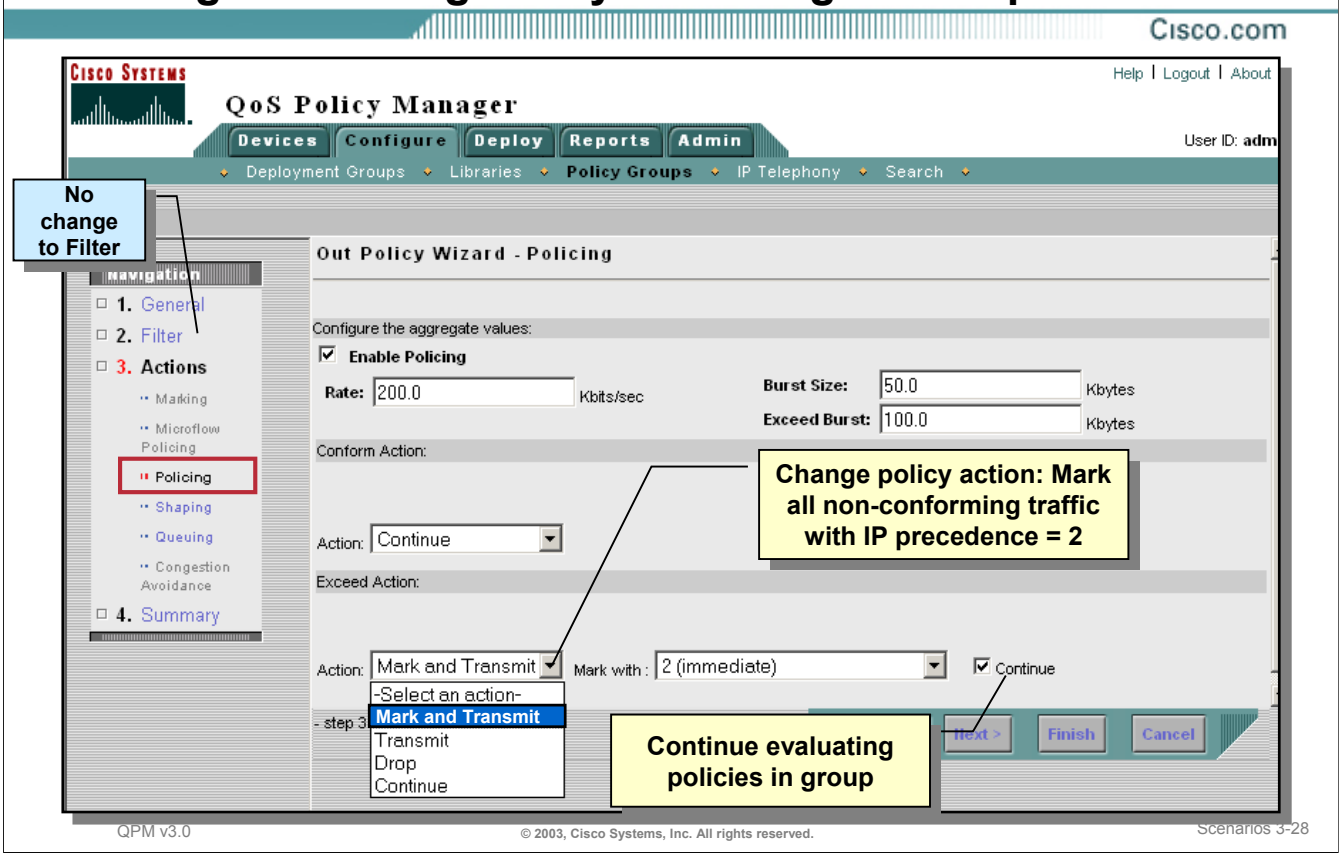


Editing an Existing Policy

Next, let's edit the existing QoS policy that was created in the previous scenario. This policy will be changed such that the policy will not drop packets exceeding the rate limit, but color them for further processing by another policy. To editing the existing policy, follow these steps:

1. This policy was set on an outbound network interface; therefore, select *Out Policies* from the TOC menu. You should see the current limiting FTP-data traffic policy.
2. To change the policy, select the policy name from the list. The general information, filter, and action settings for the policy will be displayed in the Policy Summary page.
3. Click the *Edit* button on the Policy Summary page to edit the filter and actions for the policy. (Refer to the next illustration.)

Scenario 2
Editing an Existing Policy – Limiting Technique

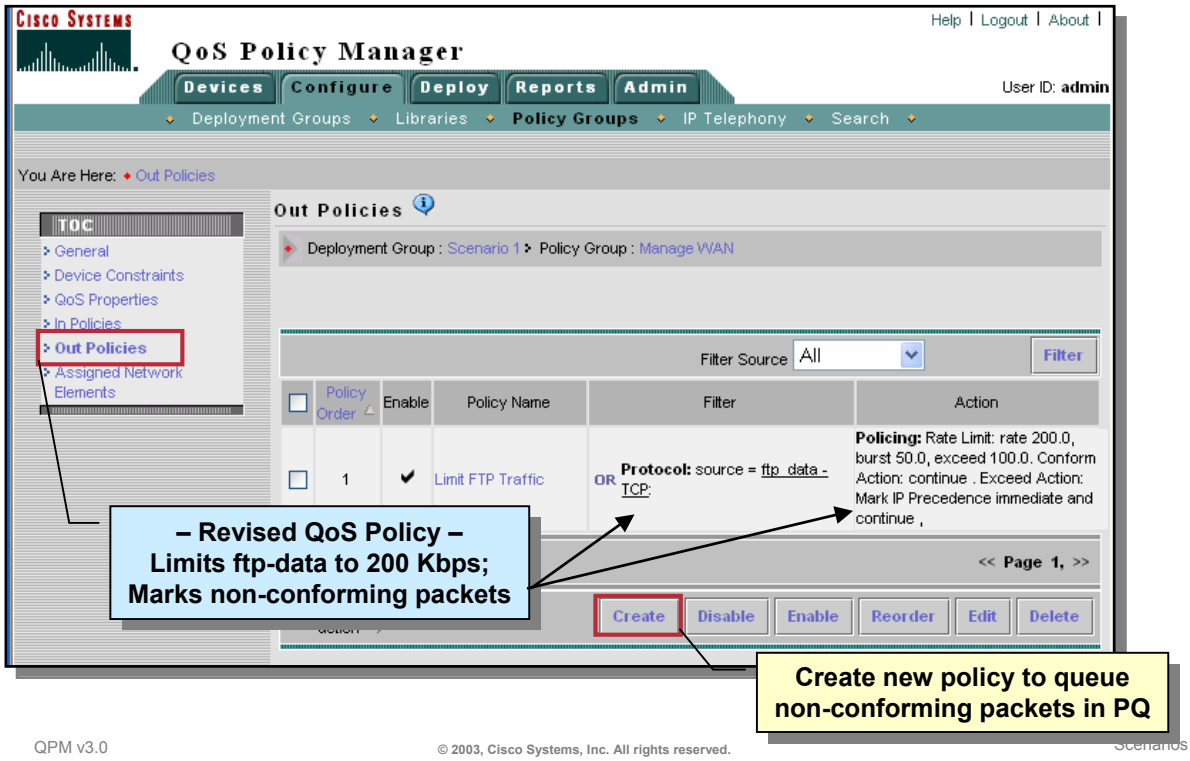


Editing an Existing Policy – Limiting Technique

Follow the steps below to change the policy's action for traffic matching the filter and exceeding the specified rate limit.

1. The General and Filter settings do not require changes; however, you may wish to change the short description for the policy.
2. Under the *Actions* settings, notice that additional types of actions are available since the QoS Property settings were changed.
3. Change the *Policing* (limiting) settings. Instead of dropping the packets exceeding the rate limit, let's color the packets and process them later. Under the Exceed Action section, select *Mark and Transmit* from the Action pull-down list.
4. Mark the packets exceeding the limit with an IP Precedence value of *2 (immediate)*.
5. Check the *Continue* checkbox. Checking this box tells the device to continue processing the packet with the next policy defined, if one exists. When a packet matches a policy, no further policies are evaluated unless the *Continue* statement exists.
6. We are now done with the changes. Click *Finish* to review the settings. Then click *Finish* in the Summary dialog.

Scenario 2
Adding a New Policy to the Policy Group

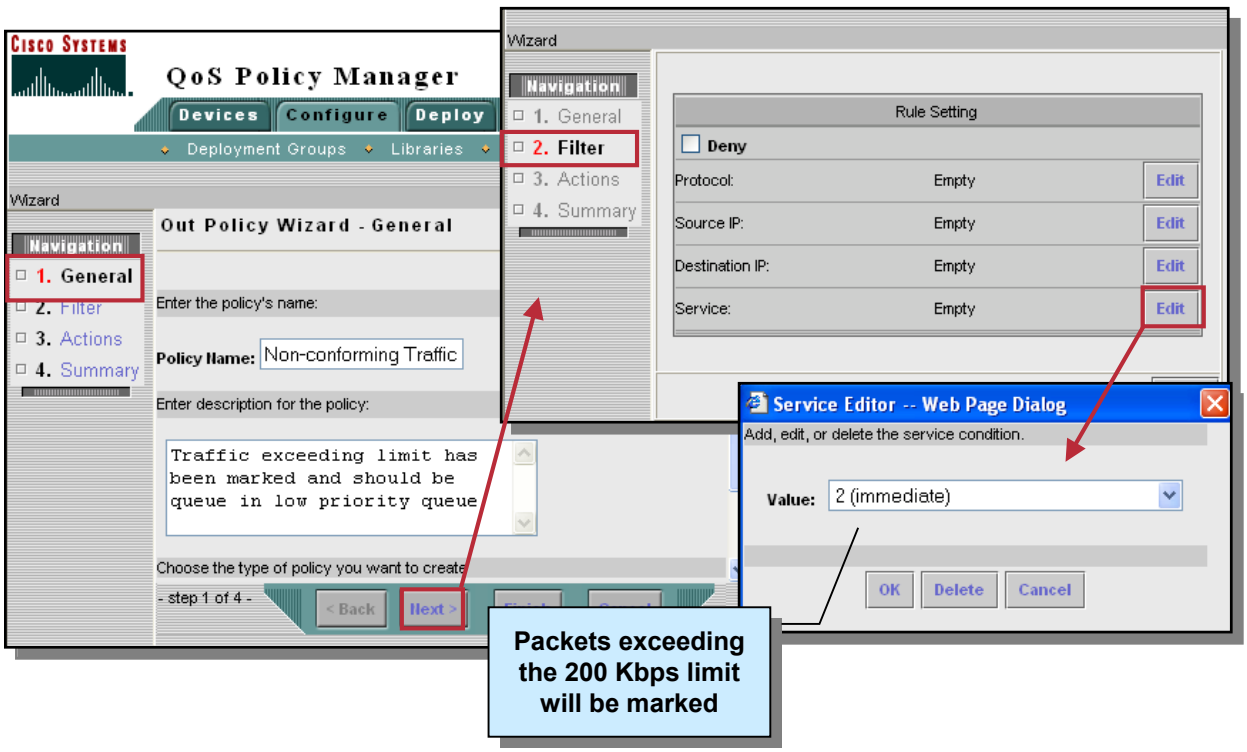


Adding a New Policy to the Policy Group

Follow the steps below to add another policy to the group to look for colored packets with IP Precedence equal to 2, indicating non-conforming ftp-data traffic, and queue the traffic in a low priority queue.

1. From the *Out Policies* page for the policy group, notice the changes to the existing policy. This policy now marks or colors the packets exceeding the rate limit instead of dropping them.
2. Click *Create* to define a new policy. You are now ready to define the general information, filters, and actions for the new policy. (Refer to the next illustration.)

Scenario 2
Adding a New Policy to the Policy Group – The Filter



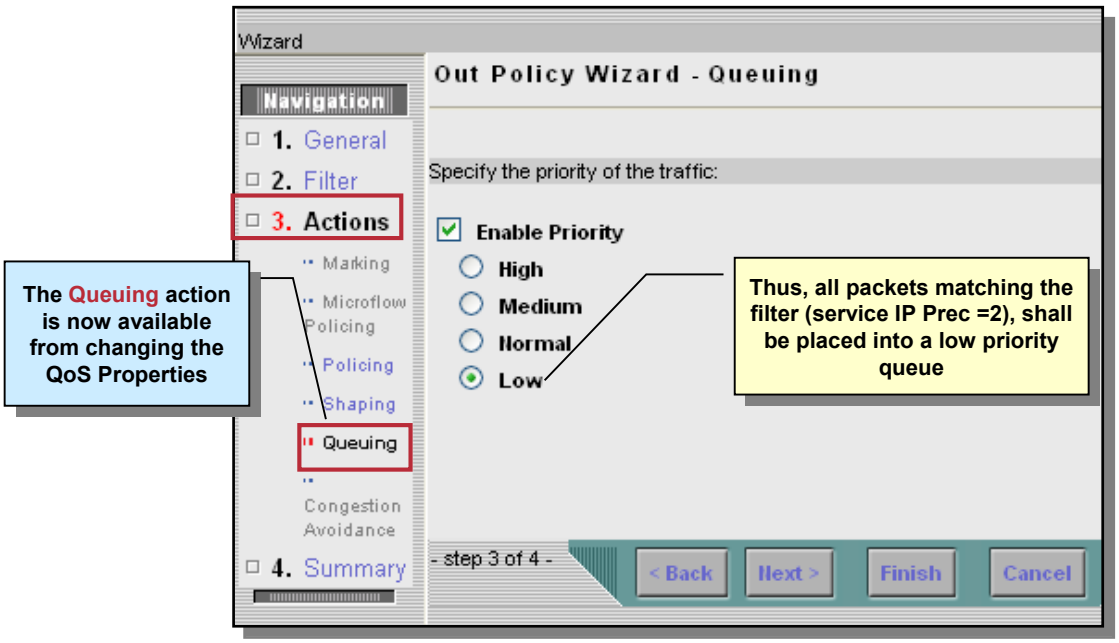
Adding a New Policy to the Policy Group – The Filter

Follow the steps below to create a new policy to filter traffic based on the IP precedence value. If the value is 2, the policy will apply the action, that is defined next.

1. In the General settings, provide a name and short description for the new policy. Then click *Next* to define the Filter.
2. From the Rule Settings dialog, edit the *Service* settings.
3. From the pull-down menu, select *2 (immediate)* and then click *OK*.
4. Click *Done* from the Rule Settings dialog to define the policy action.

Scenario 2
Adding a New Policy to the Policy Group – The Action

Cisco.com



Adding a New Policy to the Policy Group – The Action

Follow the steps below to create the policy action for packets matching the filter. If the packets match the filter just defined, then it can be assumed that the packet has been marked because it exceeded the rate limit for ftp-data traffic. The action will be to place these packets into a low priority queue. All other traffic will be transmitted first before transmitting the packets in this queue.

1. In the *Actions* settings, select *Queuing* from the actions available for selection.
2. Check the *Enable Priority* box.
3. Select *Low* to place the matching packets into a low priority queue.
4. Then click *Next* to review the policy definition and *Finish* to view the list of all policies defined for the group.

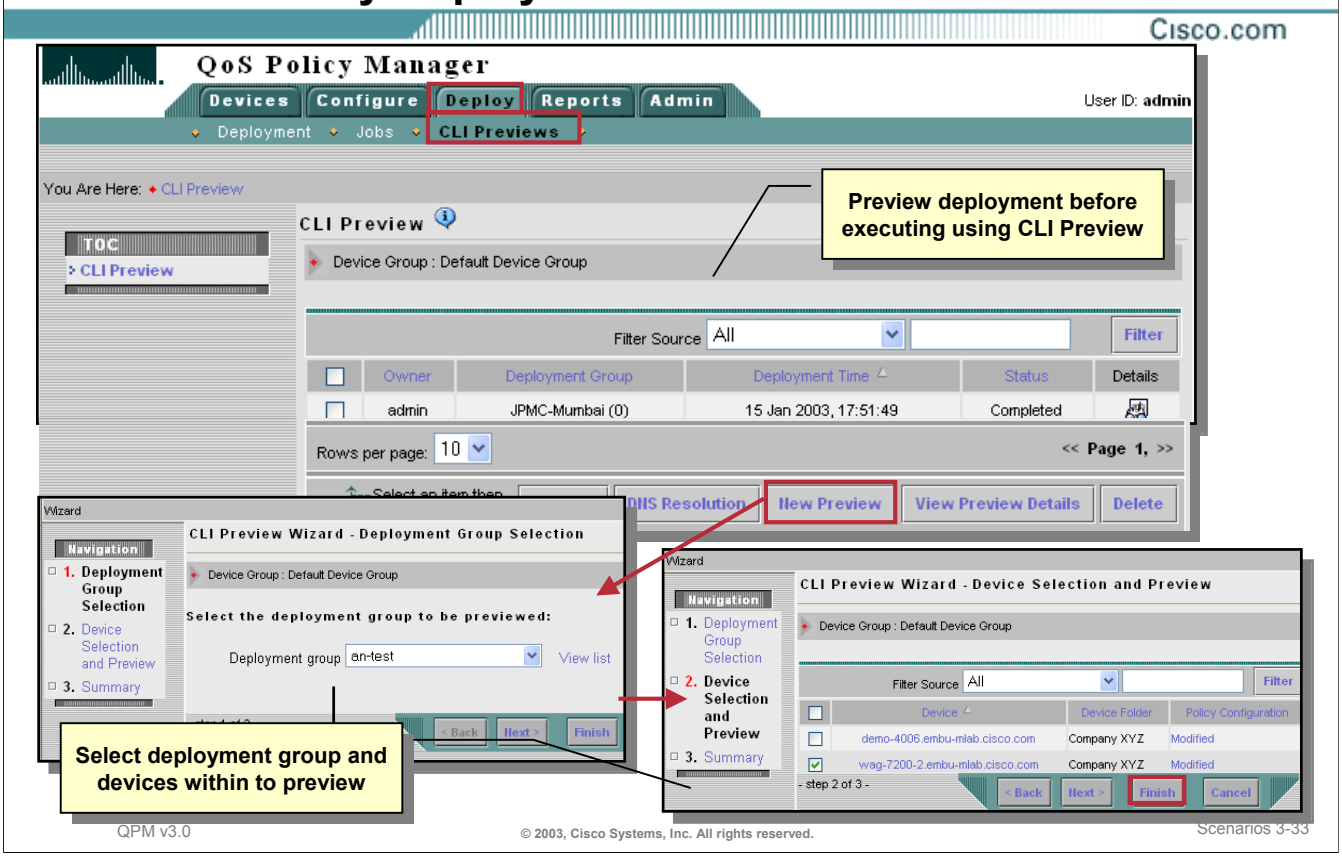
Scenario 2
Policies Defined for the Policy Group

Policies Defined For the Policy Group

Note that when the IOS software examines QoS policies, it examines them in order until a match is found. Even if a packet satisfies more than one policy, it will be treated as satisfying only the first policy that the device software encounters, unless you define your policy to include the *Continue* setting, in which case a subsequent match will be sought.

In QPM, the policies listed are examined top-down when configured on a device. To ensure policies get the priority you require, verify that your policies for an interface are in order of importance, from top to bottom. 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.

Scenario 2
Preview Policy Deployment



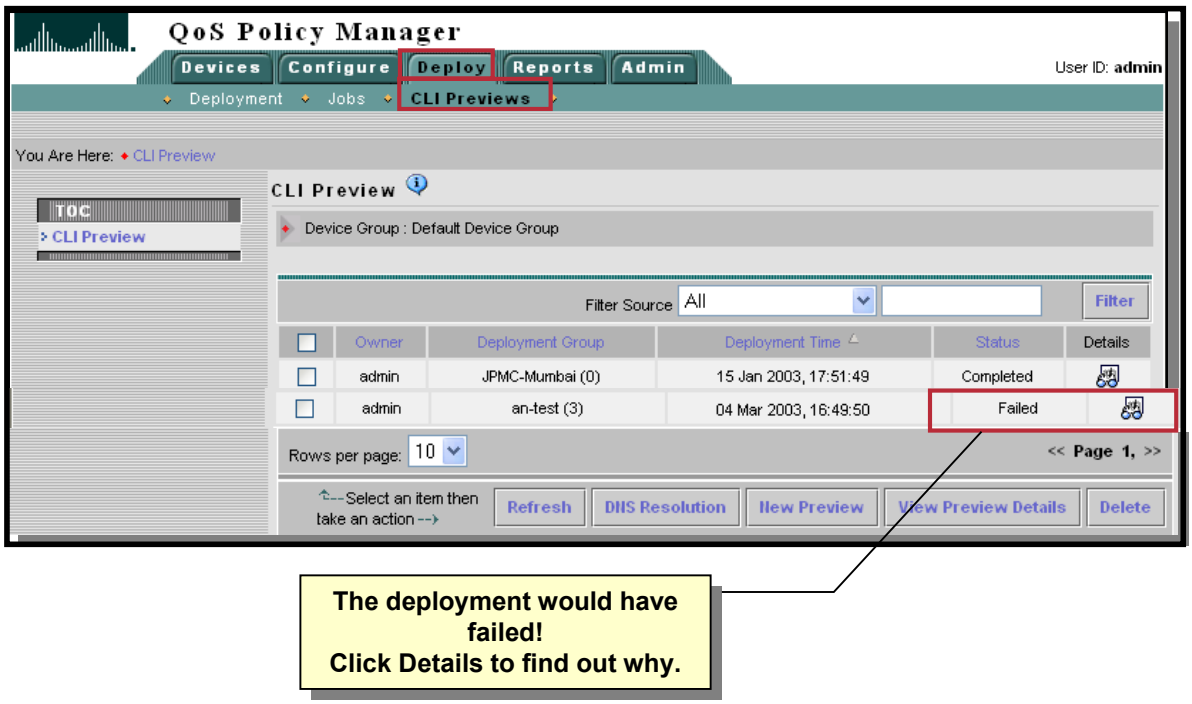
Preview Policy Deployment

Even though the policies have changed only slightly, this time the user will preview the deployment prior to executing it using the CLI Preview feature of QPM. QPM allows you to view in advance the CLI commands that will be sent to the devices upon deployment and if the commands would be successful. You can create a CLI Preview job to view the commands for the current deployment group by following these steps:

1. From the main tabs in QPM, select *Deploy* > *CLI Preview*. All previously deployed preview jobs are listed. Click *New Preview* to start a new job. The 3-step CLI Preview Wizard appears.
2. Select the deployment group name from the pull-down menu. Click *Next* to proceed to the next available step in the wizard, which is selecting the devices to preview policy deployment.
3. Only the devices whose network elements were assigned to the policy group are listed for selection. Ensure that the checkbox next to the Cisco 7200 device is checked. From the Device Selection window, click *Finish* to start the job to preview the results of possible deployment.

Scenario 2
Preview Policy Deployment (continue)

Cisco.com



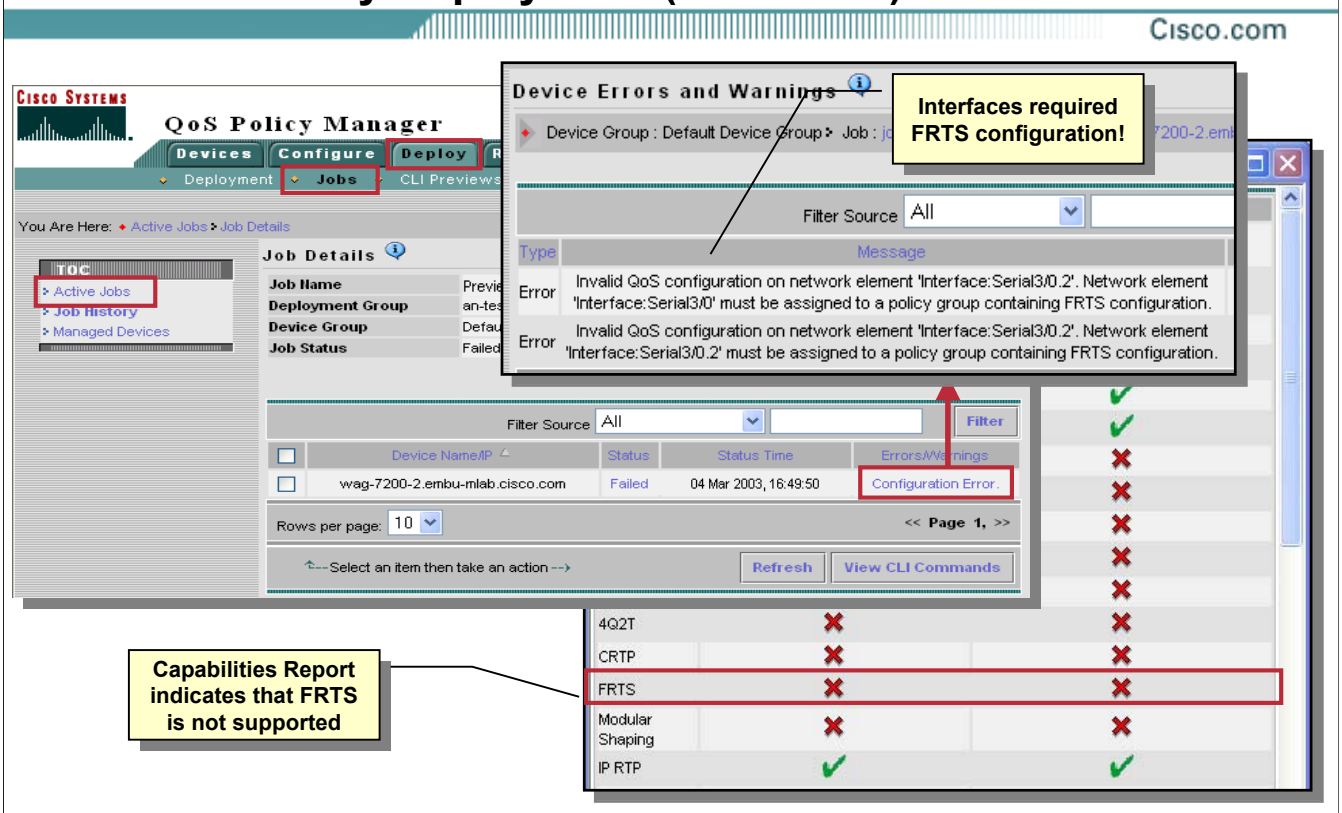
The deployment would have failed!
Click Details to find out why.

Preview Policy Deployment (continued)

After starting the preview job, the CLI Preview window reappears. The current preview job is listed at the bottom of the page. Click *Refresh* to update the results.

In this scenario, it was a good thing to run the preview job prior to deployment. The deployment job would have failed. But why? To obtain more details, click the *Details* icon for the job.

Scenario 2
Preview Policy Deployment (continued)



Preview Policy Deployment (continued)

By clicking the details icon in the previous illustration, the Job Details window appears. The job indicates configuration errors. The device errors and warnings message indicates that the interfaces need to be assigned to a policy group containing FRTS (Frame Relay Traffic Shaping) configuration in order to implement the QoS mechanisms defined in the policy.

By going back to the Capabilities Report for the policy group, the user notices that FRTS is not supported based on the device constraints configured. In this case, the user will need to review the device support requirements and the device constraints configured.

Refer to the QPM Device Support document to review the software versions and devices supported by QPM. In this scenario, the device type and software version are supported. After researching FRTS more, we can refer back to Chapter 2 for more information on FRTS. In Chapter 2, it is noted that FRTS requires a network element to be an interface of type Frame Relay. The device constraints in the scenario specified Any Interface type. Hence, the user will need to edit the device constraints for the policy group and enable FRTS on the interface and sub-interfaces prior to deployment.

Repeat the previous CLI Preview steps, prior to deployment, to verify that the changes corrected the device errors.

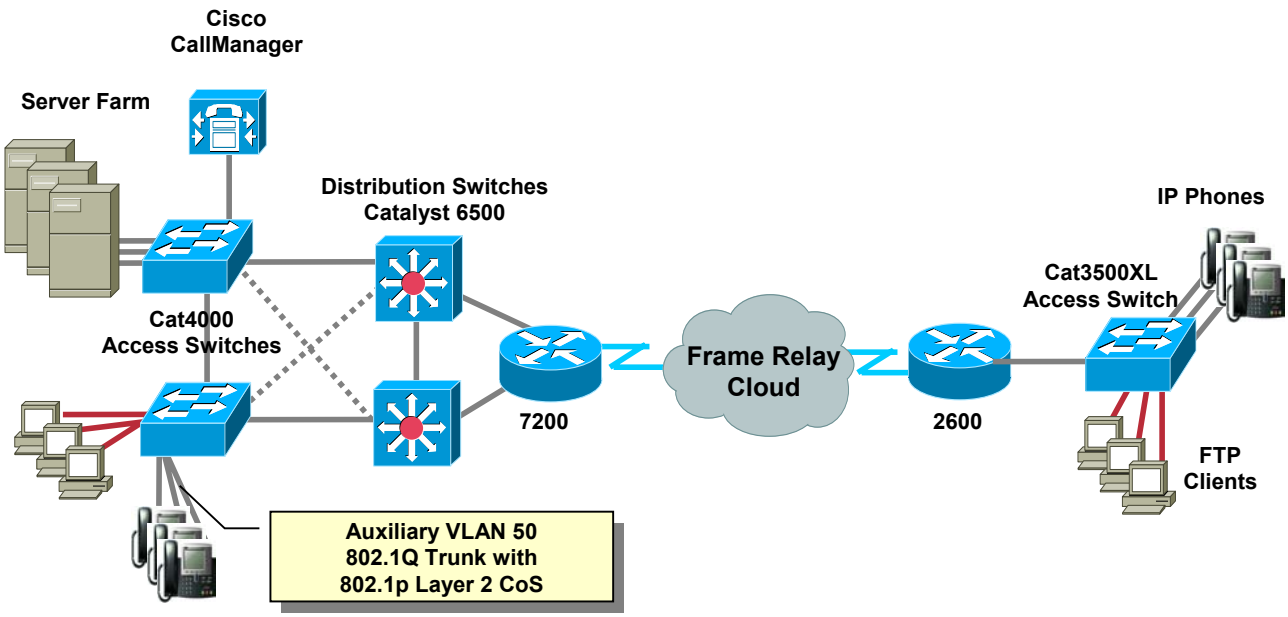
This page intentionally left blank.

Scenario 3

Providing QoS for Voice Traffic

Scenario 3
Providing QoS for Voice Traffic

Cisco.com



Scenario 3 - Providing QoS for Voice Traffic

In this scenario, the customer has recognized the tremendous cost savings resulting from the combination of voice, video, and data applications. Now the challenge is to improve or maintain the same Quality of Service (QoS) in the IP telephony network.

The campus site now includes a Cisco CallManager and IP Phones that are connected to Catalyst access switches. The IP phone ports are configured to use an auxiliary voice VLAN, Vlan50. The Catalyst access switches are connected to a core layer switch which then feeds into the Frame Relay cloud.

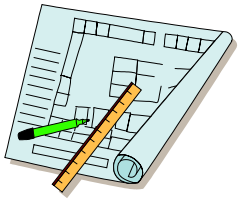
The smaller remote branch office includes several IP phones connected to a Catalyst 3500XL switch which then feeds into the Frame Relay cloud.

The network designers understand that the quality of voice is directly affected by the packet loss, packet delay, and delay variation (jitter) of voice packets. Therefore, the designers wish to implement the voice QoS features recommended by the QoS design guidelines. QoS configurations and policies are required at relevant points throughout the network. (The recommended guidelines and the relevant points are discussed next.)

In addition, the customer plans to use QPM and the IP Telephony templates to assist in the deployment of the correct device commands to implement these mechanisms throughout their enterprise network.

QoS Design Guidelines

Cisco.com



- **Campus Network**
  - **Classify voice RTP streams and voice control traffic**
  - **Extend the classification trust boundary to the phone using trust-ext commands**
  - **Never allow PC applications to send traffic at a CoS or ToS value of 5-7**
  - **Use a separate IP address space and separate VLANs for IP telephony**
- **WAN Network**
  - **Provision WAN bandwidth**
  - **Compress IP RTP header**
  - **Use low latency queuing on WAN**
  - **Use link fragmentation and interleaving or FRF techniques**

QoS Design Guidelines for VoIP

Quality of Service (QoS) for Voice over IP (VoIP) is guaranteed when proper VoIP network design is combined with the new Cisco Catalyst products, the latest Cisco IOS releases, and Cisco CallManager call admission control technologies. When building a Cisco AVVID (Architecture for Voice, Video and Integrated Data) network, the customer should adhere to the following core principles:

In the Campus Network

- Classify voice RTP streams as EF or IP Precedence 5 (critical) and place them into a second queue (preferably a priority queue) on all network elements.
- Classify Voice Control traffic as AF31 or IP Precedence 3 and place it into a second queue on all network elements.
- Catalyst 6000 switches (but not Catalyst 6000 switches with Supervisor IOS) provide the additional capability to extend the trust boundary. For example, this is particularly useful for a VoIP network where you have a PC-IP phone-Catalyst 6000 setup. You can ensure that voice packets retain their high precedence settings by extending the trust boundary to the IP phone and setting it to "untrusted" so that the precedence of all packets received from the PC is negated.
- Use a separate IP address space and 802.1Q/p connections for the IP phones and use the Auxiliary VLAN for voice.
- Enable QoS within the campus if LAN buffers are reaching 100% utilization.

QoS Design Guidelines for VoIP – continue …

In the Wide Area Network:

- Always provision the WAN properly, allowing 25% of the bandwidth for overhead, routing protocols, Layer 2 link information, and other miscellaneous traffic.
- Compress the RTP packet header from 40 bytes to 2-5 bytes.
- Use Low Latency Queuing (LLQ) on all WAN interfaces.
- Use Link Fragmentation and Interleaving (LFI) techniques for PPP interface when link speeds are below 768 K bps. Multi-link Point-to-Point Protocol (MLP) must be configured on the interface. Frame Relay Fragmentation (FRF.12) ensures that voice packets are not blocked behind large data packets (such as file transfers) by fragmenting these large packets and interleaving voice packets between the fragments in frame relay networks.

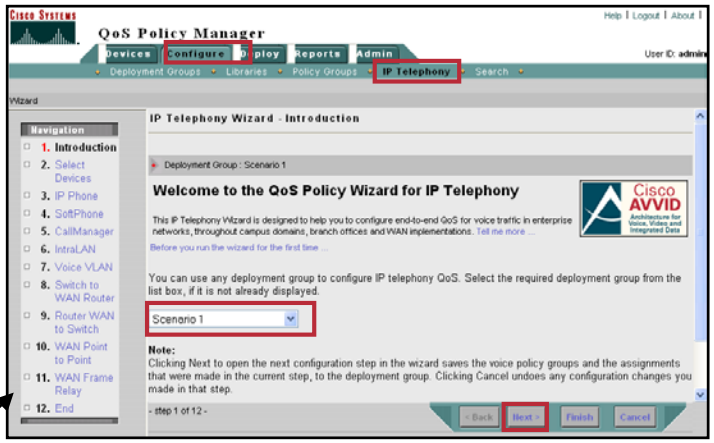
More information on these QoS Design Guidelines for VoIP can be found in the IP Telephony/VoIP Design and Implementation Guide (refer to Chapter 5 for the on-line URL). Now let's look at how to use QPM to implement these QoS design guidelines.

Scenario 3
Getting Started

Cisco.com

Ensure that the following has been completed:

- **Voice VLANs have been configured on all the relevant ports on devices (enables the wizard to correctly attach QoS properties to the Voice VLANs)**
- **Access QPM**
- **All the relevant devices have been imported to QPM (*completed in previous scenario*)**
  - **Refer to Chapter 2 to help identify network points requiring QoS for IP Telephony**
- **A deployment group has been created (*completed in previous scenario*)**
- **Start the IP Telephony Wizard**



QPM v3.0

Scenarios 3-41

Scenario 3 – Getting Started

Getting started writing QoS policies for VoIP traffic is easy with QPM. Rather than creating all the policies to meet the recommended guidelines from scratch, QPM automates the creation of them with the IP Telephony wizard.

Before launching QPM from the CiscoWorks desktop, ensure that the voice VLANs have been configured on all the relevant ports on your devices to ensure the QPM VoIP wizard correctly attaches QoS properties to them.

In this scenario, we will assume that all relevant devices in the network have been added to the QPM inventory during the device import task completed in the first scenario, and that the same deployment group will be used to deploy the QoS policies for IP Telephony.

QPM has IP Telephony templates available to ease the creation of VoIP QoS policies. To use these templates, we will use the IP Telephony wizard. The IP Telephony wizard helps you define your IP telephony network topology, and automatically creates the voice policy groups that will include the QoS policies required at each network access point (interface) where QoS is recommended. All you must do is select the devices that are in your network topology, and the wizard will automatically assign the interfaces to the appropriate voice policy groups.

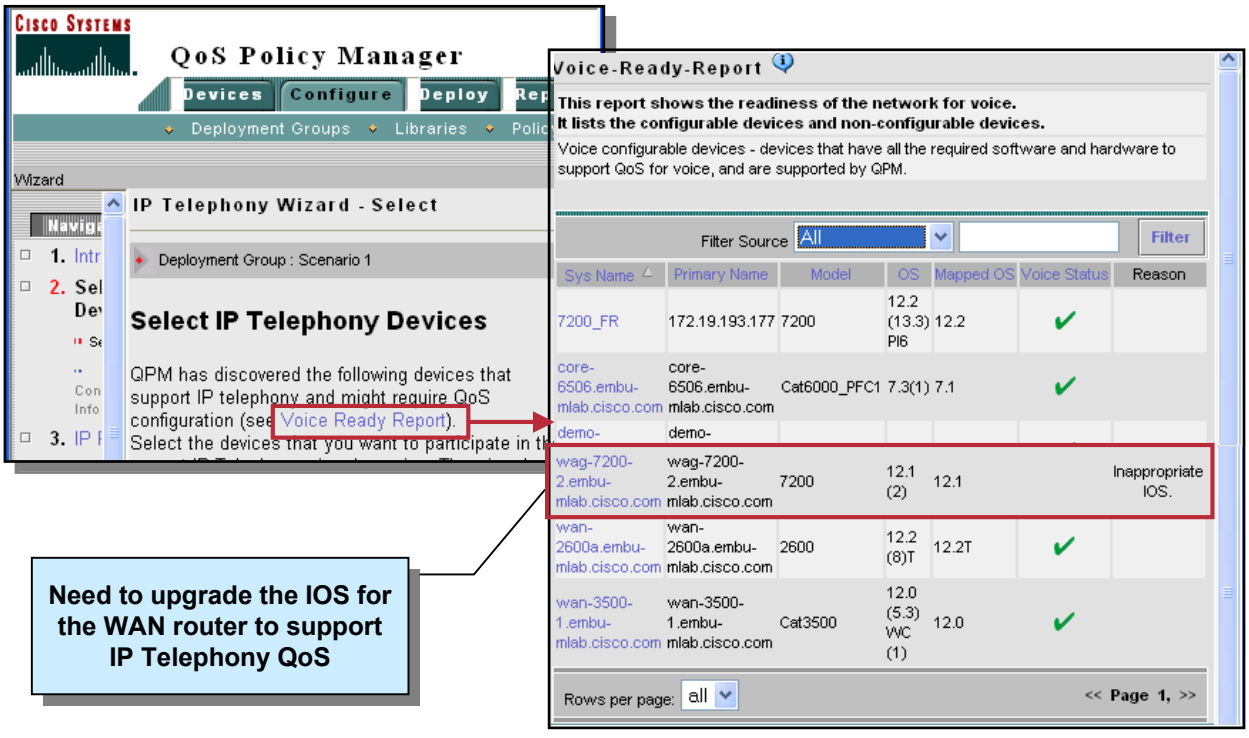
Optionally, you could also import device roles from a text file into QPM to automate the mapping of network devices to a network access point to be recognized by the IP Telephony wizard.

To start the wizard, follow these steps:

1. From QPM, click *Configure* > *IP Telephony* from the main tabs.
2. Select the previously used Deployment Group from the pull-down menu.
3. Click *Next* to start the wizard.

Scenario 3
Preparing a Voice Ready Report

Cisco.com



Preparing a Voice Ready Report

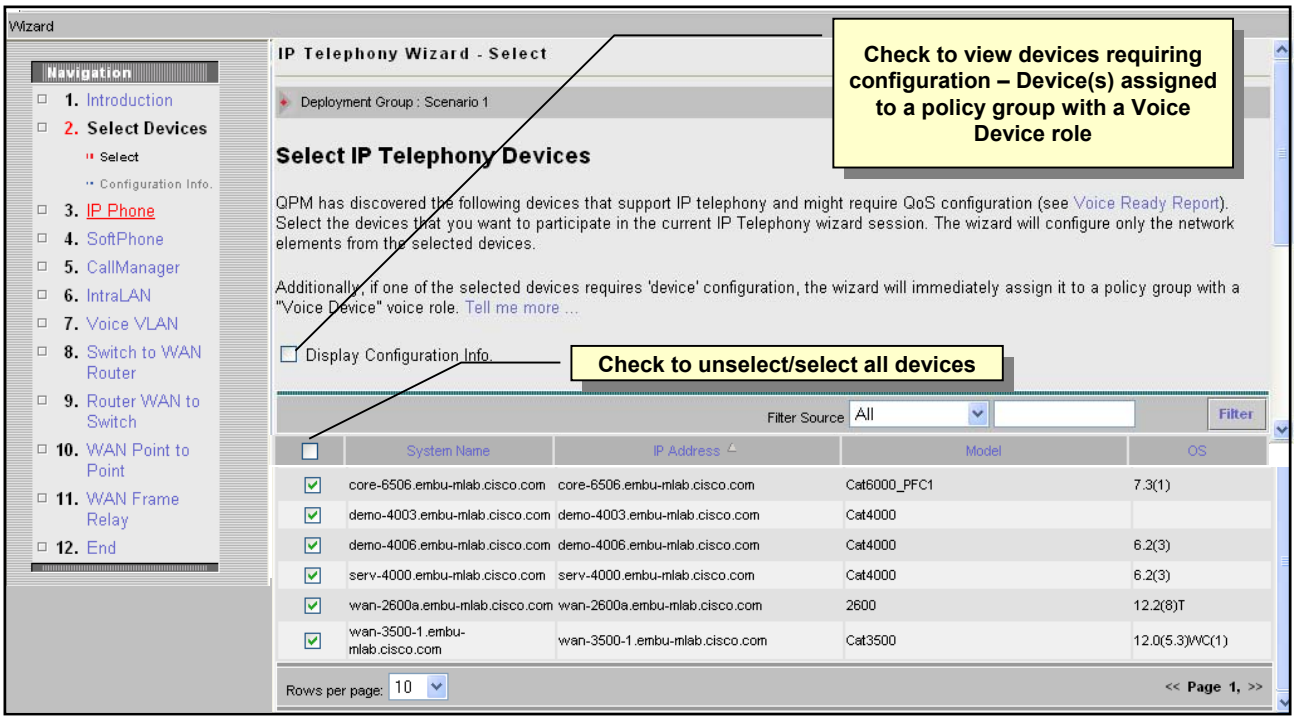
Prior to selecting the devices that require QoS configuration for voice traffic, launch the *Voice Ready Report* from the page displayed in Step 2 of the IP Telephony Wizard.

The Voice Ready Report shows the readiness of the network for voice by evaluating the devices in the network to determine if their software images provide the necessary support for VoIP QoS. The report lists the configurable devices and non-configurable devices. Voice configurable devices are devices that have all the required software and hardware to support QoS for voice and are supported by QPM.

In our scenario, we generated the Voice Ready Report by clicking on the *Voice Ready Report* link on the page displayed by Step 2 of the IP Telephony Wizard. The report quickly illustrated that the Cisco 7200 router does not have an appropriate IOS version to support the QoS voice configuration by QPM. The IOS needs to be upgraded to support voice QoS constructs. (If installed, users with CiscoWorks RME can use the Software Manager function to reliably upgrade the software on this device. CiscoWorks RME is available with the LAN Management Solution (LMS) or Routed WAN (RWAN) Management CiscoWorks bundles.)

Scenario 3
Selecting the Devices

Cisco.com



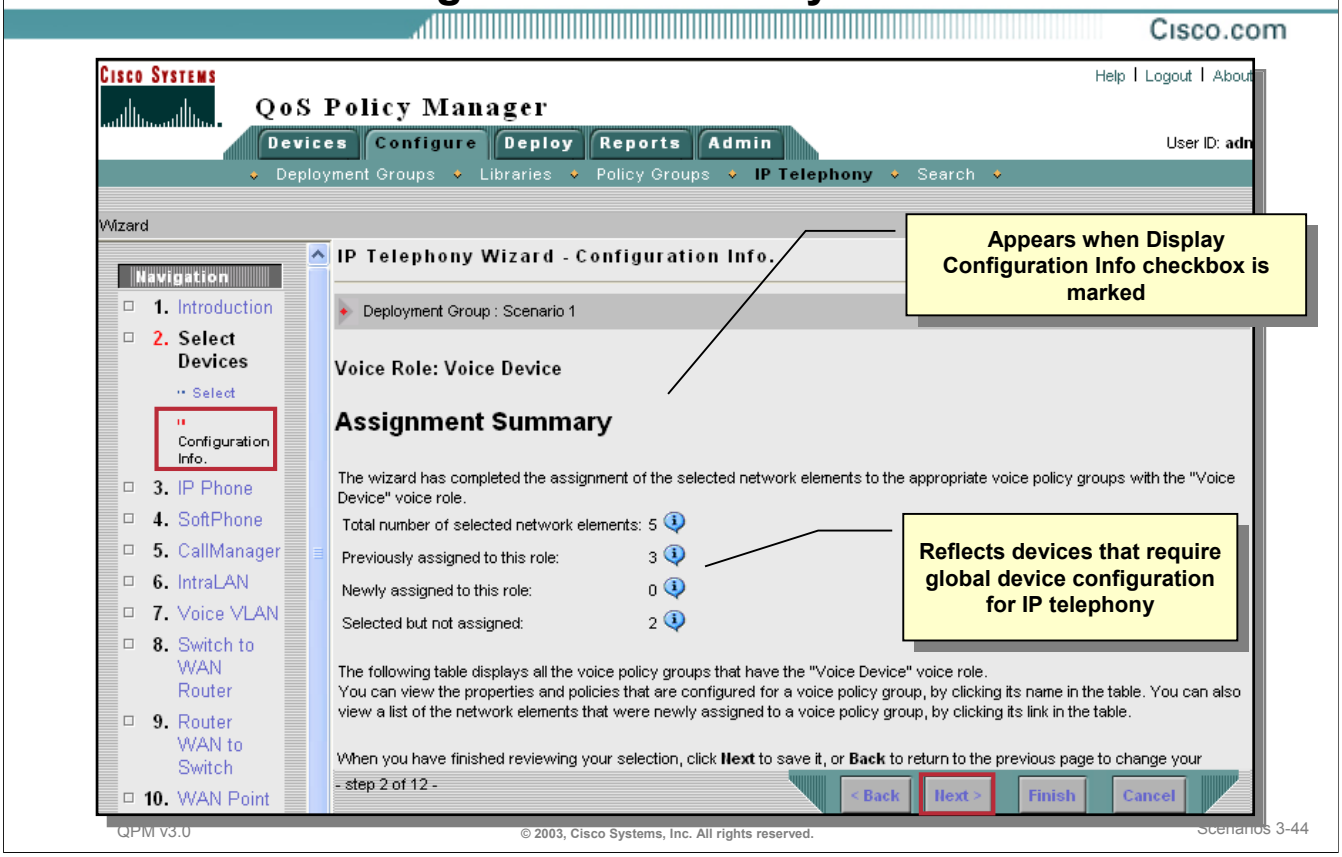
Scenario 3 - Selecting the Devices

After viewing the Voice-Ready-Report, finish this step of the wizard by selecting the devices to be configured for voice QoS. All the devices that you imported, that support IP telephony features (according to model and OS), are displayed in a table.

To select the devices, follow these steps:

1. Recommended, but optional, check the *Display Configuration Info* box. By doing so, you can view how the wizard has assigned the selected network elements to the appropriate voice policy groups. These voice policy groups are predefined templates within QPM and are stored in the QPM component library.
2. Check the boxes next to the System Names of the devices requiring QoS settings. By default, the wizard selects all the devices in the active device group. Note that you can use the checkbox in the top heading to unselect or select all devices. Also, use the Filter feature to limit viewing all the devices. Note: change the *Rows per page* field to view more or all devices on the page.
3. Click *Next* at the bottom of the page when done selecting the devices requiring QoS configuration for voice.

Scenario 3
Global Device Configuration for Catalyst 4000/6000 Switches



Global Device Configuration for Catalyst 4000/6000 Switches

In our scenario, the user selected the Display Configuration Information checkbox in the previous dialog. Of the selected devices, three devices were Catalyst 4000 or 6000 switches. These switches require global device configuration and thus are assigned by the wizard to the appropriate voice policy groups for global configuration.

Policy Group Assignments from QPM Templates:

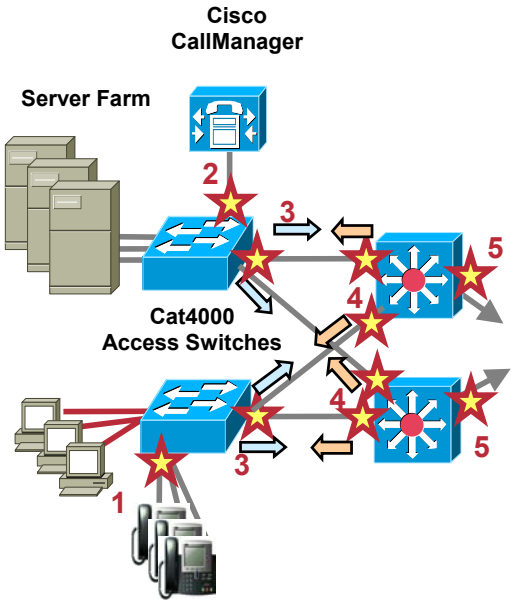
- VoiceDeviceCat4000: Contains the policies required for Catalyst 4000 devices that are part of an AVVID network. The policy group sets the scheduling on the TX queue. On Catalyst 4000 switches, the QoS for IP telephony configuration requires adding VoIP control and VoIP RTP traffic to the highest priority queue.
- VoiceDeviceCat6000: Contains the policies required for Catalyst 6000 devices that are part of an AVVID network. The policy group sets the scheduling on the TX queue and the CoS to DSCP mappings. On the Catalyst 6000 switches, the QoS for IP telephony configuration requires adding VoIP control traffic to the second-queue-first-threshold of the 2Q2T queuing scheme of the Catalyst 6000. It also requires adding the VoIP RTP traffic (CoS = 5) to the second-queue-second-threshold, or to the priority queue in the 1P2Q2T queuing scheme.

To view and save the device assignments made by the wizard, follow these steps:

1. Click on the information callout icon to view the devices selected by the wizard for assignment to these policy groups.
2. Scroll down on the page and view the new policy groups (VoiceDeviceCat4000 and VoiceDeviceCat6000) to be added to the deployment group.
3. Then click on *Next* to save it, or *Back* to change your selection.

Scenario 3
Configuring QoS at the Campus for IP Telephony

Cisco.com



Configure QoS for IP telephony at the following network points:

1. **The IP phone connections to the access switches ports**
2. **The CallManager connection to the access switch port**
3. **The uplink port on the Layer 3 access switch connection to the Layer 3 distribution switch port**
4. **The downlink ports on the Layer 3 distribution switch connections to the Layer 3 and Layer 2 access switches ports**
5. **The LAN connection from the Layer 3 distribution switch to the WAN router**

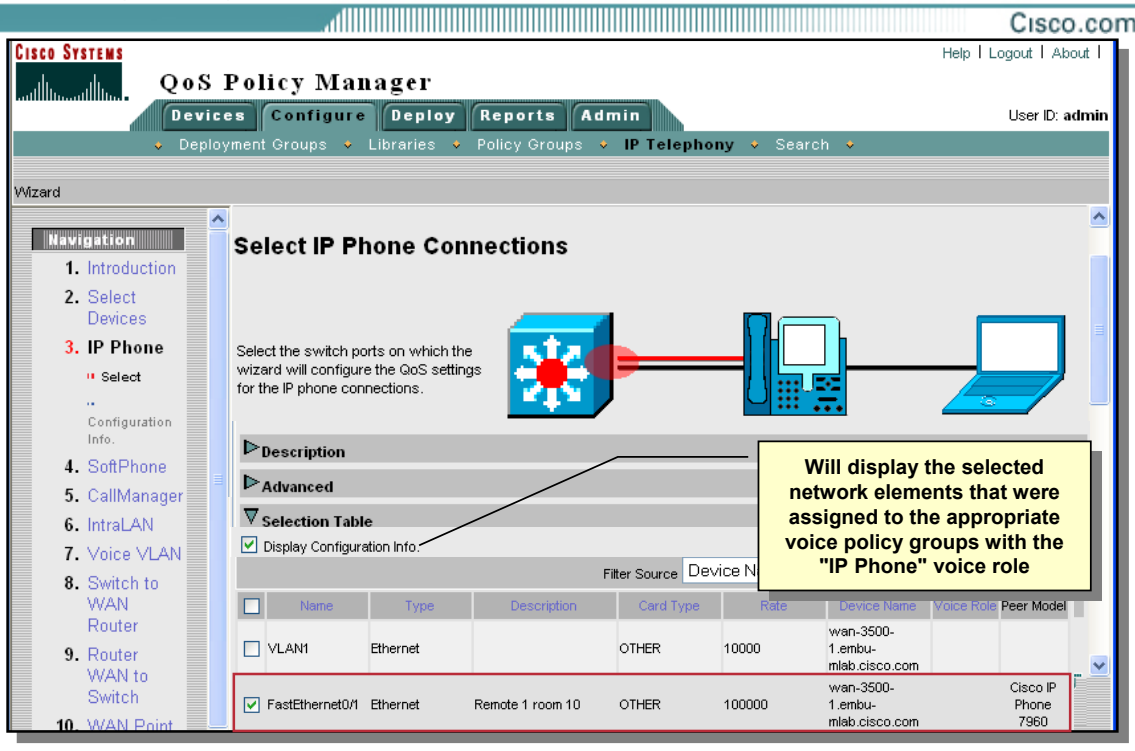
Configuring QoS at the Campus for IP Telephony

The next steps of the wizard (steps 3-9) are used to set various network access points into the appropriate policy groups. The access points and policies within the policy groups are based on the recommendations for Campus access points in the IP Telephony QoS design guidelines.

The design guidelines identify the following network access points to receive QoS settings in support of voice traffic:

1. The IP phone connections to the access switches ports
2. The CallManager connection to the access switch port
3. The uplink port on the Layer 3 access switch connection to the Layer 3 distribution switch port
4. The downlink ports on the Layer 3 distribution switch connections to the Layer 3 and Layer 2 access switches ports
5. The LAN connection from the Layer 3 distribution switch to the WAN router

Scenario 3
Configuring QoS – IP Phone Switch Ports



Configuring QoS at the Campus for IP Telephony

Use step 3 of the IP Telephony Wizard to select the switch ports connecting to IP phones so the appropriate templates can be associated with them.

You will notice that each configuration step 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. It is good to view this description if you are unfamiliar with selecting the network access points for configuration.

Also, each configuration step of the wizard includes an *Advanced* section. Here 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. Also, the *Advanced* section has a *Recommend* option. If QPM recommended rules are available for a specific voice role, clicking this option 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. (Refer to the User Guide for more information.)

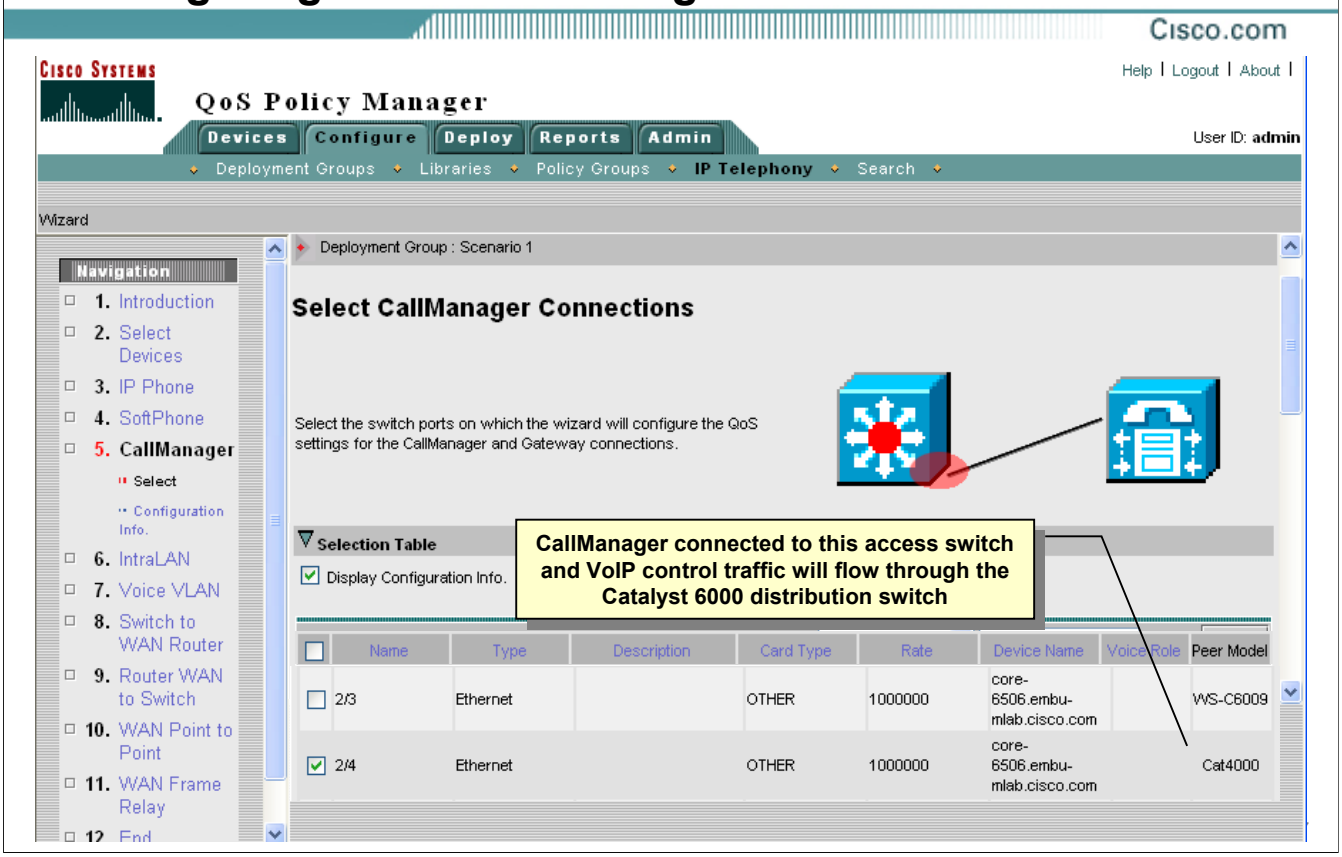
And finally, each configuration step of the wizard includes a *Selection Table* with possibly multiple pages based on the devices selected. To select a switch port to configure for IP phone connections, follow these steps:

1. To locate a specific device in the Selection Table, use the *Filter* feature. For example, to filter by a device name, select *Device Name* and enter the Sys Name of the device. Then click *Filter*.
2. Place a checkbox next to the switch ports connecting to IP phones.
3. Optionally, check the *Display Configuration Info* box to view the assignment made by the wizard. In this scenario, two ports on the remote branch access switch (Catalyst 3500XL) were assigned to the following policy group:

   Acc3500toIPPhone - Contains the policies required for a Catalyst 3500 XL family switch port that is connected to an IP phone.

4. Click *Next* to save the assignment.

Scenario 3
Configuring QoS – CallManager Connection



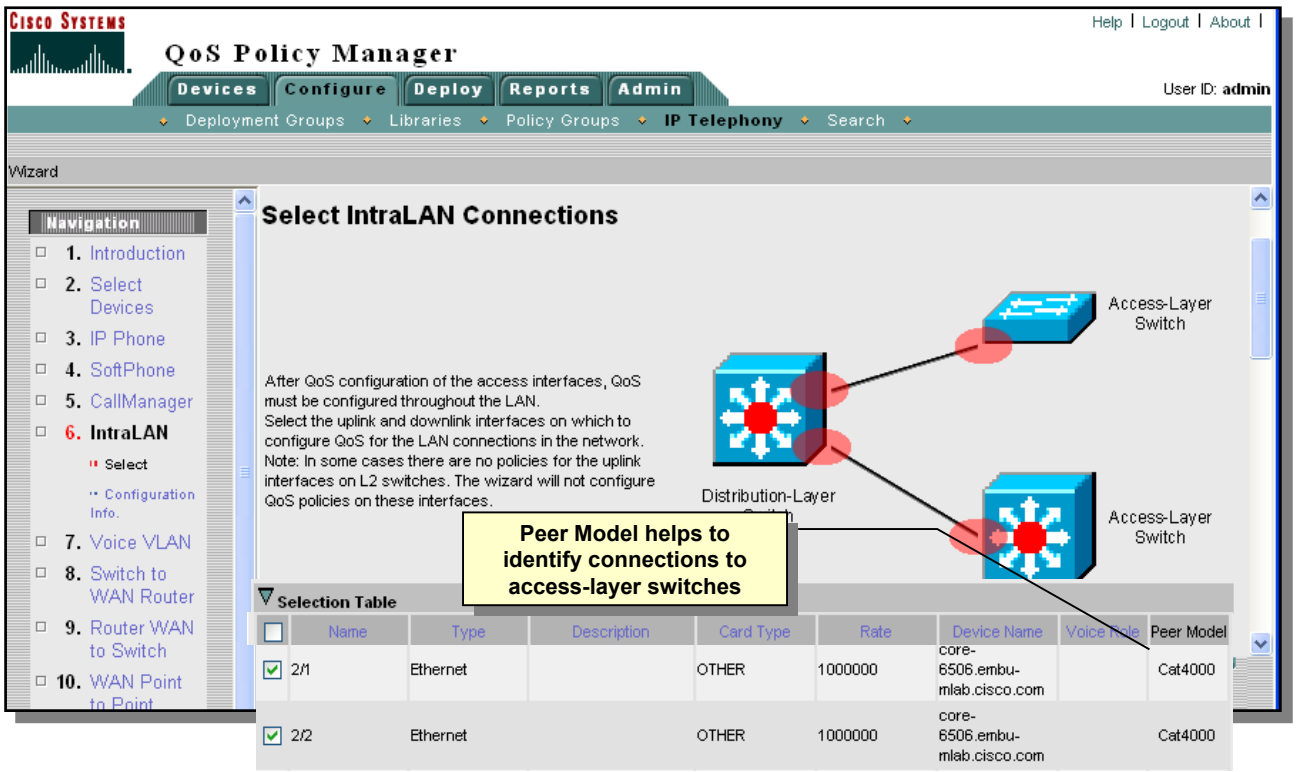
Configuring QoS at the CallManager Connection

For this scenario, step 4 of the IP Telephony Wizard will be skipped since the network does not contain any SoftPhone connections. Use step 5 of the wizard to identify the switch ports connected to Cisco CallManager and Gateway devices that require VoIP QoS settings. Follow these steps, to select the ports and assign the QPM predefined policy groups:

1. From the selection table, only Layer 3 Catalyst 6000 switches were illustrated. The Cisco CallManager is connected to a Catalyst 4000 switch and thus not illustrated for selection. Therefore, select the distribution switch port connecting to the access switch port hosting the Cisco CallManager.
2. Click *Next* to save the wizard assignment to the following policy group.

   Acc6000toVoIPControl - Contains the policies required for a Catalyst 6000 (with PFC) switch port that is connected to a Cisco CallManager or a Voice Gateway.

Scenario 3
Configuring QoS – IntraLAN Points / Voice VLAN



QPM v3.0 Scenarios 3-48

Configuring QoS at the IntraLAN Points / Voice VLAN

The next step of the wizard is to identify all the uplink and downlink interfaces between the access and distribution switches on which to configure QoS for the LAN connections in the network. Note: In some cases there are no policies for the uplink interfaces on layer 2 switches. The wizard will not list the layer 2 switches in the selection table, nor configure QoS policies on these interfaces.

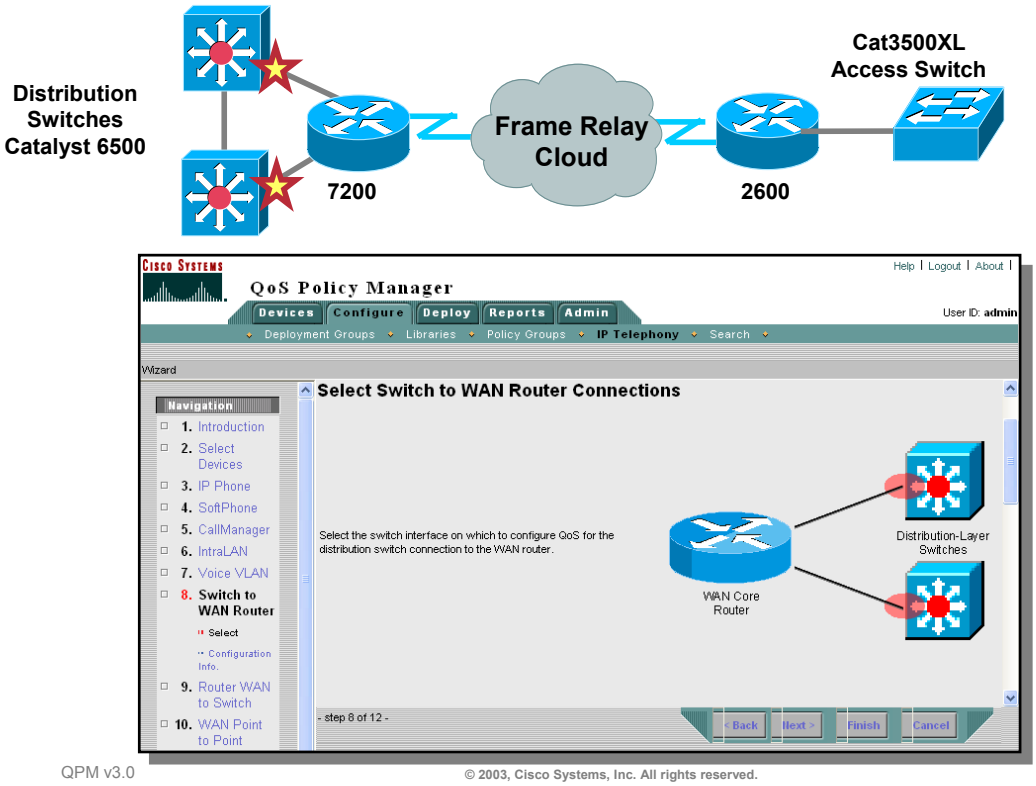
1. When selecting the uplink and downlink interfaces from the selection table, it is helpful to have a topology map illustrating the port connections between the access and distribution switches. If you have CiscoWorks Campus Manager installed, it can help identify these network points. Also, the selection table can help identify the IntraLAN points by illustrating the Peer Model connecting the switch, if known (requires CDP to be enabled on the devices).
2. If the *Display Configuration Info* box is checked, the policy group assignment information is displayed. This is helpful to view which policy group templates are being assigned to which network elements.
3. Click *Next* to save the assignment to the following policy group:

   Dist6000_GEtoL2QoSAware - Contains the policies required for the Gigabit Ethernet connection of a Catalyst 6000 in the distribution layer, to an L2 QoS aware switch in the access layer.
4. Although not illustrated here, the next step (Step 7) of the IP Telephony Wizard, is to configure the Voice VLAN. When the devices were added to QPM, QPM detected the VLANs defined on the access and distribution layer switches.

   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, configured in this scenario as VLAN 50. VLAN-based QoS style (for the auxiliary VLAN), is configured on the connection of the IP phones to the switch and also on the connection of Layer 2 switch to Layer 3 switch. The QoS configuration on the VLAN ports will be to trust CoS for any IP traffic. From the table, select the auxiliary voice VLAN and then click *Next* to go to the next step.

Scenario 3
Configuring QoS – Campus Switch to WAN Router

Cisco.com



QPM v3.0 Scenarios 3-49

Configuring QoS – Campus Switch to WAN Router

In this last step of the LAN switch settings, the wizard configures QoS for the distribution/core layer switch interface to the WAN router. Because traffic coming from the WAN side is already classified, the QoS configuration on the switch interface to the router will be to trust the layer 3 DSCP bits from the router. In cases when the layer 2 CoS bits of traffic coming from WAN are 0 because of the different layer 2 protocols on the WAN, the Catalyst 6000 switch will set those bits according to the DSCP values. The QoS configuration for the distribution switch interface to a WAN router will be to trust the DSCP bits from the router.

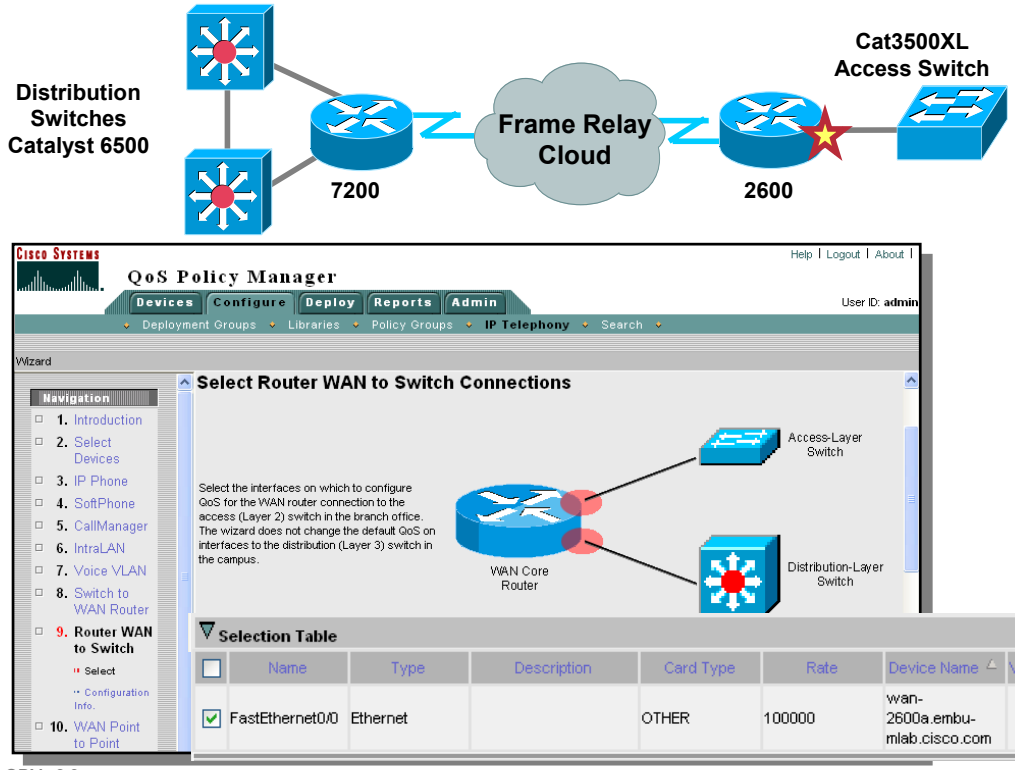
Follow the steps below to select the switch interface on which to configure QoS for the distribution switch connection to the WAN router.

1. Select the checkboxes next to the distribution switches that route traffic to the Core WAN 7200 router, as illustrated above. Use the Peer Model column in the Selection Table to help locate the correct interface numbers.
2. Click *Next* to view the Device Configuration Information, if elected via the checkbox. This information describes the following policy group assignment, the policy name, and the network elements assigned:

   Dist6K_FEtoRouter, contains the policies required for the Fast Ethernet connections from a *Catalyst 6000 to a WAN router.*
3. Click *Next* to save the wizard assignment and go to the next wizard step.

Scenario 3
Configuring QoS –WAN Router to Layer 2 Switch

Cisco.com



Configuring QoS – WAN Router to Layer 2 Switch

By default, a router trusts the interface to a distribution switch, so if a switch has layer 3 QoS capabilities, no special QoS is required on the router input direction. Also, because the layer 3 switch knows to trust DSCP from router and to set CoS bits accordingly, no special QoS is required on the output direction. But if the switch has only layer 2 QoS capabilities, such as in our remote branch, the router must classify traffic on input and set layer 2 CoS bits on output. The wizard will distinguish between these two types.

The QoS configuration for a router interface to a distribution switch is a combination of:

- Trust DSCP from layer 3 QoS aware switches. (default, wizard does not configure)
- Classify and color input traffic from layer 2 QoS aware switch.
- Set CoS bits according to DSCP bits on output traffic to layer 2 switch.

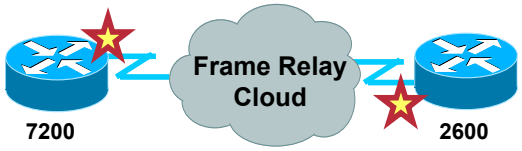
Follow the steps below to select the interfaces on which to configure QoS for the WAN router connection to the access (Layer 2) switch in the branch office. The wizard does not change the default QoS on interfaces to the distribution (Layer 3) switch in the campus.

1. Select the checkboxes next to the WAN router that is connected to the layer 2 switch at the branch network, as illustrated above. Use the Peer Model column in the Selection Table to help locate the correct interface numbers.
2. Click *Next* to view the Device Configuration Information, if elected via the checkbox. This information describes the following policy group assignment, the policy name, and the network elements assigned:

   RouterToL2QoSSwitch - Contains the policies required for a branch office WAN router Ethernet connection to an L2 QoS aware switch.
3. Click *Next* to save the wizard assignment and go to the next wizard step.

Scenario 3
Configuring QoS at the WAN for IP Telephony

Cisco.com



Per the QoS design guidelines, configure the following QoS features for IP telephony:

1. **Frame Relay Fragmentation (FRF)**
2. **Low Latency Queue (LLQ)**
3. **IP RTP Header Compression (cRTP)**
4. **Frame Relay Traffic Shaping (FRTS)**

Configuring QoS at the WAN for IP Telephony

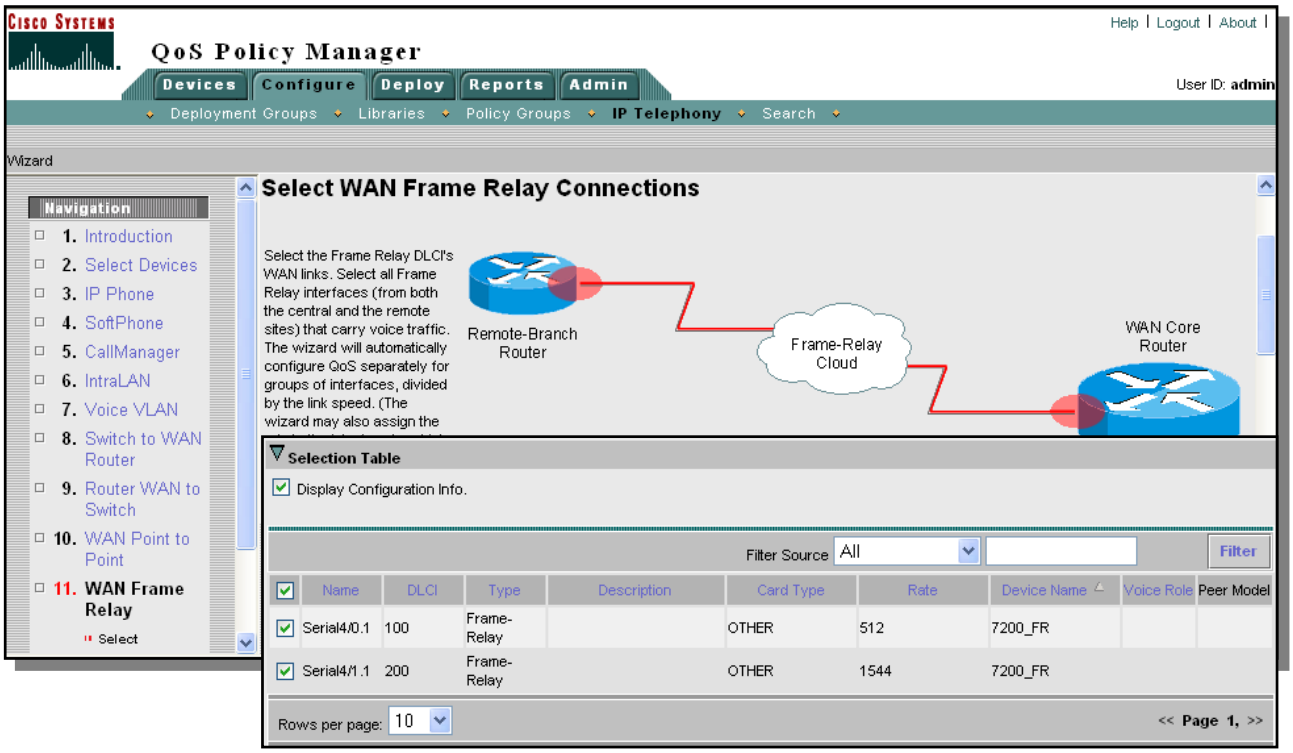
On Frame Relay WAN interfaces, like in Point-to-Point interfaces, QoS configuration is important to prevent delays. In addition, because Frame Relay is a non-broadcast technology that uses over-subscription to achieve costs savings, traffic shaping is used to prevent excessive delay from congested network interface buffers.

The wizard will configure the QoS settings for these interfaces using the following tools:

- Frame Relay Fragmentation (FRF) - ensures that voice packets are not blocked behind large data packets (such as file transfers) by fragmenting these large packets and interleaving voice packets between the fragments. Note: FRF will only be applied to those interfaces with link speed below 768kbs. Fragment size is calculated to ensure no more than 10ms delay.
- Low Latency Queue (LLQ) - allows delay-sensitive data such as voice to be de-queued and sent first (before packets in other queues are de-queued), giving delay-sensitive data preferential treatment over other traffic. The relatively small size of voice packets makes it possible to use a strict priority queue for voice without degrading network quality for the remaining traffic. It also uses CBWFQ to ensure bandwidth for VoIP control traffic. The traffic classification is set according to the DSCP value.
- Optionally, IP RTP Header Compression (cRTP) - reduces unnecessary bandwidth consumption by compressing the header, reducing its size from 40 bytes to 5 bytes. The benefits of using cRTP for voice are apparent when considering that the payload for a VoIP packet is only 20 bytes. If cRTP is enabled, monitor the CPU utilization and disable it if CPU is above 75%. At higher link rates, the bandwidth savings of cRTP may be outweighed by the additional CPU load.
- Frame Relay Traffic Shaping (FRTS) - minimizes packet loss by throttling back packets as they are forwarded into the Frame Relay cloud, based on congestion indicators. The QPM Frame Relay templates are designed for various link rates. By default, QPM sets the CIR to 95% of the link speed for low rate links, and 99% for high rate links. If necessary, you can adjust the FRTS ratio according to your links speed.

Scenario 3
Configuring QoS at the WAN for IP Telephony

Cisco.com



QPM v3.0 Scenarios 3-52

Configuring QoS at the WAN Frame Relay for IP Telephony

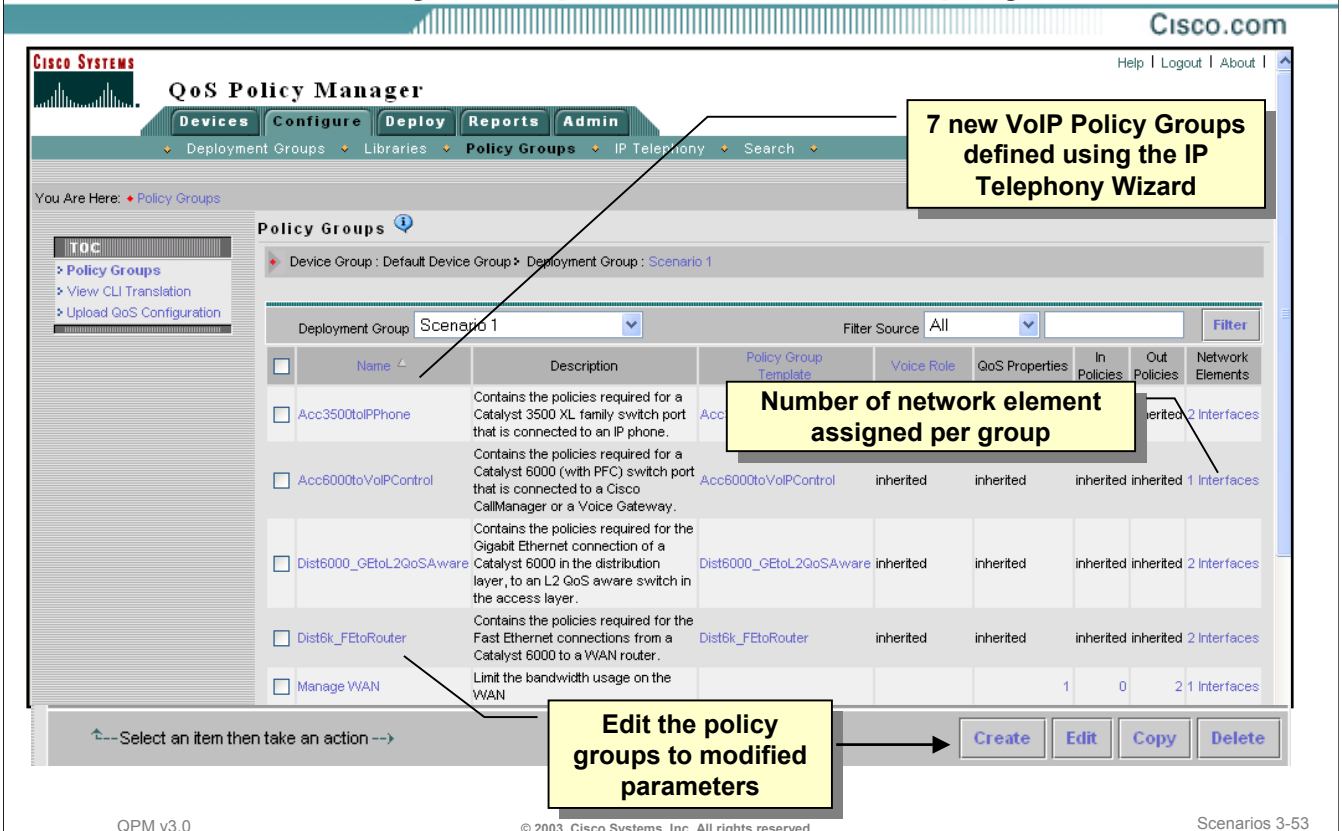
In the final step of the IP Telephony Wizard, WAN Frame Relay, select the Frame Relay DLCI's WAN links for QoS configuration. Select all Frame Relay interfaces (from both the central and the remote sites) that carry voice traffic.

The wizard will automatically configure QoS separately for groups of interfaces, divided by the link speed. (The wizard may also assign the role to the interface to which the DLCI belongs).

This is the final step prior to deploying the policies. After clicking *Next*, the wizard will ask if you want to deploy the policies by launching the Deployment Wizard.

Select *No* and then click *Finish*; the Deployment Wizard can be launched later by selecting *Deploy* > *Deployment*, as illustrated in the previous scenarios. Let's view the voice QoS policies just created.

Scenario 3
New Voice Policy Groups Created For Deployment



New Voice Policy Groups Created For Deployment

QPM allows you to view and modify any of the properties and policies of a voice policy group, except for its device constraints. This allows the user to customize voice policies, that were based upon predefined templates, to suit specific network configurations.

Refer to the *Getting Started Guide* (Chapter 5) to view an example on how to modified the predefined policy groups to perform the following:

- Enable cRTP for the WAN-FR-Main-Interface voice policy group - By compressing the RTP header in an RTP data packet (cRTP), you can reduce the delay for voice traffic transmission.
- Configure the percentage of bandwidth on the interface that should be reserved for your voice traffic.

Thank You!

We hope that you have enjoyed using the QPM application and have found its features to be an important part of your network management toolkit.

Cisco Systems

Chapter 4

Installation & System Administration

QoS Policy Manager (QPM) v3.0

Chapter 4 Objectives

Cisco.com

Upon completion of this chapter, you will be able to:

- **Install QPM**
  - **Client/Server requirements**
  - **Installation guidelines**
  - **Upgrade information**
- **Perform System Administration**
  - **Database backup/restore**
  - **View audit logs**
  - **View system status**

Chapter 4 Objectives

This chapter provides highlights and important facts for installing the QPM application, and also provides some basic system administration tips. One of the goals of this chapter is to give the reader an understanding of the overall installation process. Detailed instructions and command syntax for the actual installation steps can be found in either the *Quick Start Guide for CiscoWorks QoS Policy Manager 3.0* or the *Installation Guide for CiscoWorks QoS Policy Manager 3.0*. Troubleshooting tips can be found in the *User Guide for CiscoWorks QoS Policy Manager 3.0*.

On-line URL links to the installation and user guides can be found in Chapter 5.

Installation

- Client/Server Requirements
- Device Requirements
- Installation Guidelines
- Upgrading Information

QPM v3.0 Server Requirements

Cisco.com

System Hardware	• IBM PC-compatible computer minimum 1GHz Intel Pentium 4 • CD-ROM drive • NIC card with fixed IP address
Available Memory (RAM)	• 1 GB minimum
Available Disk Space	• 9 GB minimum (CiscoWorks Common Services + QPM) • 7 GB minimum (QPM only, CiscoWorks Common Services already installed) • 2-GB virtual memory
Operating System • **Windows 2000** • **Professional** • **Server**	• Service Pack 2
File System Type	• NTFS

*** Always check the release notes for the most up-to-date requirements**

QPM v3.0 Server Requirements

For maximum performance, it is recommended that a dedicated server be used for QPM. The CiscoWorks QPM application must be installed on a Windows 2000 platform using the Administrator account and not a cloned administrator account. Do not install QPM on a Windows server running any of the following services: Primary domain controller. backup domain controller, or terminal server.

The table above illustrates the important system requirements for the platform to host all applications needed for the Cisco QPM application: CiscoWorks Common Services (CCS) Software and QPM. As a reminder, it is always a good idea to review the release notes for the most up-to-date system requirements.

QPM should be installed on a 1 GHz or higher Pentium 4 system. The amount of RAM should be maximized when possible and should be no less than 1 GB. The virtual memory or swap space should be optimized to at least twice the size of physical memory. The platform should have at least 9 GB for installation and future data storage on a single partition when installing both the CCS software and QPM. If the CCS software is already installed, the platform should have at least 7 GB available.

Do not install the software on a Windows partition configured with a FAT file system; FAT file systems do not support file security. Use NTFS to save disk space, add file security, and to improve performance.

QPM can run on top of the Windows 2000 operating system. The user can choose between Windows 2000 Professional or Server with Service Pack 2. These are the only operating system configurations that QPM has been tested and certified to run on. No matter which Windows operating system is chosen, ensure that the required service pack is installed. To determine which service pack is currently installed on a Windows system, click the *Start>Run* menu item; then type **winver**.

QPM Client Requirements

Cisco.com

Hardware/Software	• IBM PC-compatible computer with 300-MHz Intel Pentium • Windows 98 / Windows NT 4.0 / Windows 2000 • Color monitor with video card capable of 256 colors or more
Available Memory (RAM)	• 256 MB minimum
Available Disk Space	• 400-MB virtual memory for Windows • 512-MB swap space for Solaris
Web Browser	• Microsoft Internet Explorer 5.5 Service Pack 2 or later
Additional Software	• Java Plug-In v1.3.1

Client Requirements

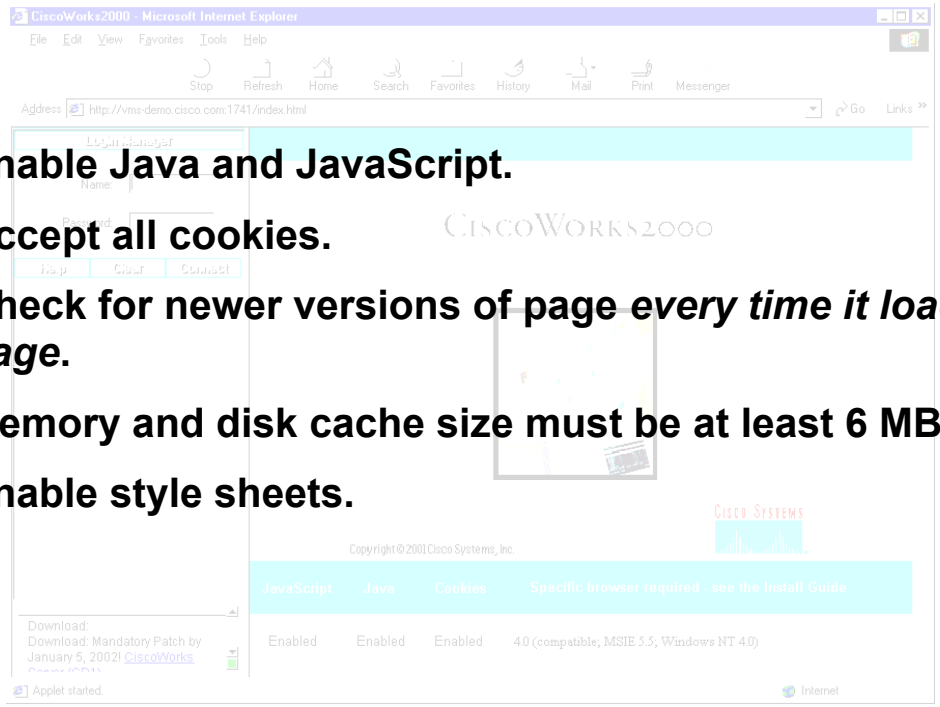
A client is used to access the CiscoWorks server and the QPM application. The client software is simply a Web browser that can be loaded on any workstation in the network. QPM has only been tested with specific versions of Microsoft Internet Explorer – version 5.5 with Service Pack 2 or later. More information on how the Web browser should be configured is discussed next.

On Windows platforms, ensure that the client's platform display properties are configured for *small fonts* and the video card color palette is configured for at least *256 colors* or more. The CiscoWorks applications will not display properly if using 16-bit colors. The display properties can be configured by going into the *Control Panel* and double-clicking on *Display*.

The CiscoWorks QPM application requires the Java Plug-In v1.3.1 to be installed on the client workstation. If the Java Plug-In is not installed, it is automatically downloaded from the CiscoWorks server and installed on the client when QPM is first used. To check whether or not the Windows workstation has the Java Plug-In installed, go to the Windows *Control Panel* and look for the *Java Plug-In* icon. Double-click on the icon and select the *About* tab to view the version number or enter **java-version** from a DOS prompt.

QPM Client Requirements
Web-Browser Configuration

Cisco.com



- **Enable Java and JavaScript.**
- **Accept all cookies.**
- **Check for newer versions of page *every time it loads a page*.**
- **Memory and disk cache size must be at least 6 MB.**
- **Enable style sheets.**

Web-Browser Configuration

In order for the client software, Microsoft Internet Explorer, to accurately display and access the data in the QPM database, the web browser needs to be properly configured. Highlighted in the chart above are the parameters that must be verified prior to accessing the server.

Enable Java and JavaScript:

- Select *Tools* > *Internet Options* > *Advanced*. Under the Microsoft VM heading, select *Java console enabled*, *JIT compiler for virtual machine enabled*, and *Java logging enabled*; then click *OK*. If there is no Microsoft VM heading, the Java Virtual Machine is not installed. Go to the CiscoWorks Server online help for a link to the Java 2 Runtime Environment (J2RE) or visit www.microsoft.com/java to obtain and install it.

Set browser cache to at least 6 MB:

- Select *Tools* > *Internet Options* > *General*, and then click *Settings*. Set the cache to at least *6 MB* using the *Amount of Disk Space to Use* slider bar. Click *OK* to close the Settings dialog box and return to the Internet Options dialog box; then click *OK* again.

Configure browser to accept all cookies:

- Select *Tools* > *Internet Options* > *Security*. Select *Internet*, and click *Custom Level*. Scroll to *Cookies* and select *Enable* for both *stored on your computer* and *per session*. Click *OK*; click *OK* again.

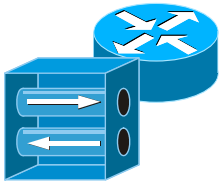
Configure browser to check for newer versions of pages every time it loads a page:

- Select *Tools* > *Internet Options* > *General;* then click *Settings*. Select the *Every visit to the Page* radio button; then click *OK*.

For more information on setting these parameters, refer to the *Installation Guide*. A link to these documents can be found in the “Reference” section.

Network Device Requirements

Cisco.com



- **SNMP community strings**
- **Authentication (telnet, TACACS, local)**
- **Supported IOS**

Network Device Requirements

QPM utilizes the Simple Network Management Protocol (SNMP) to read various Management Information Base (MIB) variables on the devices it manages. Therefore, QPM, as well as the network devices being monitor, need to have the SNMP read community string configured to work properly. (Cisco QPM receives the SNMP community string for a device from the Resource Manager Essentials (RME) inventory when importing from RME.)

Since QPM is used to modify the configuration of a device, both QPM and the device must be configured for the desired authentication method for device access. Devices added to QPM can access a device via telnet and authenticate using either standard telnet and enable passwords, local username and password, or TACACS.

Finally, a device must be running a version of IOS supported by QPM. The next page lists the devices currently supported by QPM v3.0. (An on-line URL link identifying the devices and software versions supported by QPM is also list in Chapter 5 of this tutorial.)

Network Device Requirements
Supported Devices & Software

Cisco.com

- **Campus Devices**
  - Cat 4003 & 4006 with L3, Cat4000, L2, Cat4200
  - Cat 5000, RSM
  - Cat6000 with MSFC, 6K Native, (Marina), Cat6K Native PFC2, Cat6K PFC2, Cat6K no PFC
  - 2948G-L3, 4908G-L3, 8510, 8540 29XX-XL, 3500XL, C4GWY
  - Cat3550 with 12.1E, Cat2950 with 12.1E
- **WAN Devices, including remote office**
  - Catalyst 4000 with Access Gateway Module
  - 16XX, 17XX, 26XX, 36XX, MCS3810, 45xx, 47xx, 71xx, 72xx, 7500-VIP, 6K with FlexWAN, ATM interfaces
  - VG2XX
  - 7600/IR (OSR), 7401, ICS 77XX, AS5300, AS5800, 3700, 2600XM
- **Software**
  - IOS 12.0, 12.1 12.2, 12.1E, 12.2T

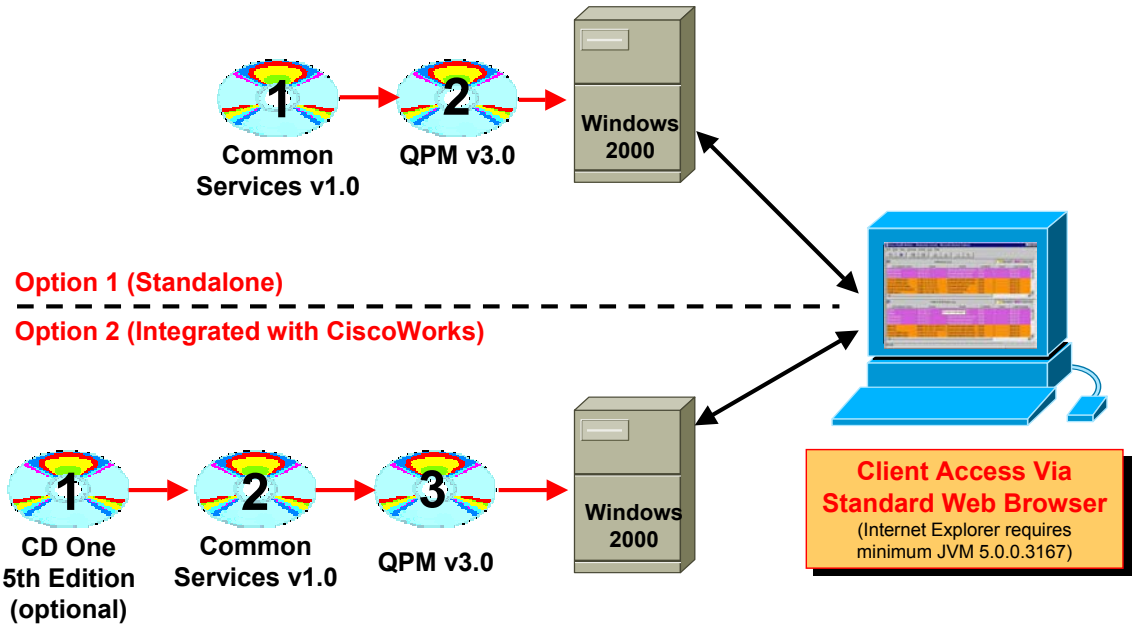
*** Always check the product documentation for the most up-to-date devices and software supported, patches typically add additional device support.**

Supported Devices and Software

The above table provides a listing of the devices and IOS software supported by QPM. Each new release of QPM, including maintenance and patch updates, include additional device and software support for QPM. Refer to the *Supported Devices and Software Versions* document (Chapter 5) for a complete list of supported devices, and the QoS features supported by each version of supported IOS.

Installation Guidelines
Installation Options

Cisco.com



QPM v3.0 Guidelines 4-9

Installation Guidelines

The installation of the CiscoWorks QPM application includes two CD components: CiscoWorks Common Services v1.0 and QPM v3.0. These two CDs must be installed on the same machine. QPM can run as a standalone application on a dedicated server or can be integrated with other CiscoWorks applications on a server.

The installation order of these applications is critical. The installation order must be as follows:

Standalone Option

1. CiscoWorks Common Services v1.0
2. CiscoWorks QPM v3.0

Integrated Option

1. CD One 5th Edition (CiscoWorks Common Management Foundation)
2. CiscoWorks Common Services v1.0
3. CiscoWorks QPM v3.0

In the integrated option approach, the QPM CDs can be installed anytime after CD One (i.e. after other CiscoWorks applications).

Installation Guidelines
Notes

Cisco.com

- **Installation order: Common Services Software, QPM, Patches**
- **Install on a Windows 2000 Professional or Server platform that is not running the following services: primary or backup domain controller, or terminal server**
- **Recommended to use a dedicated platform; Do not install on platform with the Access Control Software (ACS) application**
  - **Can install over QPM v2.1.x**
- **Server requires a fixed IP address**
- **Install software as administrator (not cloned administrator account)**
- **Disable virus protection software prior to installation**
- **The default install directory: c:\Program Files>CSCOpx**
- **Installation errors are found: c:\cw2000_inXXX.log**
- **Default HTTP port - 1741**

Installation Guidelines

The installation of the CiscoWorks QPM application includes two CD components: CiscoWorks Common Services v1.0 and QPM v3.0. These two CDs must be installed on the same machine. QPM can run as a standalone application on a dedicated server or can be integrated with other CiscoWorks applications on a server.

The installation order of these applications is critical. The installation order must be as follows:

Standalone Option

1. CiscoWorks Common Services v1.0
2. CiscoWorks QPM v3.0

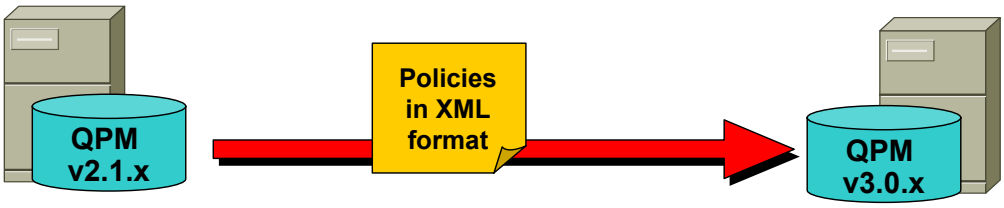
Integrated Option

1. CD One 5th Edition (CiscoWorks Common Management Foundation)
2. CiscoWorks Common Services v1.0
3. CiscoWorks QPM v3.0

In the integrated option approach, the QPM CDs can be installed anytime after CD One (i.e. after other CiscoWorks applications).

Upgrade Information

Cisco.com



- **Import policies from QPM v.2.1.x**
  - XML format (export to XML utility on QPM installation disk)
  - Creates new policy groups containing imported policies
  - Policies are converted as necessary
  - Policies for IOS 11.1, 11.2, and 11.3 not imported
  - Ensure devices to assign imported policies to exist in QPM inventory
  - Import using QPM v3.0.x task ***Admin > Import Policy Groups***

Upgrading Suggestions

Existing users of QPM version 2.1.x may have already invested a significant amount of time developing QoS policies. This work can be leveraged by importing policy information from QPM v2.1.x into QPM v3.0. New policy groups are created for the imported policies and they are converted as necessary to meet the new QPM standards and constructs.

The main differences between QPM v3.0 and QPM 2.1.x are:

- QPM v3.0 is integrated with CiscoWorks, and all QPM applications are accessed from a single web interface, instead of the separate Policy Manager window and Distribution Manager window in QPM 2.1.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 2.1.x.

  Note: QPM v3.0 device groups are administrative device domains. They are *not* the same as QPM 2.1.x device groups.

- QPM v3.0's IP telephony configuration feature facilitates the QoS configuration for IP telephony. A configuration wizard guides the user through the definition of the network topology, and then automatically assigns the relevant network points to the appropriate voice policy groups. The default voice policy groups can be modified.
- QPM v3.0 supports policy monitoring. The user can select policies and devices for monitoring, schedule monitoring tasks, and generate monitoring reports. These features are accessed from the Performance Analysis option in the Reports tab.
- QPM v3.0 contains a global inventory system. Devices can be added manually, or imported directly from Essentials. Device import and device management options are accessed 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 v3.0 creates new policy groups. This option is now accessed from the Policy Groups page of the Configure tab.
- If ACS is running on the network, the ACS user permissions can be used in QPM v3.0. When ACS user permissions are used, 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 2.1.x. Device groups are managed through the Devices tab.
- Additional devices and QoS features supported.

To import QPM v2.1.x policies into QPM v3.0, first export the QPM v2.1.x databases using the *Export to XML* utility found on the QPM distribution CD. Ensure that the devices to assign the imported policies to exist in the QPM v3.0 device inventory.

Note: devices can be imported into the QPM v3.0 device inventory from a QPM 2.1.x exported database.

Use the following steps to perform the policy import:

1. Select *Admin* > *Import Policy Groups*. The *Import Policy Groups From 2.1* page appears.
2. Select the deployment group to import the policies to.
3. In the Import file path field, enter the name and location of the QPM2.1.x XML file to import, or click the *Browse* button to select the file.
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.
5. Clear the check boxes by those devices you do not want to assign to imported policy groups. Click *Import Policies*.
6. A dialog box appears informing you that the import process has started. 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.

       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 working with multiple ACS device groups, this procedure should be repeated for each device group in QPM v3.0.

System Administration

- Database Backup/Restore
- Audit Logs
- System Status

Database Backup/Restore
Overview

Cisco.com

- **Full Backup**
  - **Backs up all QPM information**
  - **Name contains date and time of backup**
  - **Restore QPM via retrieval of full backup**
  - **Can delete full backups**
  - **Created on-demand**
- **Incremental Backup**
  - **Backs up all changes since last incremental backup**
  - **Database restoration uses all incremental backups**
  - **Cannot delete individual incremental backups**
  - **Created on-demand or on scheduled basis**

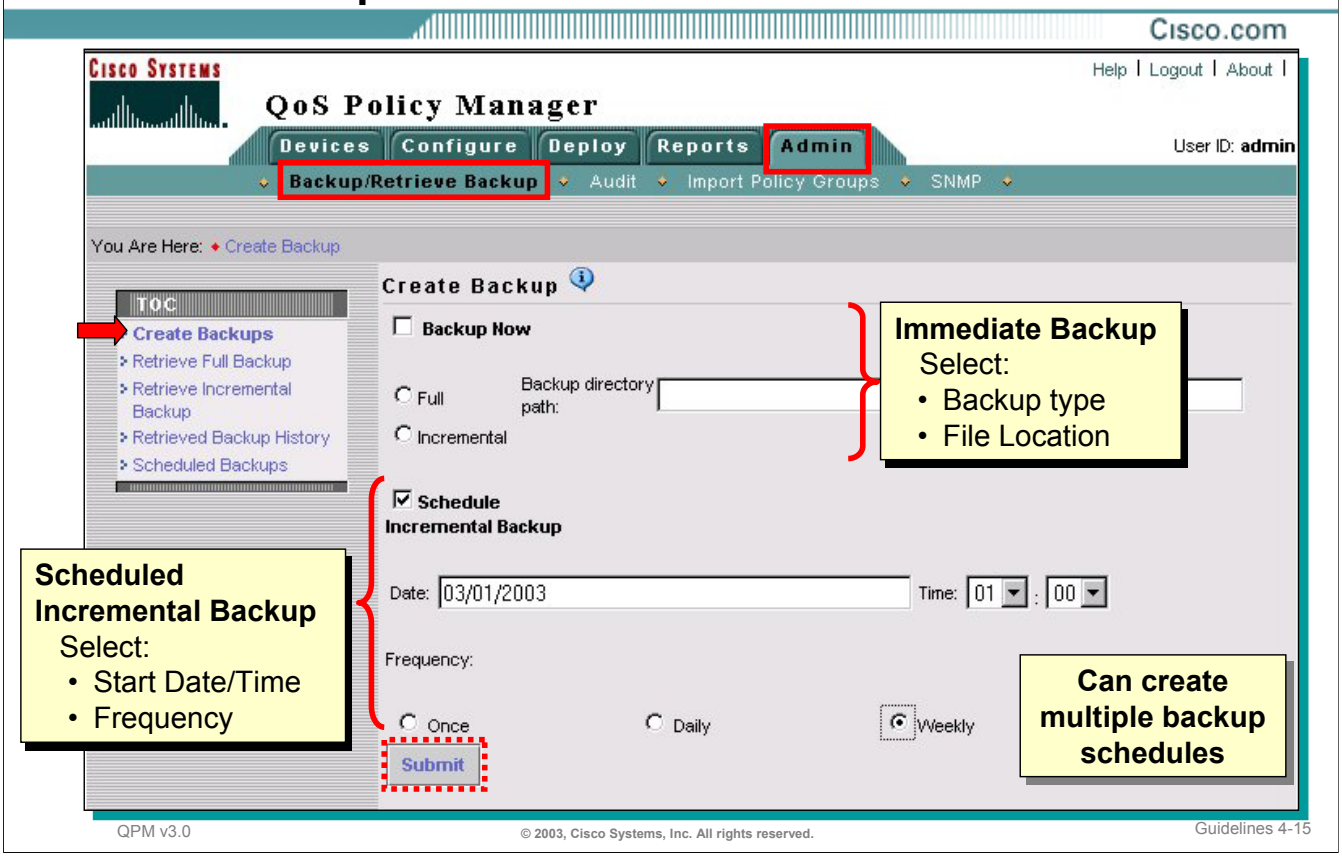
Database Backup/Restore - Overview

It is important to backup the QPM database on a regular basis to avoid losing critical configuration information. QPM v3.0 allows for two types of backups – full and incremental. Both backup types can be performed on-demand, and the incremental backup can be scheduled to automatically execute on a regular basis.

- Full backup – Backs up all the QPM information on the server. Full backups are only performed on-demand. The user must specify a local or networked drive to save the backup to. The backup file name contains the date and time of the backup. QPM can be restored with a full backup, and full backups can be deleted to save disk space.
- Incremental backup – Saves all changes to QPM made since the last incremental backup. These backups are stored in a system defined location on the QPM server. Incremental backups can be create on-demand or can be scheduled to occur on a regular basis. To restore QPM from incremental backups requires all previous incremental backups. Therefore, a single incremental backup cannot be deleted; rather all incremental backups must be deleted.

Tip: Schedule incremental backups to occur on a regular basis. Perform a full backup less frequently and delete all incremental backups after a successful full backup.

Database Backup/Restore
Create Backup



Database Backup/Restore – Create Backup

Use the following procedure to create a full or incremental backup immediately or to schedule an incremental backup:

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.

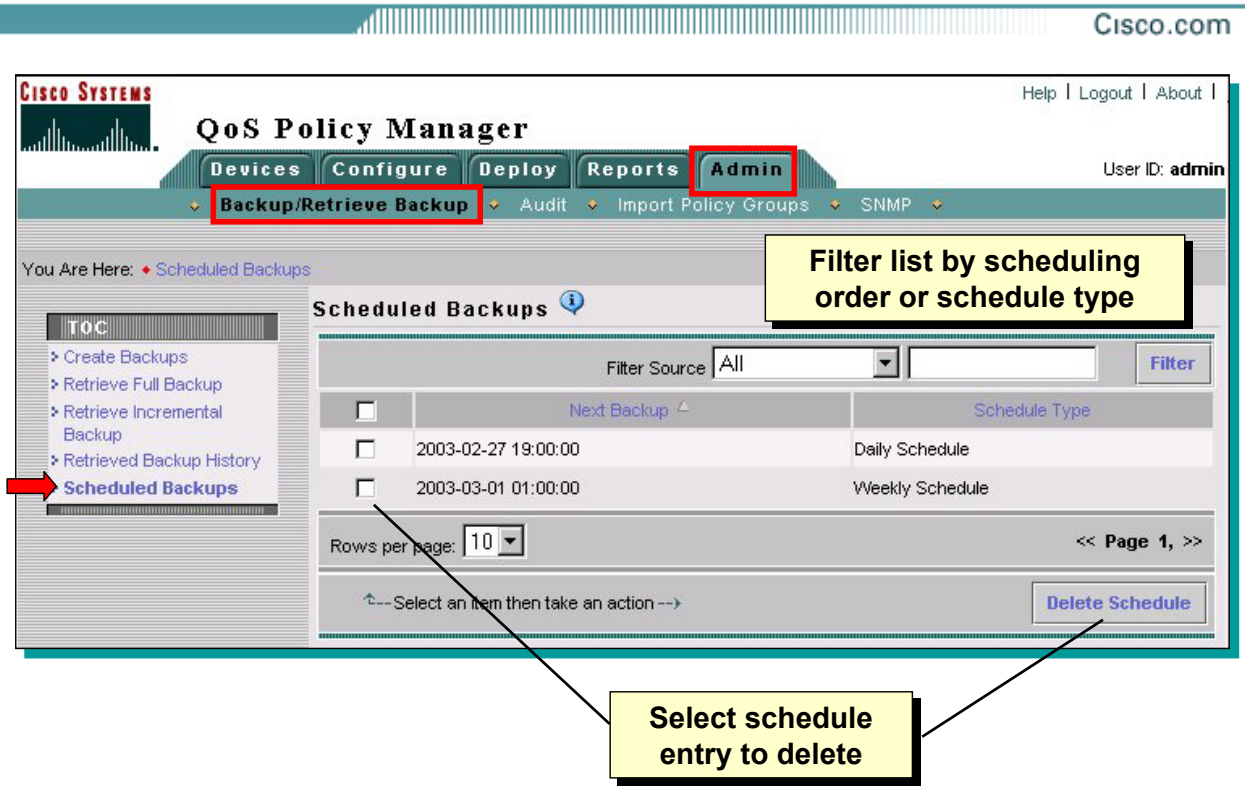
   The *Create Backup* page appears.

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 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.
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.
4. Click *Submit*.

   If an immediate backup was selected, the backup process starts, and the corresponding *Retrieve Backup* page appears.

   If a backup schedule was created, the *Scheduled Backups* page appears displaying the next scheduled backup (multiple times can be selected for scheduling incremental backups).

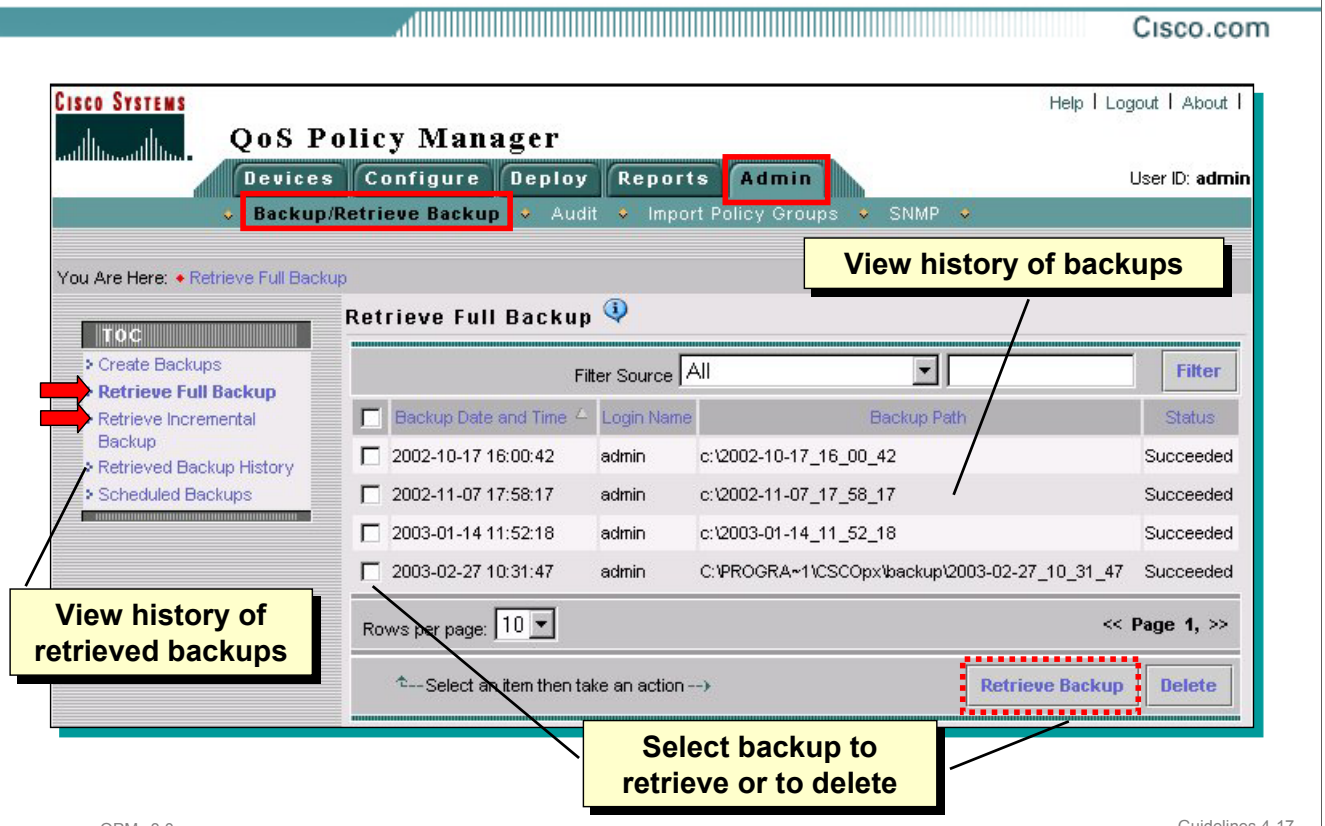
Database Backup/Restore
View Schedule



Database Backup/Restore – View Schedule

After scheduling an incremental backup the *Scheduled Backups* page is displayed. This page can also be viewed at anytime by selecting *Admin* > *Backup/Retrieve Backups* and the *Scheduled Backups* entry in the TOC menu. By default the list displays the scheduled backups in order of next to run. The list can also be filtered by frequency. Use this screen to delete any scheduled incremental backup entry by checking the entry to delete and clicking the *Delete Schedule* button.

Database Backup/Restore
Restore



Database Backup/Retrieval– Restore

In the event of a catastrophe which corrupts the QPM data, the QPM database can be restored by retrieving either a specific full backup or from the incremental backups. The retrieved data overwrites the current data on the QPM server. The retrieve backup pages can also be used to view the success of the backups and to delete them.

Use the following steps to retrieve a full backup (the steps to retrieve an incremental backup would be similar):

1. Select *Admin* > *Backup/Retrieve Backup*. The *Create Backup* page appears.
2. In the TOC in the left pane, select *Retrieve Full Backup*. The *Retrieve Full Backup* page appears displaying a list of full backups.
3. Select the backup you want to retrieve.
4. Click Retrieve Backup. The *Retrieved Backup History* page appears displaying the status and other details of the retrieved backup.
5. Log out of QPM and the CiscoWorks desktop, and restart the QPM server.

   Note: After you retrieve a full backup, all previous incremental backups must be deleted before making incremental backups for the retrieved database.

Deleting a Backup

To delete a full backup, follow steps 1 through 3 above (except select the backup to delete not retrieve) and click the **Delete** button.

Viewing Backup History

After restoring a database the *Retrieved Backup History* page appears. This page can be displayed at any time by selecting *Admin* > *Backup/Retrieve Backup* and the *Retrieved Backup History* entry in the TOC menu.

Audit Logs
Overview

Cisco.com

Track changes made to QPM deployment groups, global libraries, and device information

- **Policy Groups – track changes to policy group properties, policies and policy device group assignment in a specified deployment group**
- **Deployment Groups – track deploy, save, restore, upload, and import actions of a development group (information, warning, and error messages for each action)**
- **Libraries - track changes to IP aliases, application aliases, and policy group templates**
- **General – track changes to QPM device inventory following device rediscovery**

Audit Logs – Overview

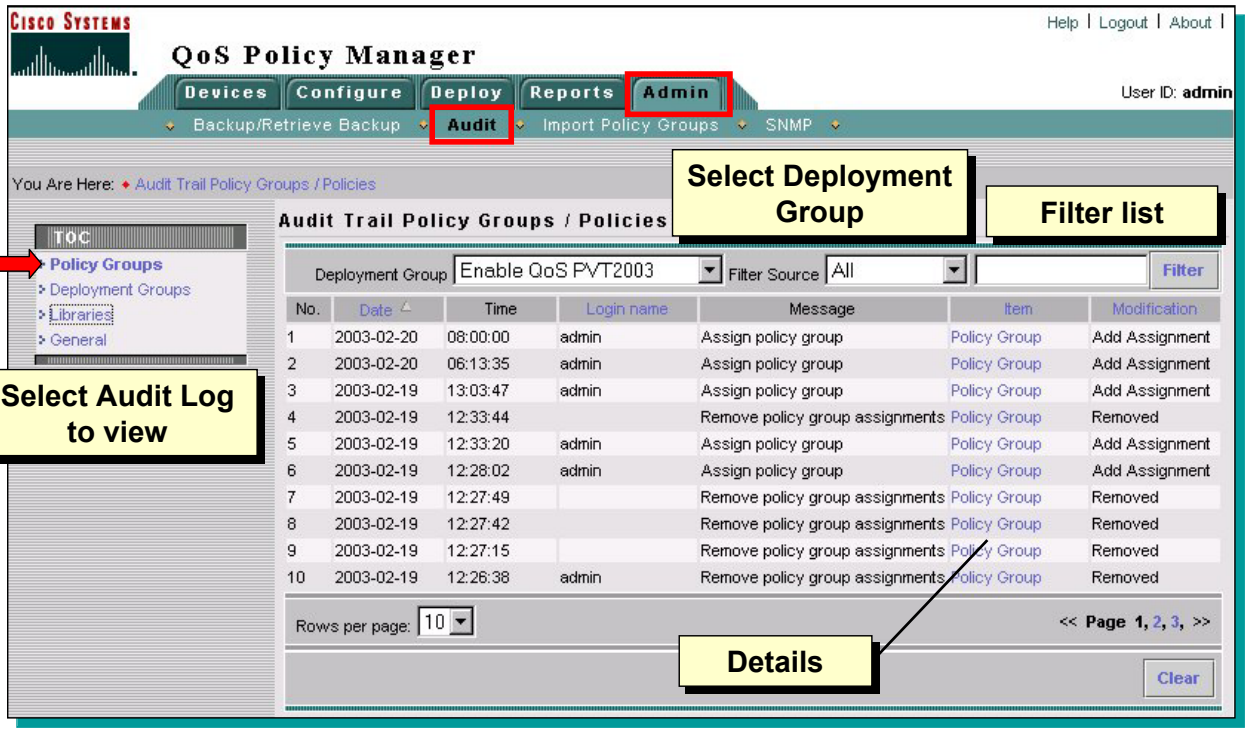
QPM provides the user with an audit trail with information about all changes made to the policy groups in a deployment group, and any deployment group actions. The audit entry registers the modification made, the time of the change, and the login name of the user making the change.

QPM provides 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.

Audit Logs
Viewing



Audit Logs – Viewing

To view the entries in an audit log use the following steps:

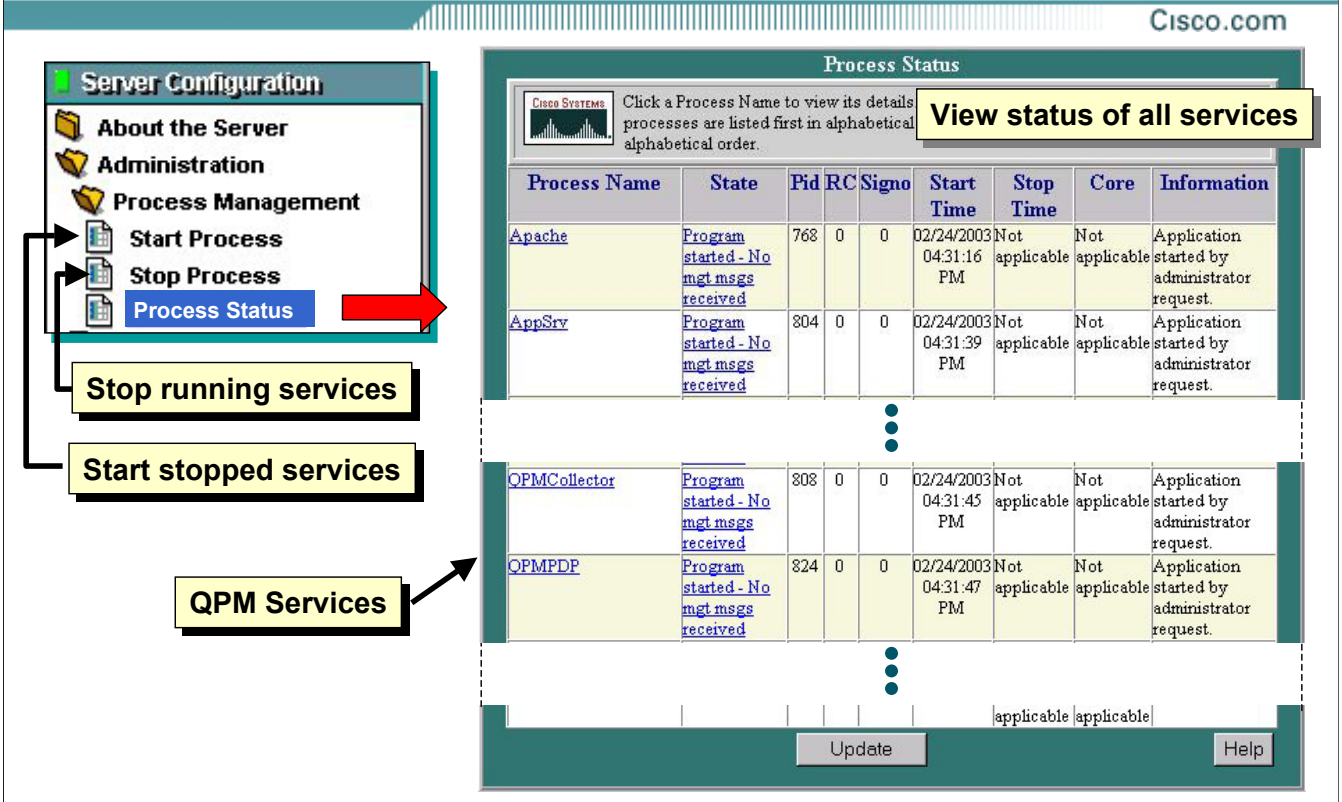
1. Select *Admin* > *Audit*. The *Audit Trail Policy Groups/Policies* page appears.
2. Select the type of logs you want to view in the TOC.
3. For policy groups and deployment groups logs, select the deployment group for which you want to view information.

Deleting Audit Logs

Audit logs no longer needed can be deleted by using the following steps:

1. Select *Admin* > *Audit*. The *Audit Trail Policy Groups/Policies* page appears.
2. Select the type of logs you want to delete in the TOC.
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.
4. Click *Clear*. A Calendar dialog box opens.
5. Use the navigation arrows above the calendar table to navigate through the calendar. In the calendar table, choose the date to the delete logs for.
6. Click *OK*. The audit logs before and including the selected date are deleted, and no longer appear in the Audit display.

System Status



Verify System Status

The CiscoWorks desktop contains tasks that can be used to view the status of the various processes running. Check the system status if QPM appears to hang. If a process is stopped, it can be restarted. Prior to rebooting the server, a poor performing QPM may be stopped and restarted to improve performance.

System Status

1. Select the *Server Configuration* drawer from the navigation menu of the CiscoWorks desktop.
2. Open the *Administration* and Process Management folders.
3. Select the *Process Status* task. The *Process Status* page is displayed. Review the report for any QPM processes which may be stopped.

Starting Processes

1. Select *Server Configuration* > *Administration* > *Process Management* > *Start Process* task from the navigation tree on the CiscoWorks desktop. The *Start Process* page appears.
2. Select *Process* in the start column.
3. Select the process to restart from the Process Name pull-down list.
4. Click *Finish*. The *Process Status* page appears.

Stopping Processes

1. Select *Server Configuration* > *Administration* > *Process Management* > *Stop Process* task from the navigation tree on the CiscoWorks desktop. The *Stop Process* page appears.
2. Select *Process* in the start column.
3. Select the process to stop from the Process Name pull-down list.
4. Click *Finish*. The *Process Status* page appears.

Thank You!

We hope that you have enjoyed using the QPM application and have found its features to be an important part of your network monitoring toolkit.

Cisco Systems

Chapter 5

References

QoS Policy Manager (QPM) v3.0

Reference Materials

Many Cisco reference documents have been created to help users understand the use of the QoS Policy Manager (QPM) application v3.0. However, finding them can often be a challenge. This reference chapter has been created to assist you in your pursuit of additional product information. Below are links to documents and Web pages that provide further details on the QPM product.

- **QoS Policy Manager (QPM) v3.0 Product Information**
  - **Data Sheet (URL)**
  - **User Guide (URL) (PDF)**
  - **Installation Guide (URL) (PDF)**
  - **Quick Start Installation Guide (URL) (PDF)**
  - **Release Notes (URL) (PDF)**
  - **Getting Started Guide (URL) (PDF)**

- **Related Material**
  - **Supported Devices and Software Releases (URL) (PDF)**
  - **Frequently Asked Questions (URL)**

- **Online Bug Tracker (On Line URL)**

  Search for known problems on the Cisco bug tracking system tool, called Bug Toolkit. To access Bug Toolkit, perform the following steps:
  - Click on the link above and click Launch Bug Toolkit.
  - Locate CiscoWorks QoS Policy Manager from the list of Cisco Software Products
  - Then click Next.

- **Technical Notes**
  - **IP Telephony/VoIP Design and Implementation Guide (URL)**

    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.

- **White Papers**
  - **Getting Started with QPM v3.0 (URL)**
  - **Cisco Enterprise: QoS (URL)**

    Overview with links to detailed white papers and other general discussions
  - **Cisco IOS Quality of Service (URL)**

    Links to QoS resources including white papers
  - **Cisco IOS Enabling Network Services (URL)**

    QoS Services--QoS overview with links to white papers on all major QoS technologies
  - **Cisco Enterprise: Design Guidance (URL)**

    General information on designing enterprise networks, including QoS deployment
  - **Quality of Service (Internetworking Technology Overview) (URL)**

    Detailed overview of QoS capabilities
  - **Gigabit Campus Network Design White Paper (URL)**

    General design guidance, including a brief discussion of QoS
  - **Intelligent Service-Level Management: Cisco Tools for Total Control of QoS (URL)**

    How the Cisco QoS Policy Manager (QPM) and Service Management Solution (SMS) work together to enforce and track QoS levels