



# Getting Started Guide for QoS Policy Manager 3.0

CiscoWorks

## Corporate Headquarters

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

Customer Order Number: DOC-7813442=  
Text Part Number: 78-13442-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

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

JClass ServerChart 1.1. Copyright ©1997-2000 by Sitraka Inc. All rights reserved. The JpegEncoder and its associated classes are Copyright (c) 1998, James R. Weeks and BioElectroMech. This software is based in part on the work of the Independent JPEG Group. THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED 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.

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

*Getting Started Guide for QoS Policy Manager 3.0*

Copyright © 1998-2002, Cisco Systems, Inc.

All rights reserved.



## **Preface** vii

Audience vii

Conventions vii

Related Documentation viii

Obtaining Documentation ix

World Wide Web ix

Ordering Documentation ix

Documentation Feedback x

Obtaining Technical Assistance x

Cisco.com xi

Technical Assistance Center xi

Cisco TAC Web Site xii

Cisco TAC Escalation Center xii

---

## **CHAPTER 1**

### **Introduction** 1-1

Lesson 1-1: Getting Started with QPM 1-2

Starting QPM 1-3

Understanding the QPM User Interface 1-4

Exiting QPM 1-6

Lesson 1-2: Importing the Tutorial Virtual Devices 1-7

Lesson 1-3: Creating the Tutorial Device Folder 1-9

Lesson 1-4: Creating the Tutorial Deployment Group 1-11

**Data Network Tutorial 2-1**

Understanding the Data Network Tutorial 2-2

Understanding the Data Network Tutorial Example Network 2-2

Understanding the Data Network Tutorial Devices 2-4

Understanding the Data Network Tutorial Scenarios 2-6

Using the QPM Policy Wizards 2-7

Lesson 2-1: Creating the Campus Access Cat6000 Port Policy Group 2-9

Step 1: Defining the Campus Access Cat6000 Port Policy Group 2-9

Step 2: Defining the Campus Access Cat6000 Port Policy Group QoS Properties 2-12

Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy Group 2-14

Step 4: Creating the ERP Traffic Coloring Policy 2-15

Lesson 2-2: Defining Policy Groups and Policies To Color Campus Web Traffic 2-19

Lesson 2-2-1: Defining the Campus Access VLAN Policy Group 2-19

Step 1: Defining the Campus Access VLAN Policy Group 2-20

Step 2: Assigning Elements to the Campus Access VLAN Policy Group 2-22

Step 3: Creating the Web Traffic Coloring Policy 2-24

Lesson 2-2-2: Defining the Campus Access VLAN Ports Policy Group 2-26

Step 1: Defining the Campus Access VLAN Ports Policy Group 2-27

Step 2: Defining the Campus Access VLAN Ports Policy Group QoS Properties 2-29

Step 3: Assigning Elements to the Campus Access VLAN Ports Policy Group 2-31

Lesson 2-3: Creating the Remote FastEthernet Policy Group 2-32

Step 1: Defining the Remote FastEthernet Policy Group 2-34

Step 2: Defining the Remote FastEthernet Policy Group QoS Properties 2-36

Step 3: Assigning Elements to the Remote FastEthernet Policy Group 2-38

Step 4: Creating the Web Traffic Coloring Policy 2-39

Step 5: Creating the ERP Traffic Coloring Policy	2-42
Lesson 2-4: Creating the WAN PPP Policy Group	2-45
Step 1: Defining the WAN PPP Policy Group	2-46
Step 2: Defining the WAN PPP Policy Group QoS Properties	2-49
Step 3: Assigning Elements to the WAN PPP Policy Group	2-50
Step 4: Creating the MQC CBWFQ Queuing Policies	2-52
Step 4a: Creating the ERP Traffic Queuing Policy	2-53
Step 4b: Creating the Web Traffic Queuing Policy	2-56
Step 4c: Creating the Class Default Policy	2-59
Lesson 2-5: Adding FTP Policing To the Campus Access VLAN Policy Group	2-61
Lesson 2-6: Deploying the Data Network Tutorial Policies	2-64
Lesson 2-7: Monitoring the Deployment Process	2-66

---

**CHAPTER 3****IP Telephony Network Tutorial 3-1**

Understanding the IP Telephony Network Example	3-3
Configuring QoS for the Campus Site	3-4
Configuring QoS for the WAN	3-5
Configuring QoS for the Remote Branch	3-5
Network Example Device Information	3-6
Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard	3-8
Using the IP Telephony Wizard	3-9
Step 1: Introduction	3-11
Step 2: Selecting Devices for QoS Configuration	3-12
Step 3: Selecting the IP Phone Connections	3-15
Step 4: Selecting the SoftPhone Connection	3-17
Step 5: Selecting the CallManager Port	3-19
Step 6: Selecting the IntraLAN Connections	3-21
Step 7: Selecting the Voice VLAN Connections	3-23
Step 8: Selecting the Switch to WAN Router Connection	3-25

Step 9: Selecting the Router WAN to Switch Connection **3-27**

Step 10: Selecting the WAN Frame Relay Connections **3-29**

Step 11: End **3-31**

Lesson 3-2: Modifying the Voice Policies **3-32**

Lesson 3-2-1: Enabling cRTP for the WAN-FR-Main-Interface Voice Policy Group **3-33**

Lesson 3-2-2: Configuring the Voice Traffic Bandwidth for the WAN-FR-DLCI-Slow Voice Policy Group **3-37**

Lesson 3-3: Deploying the IP Telephony QoS Policies **3-45**

Lesson 3-4: Monitoring the Deployment Process **3-47**

---

**CHAPTER 4**

**QoS Analysis Tutorial 4-1**

Understanding QPM Monitoring **4-1**

What is the Purpose of QoS Analysis? **4-2**

What Can You Monitor Using QPM? **4-2**

What Is the Difference Between Historical and Real-Time Monitoring? **4-3**

How Much Disk Space Is Required for Historical Monitoring? **4-4**

Lesson 4-1: Doing a Baseline Traffic Analysis **4-5**

Understanding How to Monitor Traffic for Baseline Analysis **4-5**

Step 1: Filtering Traffic for Analysis **4-6**

Step 2: Setting Up an Historical Monitoring Task **4-11**

Step 3: Reading the Historical Monitoring Graphs **4-13**

Lesson 4-2: Monitoring QoS **4-18**

Lesson 4-3: Monitoring QoS in Real Time **4-28**



## Preface

---

This manual describes getting started with CiscoWorks QoS Policy Manager, and provides scenarios for using it.

## Audience

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

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

## Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	<b>boldface font</b>
Variables for which you supply values	<i>italic font</i>
Displayed session and system information	screen font
Information you enter	<b>boldface screen font</b>
Variables you enter	<i>italic screen font</i>

Item	Convention
Menu items and button names	<b>boldface</b> font
Selecting a menu item	<b>Option&gt;Network Preferences</b>

**Note**

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

**Caution**

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

## Related Documentation

**Note**

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

The following documentation is available:

**PDF Files**

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

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

**Note**

Adobe Acrobat Reader 4.0 or later is required.



### Online Documentation

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

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

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

- Context-sensitive online help for QPM.

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

## Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Ordering Documentation

Cisco documentation is available in these ways:

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

[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

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

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

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

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

We appreciate your comments.

## Obtaining Technical Assistance

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

## Cisco.com

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

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

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

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

<http://www.cisco.com>

## Technical Assistance Center

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

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

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

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

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

## Cisco TAC Web Site

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

<http://www.cisco.com/tac>

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

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

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

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

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

## Cisco TAC Escalation Center

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

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

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

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





# Introduction

---

This tutorial introduces you to QoS Policy Manager (QPM) version 3 and provides examples of many of the tasks that you can perform with it. To make these examples easier to follow, you can practice the procedures on virtual devices that are provided with the product.

This tutorial is not intended as an exhaustive description of QPM's features or of quality of service (QoS) technology. For more information about these topics, refer to the QPM online help and *User Guide for QoS Policy Manager 3.0*.

The tutorial is structured as follows:

- [Chapter 1, “Introduction,”](#) provides information about getting started with the product and the tutorial.
- [Chapter 2, “Data Network Tutorial,”](#) allows you to practice configuring QoS for data networks.
- [Chapter 3, “IP Telephony Network Tutorial,”](#) allows you to practice configuring QoS for voice-over-IP (VoIP) networks.

Chapters 2 and 3 use separate example networks, but the virtual devices on which you perform the tutorial procedures are provided in one virtual device file, which is provided with the product. For more information about the virtual devices, see [“Lesson 1-2: Importing the Tutorial Virtual Devices” section on page 1-7](#).

## Understanding the Tutorial Environment

The QPM environment for the tutorial has the following characteristics:

- The virtual devices you import from the provided file use IP addresses that are within a range designated as internal and private, so they are unlikely to conflict with any real addresses already in your QPM inventory.

- To separate the tutorial policy groups from your existing policy groups, the tutorial instructs you to create a new deployment group for the tutorial. For more information, see [Lesson 1-4: Creating the Tutorial Deployment Group, page 1-11](#).

### **Tutorial User Permission Requirements**

To use the tutorial, you must log into QPM with user permissions to modify devices in the default device group. For more information, see the user permissions information in *Installation Guide for QoS Policy Manager 3.0*.

This chapter includes the following sections:

- [Lesson 1-1: Getting Started with QPM, page 1-2](#)
- [Lesson 1-2: Importing the Tutorial Virtual Devices, page 1-7](#)
- [Lesson 1-3: Creating the Tutorial Device Folder, page 1-9](#)
- [Lesson 1-4: Creating the Tutorial Deployment Group, page 1-11](#)

## **Lesson 1-1: Getting Started with QPM**

The following topics describe getting started with QPM:

- [Starting QPM, page 1-3](#)
- [Understanding the QPM User Interface, page 1-4](#)
- [Exiting QPM, page 1-6](#)



# Starting QPM

QoS Policy Manager is accessed from the CiscoWorks2000 desktop.

## Procedure

---

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

The CiscoWorks2000 desktop is displayed.



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

---



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

---

**Step 2** Log into CiscoWorks with your username and password.  
The CiscoWorks navigation tree appears in the left pane.

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

**Step 4** Click **QPM** under the QoS Policy Manager drawer.  
A Security Alert window opens. Click **Yes** to proceed.  
QPM opens in a separate browser window.

---

## Related Topics

- [Understanding the QPM User Interface, page 1-4](#)
- [Exiting QPM, page 1-6](#)

## Understanding the QPM User Interface

All the pages in the web-based QPM user interface have a consistent look and feel.

Figure 1-1 shows an example of a QPM page.

**Figure 1-1** Example of a QPM Page

The screenshot shows the QoS Policy Manager web interface. The top navigation bar includes the Cisco Systems logo, the title "QoS Policy Manager", and tabs for "Devices", "Configure", "Deploy", "Reports", and "Admin". Below the navigation bar are dropdown menus for "Deployment Groups", "Libraries", "Policy Groups", and "IP Telephony", along with a "Search" field. The user ID "admin" is displayed in the top right corner. A breadcrumb trail reads "You Are Here: Deployment Groups > Policy Groups". A left-hand navigation pane shows a tree structure with "Policy Groups" selected. The main content area displays a table of policy groups under the heading "Policy Groups". The table has columns for Name, Description, Policy Group Template, Voice Role, QoS Properties, In Policies, Out Policies, and Network Elements. The table lists several policy groups, including "Campus Access Cat5000 P", "Campus Access VLAN", "Campus Access VLAN Ports", "Remote FastEthernet", and "WAN PPP". At the bottom of the table, there are controls for "Rows per page" (set to 10) and "Page 1" navigation. A footer bar contains a message "Select an item then take an action" and buttons for "Create", "Edit", "Copy", and "Delete".

Name	Description	Policy Group Template	Voice Role	QoS Properties	In Policies	Out Policies	Network Elements
<input type="checkbox"/> Campus Access Cat5000 P	Colors inbound ERP traffic.				2	1	0 1 Interfaces
<input type="checkbox"/> Campus Access VLAN	Colors outbound web traffic.				0	2	0 1 Vlans
<input type="checkbox"/> Campus Access VLAN Ports	Applies VLAN-based QoS style.				2	0	0 1 Interfaces
<input type="checkbox"/> Remote FastEthernet	Colors web and ERP traffic from remote sites.				1	2	0 2 Interfaces
<input type="checkbox"/> WAN PPP	Applies MQC CBWFQ to ERP and web traffic entering the WAN.				1	0	3 4 Interfaces

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

68300

**Table 1-1 Common GUI Elements in a QPM Page**

Number	Area	Description
1	TOC	<p>Provides up to two additional levels of navigation, if required:</p> <ul style="list-style-type: none"> <li>• A submenu for the selected option.</li> <li>• In a wizard context, this area displays the wizard steps.</li> </ul>
2	Path bar	Provides a context for the displayed page. Indicates from which tab and option the current page is derived.
3	Content area	Displays the pages in which you perform application tasks.
4	QPM tabs	<p>Contains tabs that provide access to QPM functionality. Click a tab to access its options:</p> <ul style="list-style-type: none"> <li>• <b>Devices</b>—Contains options for managing devices and device groups in the QPM inventory.</li> <li>• <b>Configure</b>—Contains options for defining policy groups and policies, and configuring QoS for IP telephony. This tab also includes options for working with global library policy components.</li> <li>• <b>Deploy</b>—Contains options for deploying QoS policies, and for previewing the CLI configuration on the devices. You can also view and restore previously deployed jobs through this tab.</li> <li>• <b>Reports</b>—Provides access to QPM reports, and to the Performance Analysis application.</li> <li>• <b>Admin</b>—Contains additional administration options.</li> </ul>

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

Number	Area	Description
5	Option bar	Displays the options available for the selected tab.
6	QPM banner	<p>Contains the Help, Logout, and About buttons:</p> <ul style="list-style-type: none"> <li>• Click <b>Help</b> to open a window that displays context-sensitive help for the currently displayed page. The Help page also contains help contents, so that you can use this button to access any online help topic.</li> <li>• Click <b>Logout</b> to log out of QPM and close the QPM window.</li> <li>• Click <b>About</b> to display details about the version of the application.</li> </ul>

**Note**

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

Now that you understand the QPM user interface, you are ready to learn how to exit QPM.

**Related Topics**

- [Starting QPM, page 1-3](#)
- [Exiting QPM, page 1-6](#)

## Exiting QPM

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

**Procedure**

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

- Step 2** Click **Logout** in the CiscoWorks2000 Desktop window.  
The CiscoWorks session ends.
- 

Now you are ready to add devices to the QPM device inventory.

#### Related Topics

- [Starting QPM, page 1-3](#)
- [Understanding the QPM User Interface, page 1-4](#)
- [Lesson 1-2: Importing the Tutorial Virtual Devices, page 1-7](#)

## Lesson 1-2: Importing the Tutorial Virtual Devices

A file of the virtual devices that are used in the tutorial is included with QPM. To import the tutorial virtual devices, you must first copy the virtual devices file to your client system.

For information about the virtual devices used in the data network tutorial, see the [Understanding the Data Network Tutorial, page 2-2](#). For information about the devices used in the voice-over-IP network tutorial, see [Understanding the IP Telephony Network Example, page 3-3](#).

Virtual devices are not physical devices, but rather are defined in a file that contains the same device information required to import a physical device. You can import these virtual devices into the inventory and use them to perform the tasks described in the tutorial.

#### Procedure

---

- Step 1** Copy the tutorial virtual devices file from the QPM server to a location you will remember on your client system.

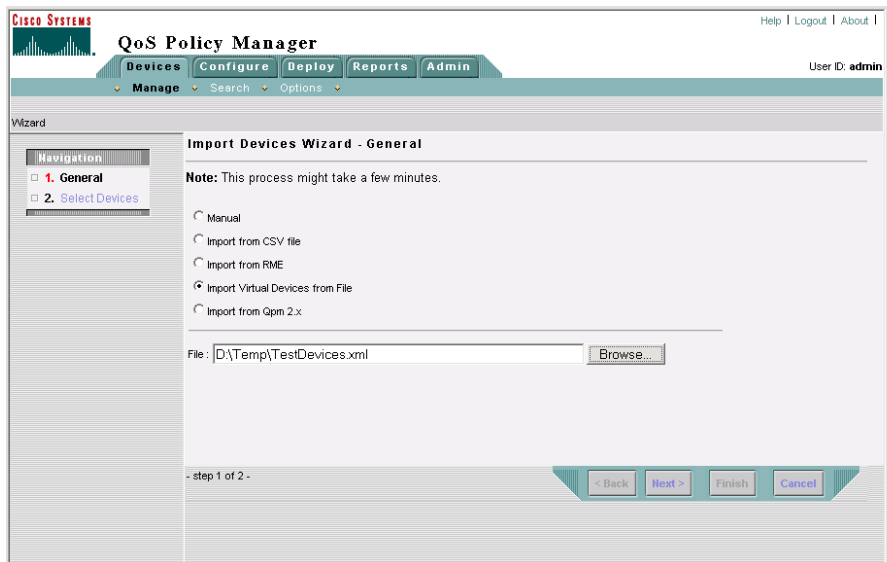
The file is named TutorialDevices.xml. It is located in the Tutorial folder that is located in the CiscoWorks Common Services installation directory on the QPM server at CSCOPx\MDC\qpm\tutorial.

- Step 2** Select **Devices > Manage**. The Device Table page appears.

- Step 3** Select **Add Device**. The Import Devices Wizard - General page appears.

- Step 4** Do the following in the Import Devices Wizard - General page:
- Select the Import Virtual Devices from File radio button.
  - Enter the path to the virtual devices file on your client system in the File field, or click **Browse** to navigate to the file. [Figure 1-2](#) shows the completed Import Devices Wizard - General page.
  - Click **Next**. The Import Devices Wizard - Select Devices page appears.

**Figure 1-2 Lesson 1-2—Importing the Tutorial Virtual Devices**



- Step 5** In the Import Devices Wizard - Select Devices page, select the check box next to all of the devices, then click **Finish**.

QPM imports the devices from the file, and displays the Discovery Status page so you can see the status of the import. The discovery job that you just started is the first entry in the table. Wait until the discovery job is complete, as indicated by an entry appearing in the End column.

- Step 6** Verify that the tutorial virtual devices and their elements were added to the inventory:

- Select **Device Table** from the TOC. The Device Table page appears.  
Note that the imported devices now appear in the device table.

- b. To view the network elements on a device, click the icon in the Interfaces column. The Interfaces page appears, and links to view any other network elements on the device appear in the TOC.
- 

Now that you have imported the tutorial virtual devices, you are ready to create the tutorial deployment group.

#### Related Topics

- [Lesson 1-3: Creating the Tutorial Device Folder, page 1-9](#)
- [Lesson 1-4: Creating the Tutorial Deployment Group, page 1-11](#)

## Lesson 1-3: Creating the Tutorial Device Folder

To make it easier to keep track of the devices used in the tutorial, create a device folder named “Tutorial” for the tutorial and move the tutorial virtual devices into it.

#### Procedure

---

- Step 1** In the **Devices > Manage** TOC, select **Device Folders**. The Device Folders page appears.
- Step 2** Click **Create**. The Device Folder Properties page appears.
- Step 3** Do the following in the Device Folder Properties page:
  - a. Enter **Tutorial** in the Device Folder Name field.
  - b. Enter **Tutorial device folder** in the Description field.
  - c. Click **Save**. The Device Folders page appears.
- Step 4** Select **Device Table** in the TOC. The Device Table page appears.

- Step 5** Do the following in the Device Table page:
- a. Select the tutorial virtual devices by selecting the check boxes next to them.  
The following are the tutorial virtual devices:
    - Access-Cat2900-2
    - Access-Cat3500-2
    - Access-Cat6000-1
    - Access-Cat6000-2
    - Access-Cat6000-3
    - Access-Cat6000-4
    - Core-2600-1
    - Core-3600-1
    - Core-3600-2
    - Core-7200-1
  - b. Click **Set Device Folder**. The Device Folder setting dialog box opens.
- Step 6** Do the following in the Device Folder Setting dialog box:
- a. Select the Set Device Folder radio button.
  - b. Select the radio button next to the Tutorial folder name.
  - c. Click **OK**. The Device Table page refreshes.
- 

### Related Topics

- [Lesson 1-2: Importing the Tutorial Virtual Devices, page 1-7](#)
- [Lesson 1-4: Creating the Tutorial Deployment Group, page 1-11](#)



# Lesson 1-4: Creating the Tutorial Deployment Group

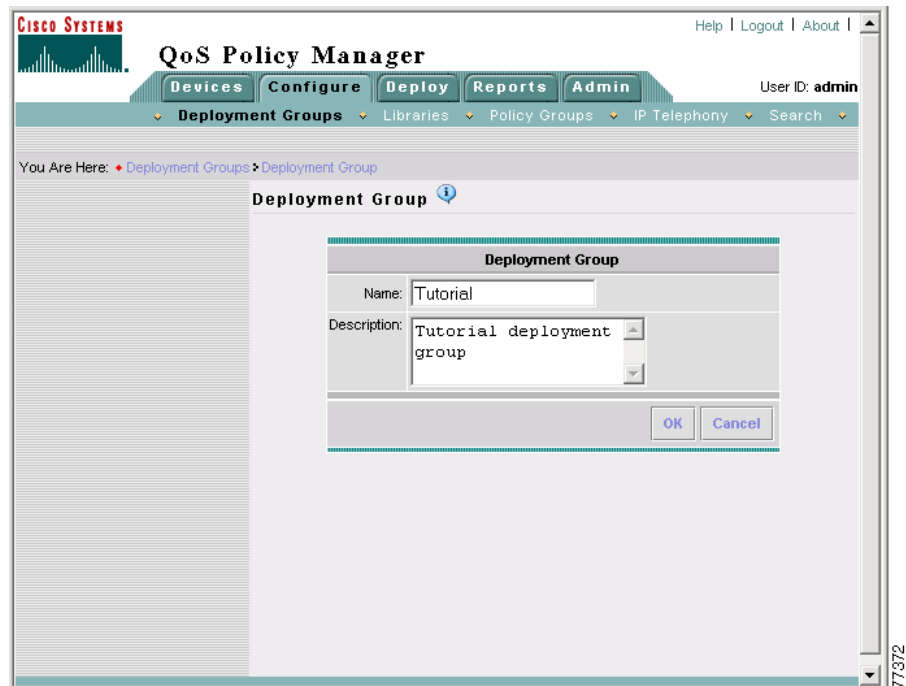
To separate the tutorial policy groups from any existing policy groups, create a deployment group named “Tutorial” for the tutorial.

## Procedure

---

- Step 1** Select **Configure > Deployment Groups**. The Deployment Groups page appears.
- Step 2** Do the following in the Deployment Groups page:
- Click **Create**. The Deployment Group page appears.
  - Enter the name **Tutorial** in the Name field.
  - Enter the description **Tutorial deployment group** in the Description field. [Figure 1-2](#) shows the completed Deployment Group page.
  - Click **OK**. The Deployment Groups page appears.

Figure 1-3 Lesson 1-3—Creating the Tutorial Deployment Group



**Step 3** Verify that the Tutorial deployment group appears in the list.

After completing all the lessons in this chapter, you are ready to proceed with the data network or IP telephony tutorial. You can use the tutorials in any order (they are not sequential).

#### Related Topics

- [Chapter 2, “Data Network Tutorial”](#)
- [Chapter 3, “IP Telephony Network Tutorial”](#)



# Data Network Tutorial

---

This chapter shows you how to configure QoS on a data network using the provided virtual devices. QPM includes a file of virtual devices that you can import into the inventory to create this example network. By working with virtual devices, you can practice using QPM without the risk of working on live devices on your network.

If you have not yet imported the tutorial virtual devices and created the tutorial deployment group, see [Lesson 1-2: Importing the Tutorial Virtual Devices, page 1-7](#) and [Lesson 1-4: Creating the Tutorial Deployment Group, page 1-11](#).

In lessons 2-1 through 2-5, you use QPM techniques and principles to configure QoS on specific segments of this network. In each lesson, a diagram clearly illustrates the relevant network segments, the data path, and the QoS features or policies applied. Lessons 2-6 and 2-7 describe how to deploy the QoS configurations you created in the previous lessons.

This chapter includes the following sections:

- [Understanding the Data Network Tutorial, page 2-2](#)
- [Lesson 2-1: Creating the Campus Access Cat6000 Port Policy Group, page 2-9](#)
- [Lesson 2-2: Defining Policy Groups and Policies To Color Campus Web Traffic, page 2-19](#)
- [Lesson 2-3: Creating the Remote FastEthernet Policy Group, page 2-32](#)
- [Lesson 2-4: Creating the WAN PPP Policy Group, page 2-45](#)
- [Lesson 2-5: Adding FTP Policing To the Campus Access VLAN Policy Group, page 2-61](#)

- [Lesson 2-6: Deploying the Data Network Tutorial Policies, page 2-64](#)
- [Lesson 2-7: Monitoring the Deployment Process, page 2-66](#)

## Understanding the Data Network Tutorial

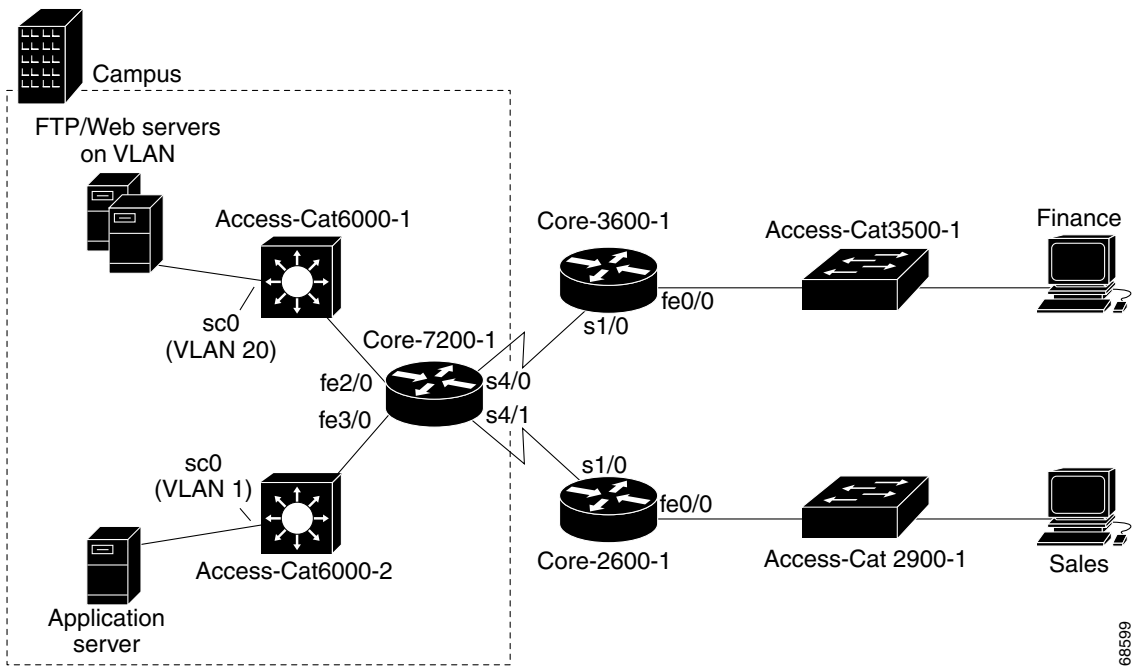
The following topics describe the data network tutorial example network and the scenarios on which the data network tutorial is based:

- [Understanding the Data Network Tutorial Example Network, page 2-2](#)
- [Understanding the Data Network Tutorial Devices, page 2-4](#)
- [Understanding the Data Network Tutorial Scenarios, page 2-6](#)
- [Using the QPM Policy Wizards, page 2-7](#)

## Understanding the Data Network Tutorial Example Network

The data network tutorial is based on an example enterprise data network that consists of a campus site and two remote sites. [Figure 2-1](#) shows the design of the example data network. Interfaces that do not have QoS applied to them in the tutorial are not labeled.

Figure 2-1 Sample Network Used in Data Network Tutorial



68599

### Campus Site

The campus site contains the following components:

- FTP, web, and application servers, which are the major servers used in the network.
- Two Catalyst 6509 switches (Access-Cat6000-1 and Access-Cat6000-2), running Catalyst OS version 6.3.
- A Cisco 7204 router (Core-7200-1), running IOS version 12.2. Packets from the major servers pass through switches Access-Cat6000-1 and Access-Cat6000-2 to this router, and then on to the WAN.

**Remote Site (Finance Users)**

The Finance remote site contains the following components:

- A Cisco 3620 router (Core-3600-1), running IOS version 12.2.
- A Catalyst 3524-XL switch (Access-Cat3500-1), running Catalyst OS 6.3.

The Finance users primarily require data from the application server and the FTP and web servers on the campus site. The primary path of data from these servers is from router Core-7200-1 on the campus site to remote router Core-3600-1.

**Remote Site (Sales Users)**

The Sales remote site contains the following components:

- A Cisco 2621 router (Core-2600-1), running IOS version 12.2.
- A Catalyst 2900 switch (Access-Cat2900-1), running Catalyst OS 6.3.

The Sales users primarily communicate with the application and web servers on the campus site. The primary path of data from these servers to the Sales users is through router Core-7200-1 on the campus site to remote router Core-2600-1.

## Understanding the Data Network Tutorial Devices

The following table provides the technical details of the devices in the example network shown in the preceding figure. Interfaces that do not have QoS applied to them in the tutorial are not listed.

**Table 2-1 Sample Data Network Device Information**

<b>Device Name</b>	<b>Device Model and IP Address</b>	<b>Software Version</b>	<b>Interfaces</b>	<b>IP Address</b>	<b>Mask</b>
Core-7200-1	7204 10.1.1.1	12.2	FastEthernet2/0	10.1.1.1	255.255.255.0
			FastEthernet 100,000 Kbit/sec (100 Mb/sec)		
			FastEthernet3/0	10.1.2.1	255.255.255.0
			FastEthernet 100,000 Kbit/sec (100 Mb/sec)		
			Serial4/0	10.2.2.1	255.255.255.0
	T1 line at 1544 Kbit/second (PPP)				
Core-3600-1	3620 10.3.1.1	12.2	FastEthernet0/0	10.3.1.1	255.255.255.0
			FastEthernet 100,000 Kbit/sec (100 Mb/sec)		
			Serial1/0	10.2.2.2	255.255.255.0
	T1 line at 1544 Kbit/second (PPP)				
Core-2600-1	2621 10.3.2.1	12.2	FastEthernet0/0	10.3.2.1	255.255.255.0
			FastEthernet 100,000 Kbit/sec (100 Mb/sec)		
			Serial1/0	10.2.3.2	255.255.255.0
	T1 line at 512 Kbit/second (PPP)				
Access-Cat6 000-1	6509 10.1.1.2	6.3	SC0 [VLAN 20]	10.1.1.2	255.255.255.0

**Table 2-1 Sample Data Network Device Information (continued)**

Device Name	Device Model and IP Address	Software Version	Interfaces	IP Address	Mask
Access-Cat6 000-2	6509 10.1.2.2	6.3	SC0 [VLAN 1]  Ethernet 10,000 Kbit/sec (10 Mb/sec)	10.1.2.2	255.255.255.0
Application (ERP) Server	10.1.2.3	—	—	—	255.255.255.0

## Understanding the Data Network Tutorial Scenarios

The goal of the data network tutorial is to guide you through the process of creating and deploying QoS policies to the sample network virtual devices. These policies are designed to achieve the goals of the following QoS scenarios.

### Scenario 1—Coloring Campus ERP Traffic

The goal of scenario 1 is to color enterprise resource planning (ERP) traffic that originates from the Campus application servers so that the devices between these servers and the Sales and Finance users can provide good response time for these traffic types.

Implementing this scenario is described in the [Lesson 2-1: Creating the Campus Access Cat6000 Port Policy Group](#), page 2-9.

### Scenario 2—Coloring Campus Web Traffic

The goal of scenario 2 is to color web traffic that originates from the Campus web server so that the devices between it and the Sales and Finance users can provide good response time for this traffic type.

Implementing this scenario is described in the [Lesson 2-2: Defining Policy Groups and Policies To Color Campus Web Traffic](#), page 2-19.



**Scenario 3—Coloring Remote Web and ERP Traffic**

The goal of scenario 3 is to color web and ERP traffic originating from the remote sites so that the devices between these sites and the Campus web and application servers can provide good response time for these traffic types.

Implementing this scenario is described in the [Lesson 2-3: Creating the Remote FastEthernet Policy Group, page 2-32](#).

**Scenario 4—Queuing Web and ERP Traffic at WAN Edge**

The goal of scenario 4 is to queue web and ERP traffic as it leaves the LAN and enters the WAN. This queuing ensures that each traffic type gets the desired percentage of the available bandwidth.

Implementing this scenario is described in [Lesson 2-4: Creating the WAN PPP Policy Group, page 2-45](#).

**Scenario 5—Policing FTP Traffic**

The goal of scenario 5 is to police FTP traffic that originates from the Campus FTP server to limit its usage of network bandwidth.

Implementing this scenario is described in [Lesson 2-5: Adding FTP Policing To the Campus Access VLAN Policy Group, page 2-61](#).

Now that you understand the data network tutorial network and scenarios, you are ready to proceed with the tutorial.

**Related Topics**

- [Lesson 2-1: Creating the Campus Access Cat6000 Port Policy Group, page 2-9](#)

## Using the QPM Policy Wizards

The lessons in this chapter use several QPM policy wizards to create the necessary policy groups and policies.

The following are some tips about how these wizards work:

- Some of the pages contain sections that you can choose to hide or display by clicking the green arrow next to the top of the section. These sections typically contain the following types of content:
  - Advanced, so many users will not need to use it.
  - Very long (for example, lists of devices or interfaces).
- There are two methods of navigating through the wizards:
  - Using the navigation buttons at the bottom of the page: Back to return to the previous step; Next to proceed to the next step; Finish to finish the wizard; Cancel to cancel the wizard. Back, Next, and Finish are not always available, depending on your position in the wizard and whether you have completed enough of it to finish the task.
  - Using the navigation links in the Navigation area to the left of the wizard pages. The Navigation area contains a list entry for each major step in the wizard. If a step name is a link, you can go to that step by clicking the link. If you cannot go directly to a step (for example, because you must enter required information in a prior step first), that step's list entry is not a link.
- Changes are not made to policy groups or policies until you finish a wizard, except in the IP Telephony wizard. At any time before you click the final Finish button in a policy wizard, you can click Cancel to cancel the wizard without saving any changes.
- Changes made to policy groups and policies are not deployed to the network automatically. You must use QPM's deployment process to deploy changes to the network. For more information, see [Lesson 2-6: Deploying the Data Network Tutorial Policies, page 2-64](#).

# Lesson 2-1: Creating the Campus Access Cat6000 Port Policy Group

The Campus Access Cat6000 Port policy group colors ERP traffic that originates from the Campus application server so that the devices between these servers and the Sales and Finance users can provide good response time for these traffic types. It is applied to the ingress interfaces of switch Access-Cat6000-2.

The details of the Campus Access Cat6000 Port policy group are as follows.

- Device Constraints:
  - Catalyst 6000 FastEthernet interfaces
  - CatOS 6.3
- Network Element Assignments: SC0 on switch Access-Cat6000-2
- QoS Properties: QoS Style=Port Based
- QoS Policies: Color ERP traffic DiffServ Code Point (DSCP) 32

Marking ERP traffic as DSCP 32 (which corresponds to IP precedence value 4), indicates that it is higher priority than web traffic, which will be marked as DSCP 16 (which corresponds to IP precedence value 2).

The following topics describe how to create the Campus Access VLAN policy group. Each step assumes that you have completed the previous step:

- [Step 1: Defining the Campus Access Cat6000 Port Policy Group, page 2-9](#)
- [Step 2: Defining the Campus Access Cat6000 Port Policy Group QoS Properties, page 2-12](#)
- [Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy Group, page 2-14](#)
- [Step 4: Creating the ERP Traffic Coloring Policy, page 2-15](#)

## Step 1: Defining the Campus Access Cat6000 Port Policy Group

In this step you define the basic properties of the policy group, including:

- Name
- Description

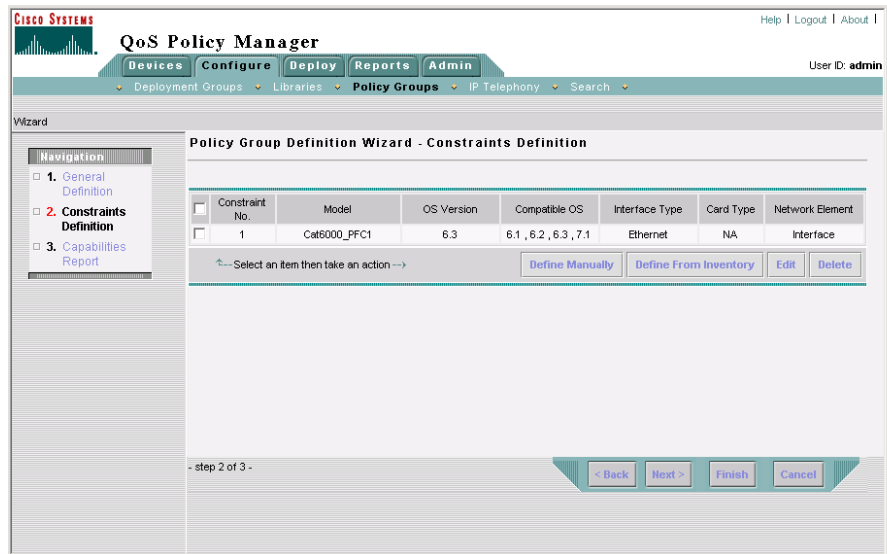
- Constraints:
  - Catalyst 6000 FastEthernet interfaces
  - CatOS 6.3

### Procedure

---

- Step 1** Select **Configure > Policy Groups**. The Policy Groups page appears.
- Step 2** Select **Tutorial** from the Deployment Group list box.  
The page refreshes to display the policy groups in the Tutorial deployment group. If you have not added any policy groups to the deployment group, the list is empty.
- Step 3** Click **Create**. The Policy Group Definition wizard starts.
- Step 4** Do the following in the Policy Group Definition Wizard - General Definition page:
- a. Enter **Campus Access Cat6000 Port** in the Policy Group Name field.
  - b. Enter **Colors inbound ERP traffic** in the Policy Group Description field.
  - c. Do not modify the other page fields.
  - d. Click **Next**. The Policy Group Definition Wizard - Constraints Definition page appears.
- Step 5** Do the following in the Policy Group Definition Wizard - Constraints Definition page:
- a. Click **Define Manually**. The Manual Constraint Definition page appears.
  - b. Select **Cat6000\_PFC1** from the Model list.
  - c. Select **6.3** from the OS Version list.
  - d. Select **Interface** from the Network Element Type list.
  - e. Select **Ethernet** from the Interface Type list.
  - f. Click **OK**. The Policy Group Definition Wizard - Constraints Definition page appears. [Figure 2-2](#) shows the completed Policy Group Definition Wizard - Constraints Definition page.

**Figure 2-2 Lesson 2-1—Campus Access Cat6000 Port Policy Group Constraints Definition Page**



77366

- Step 6** In the Policy Group Definition Wizard - Constraints Definition page, click **Next**. The Policy Group Definition Wizard - Capabilities Report page appears, where you can view a summary of the QoS features that can be configured for the policy group, according to the device constraints.
- Step 7** In the Policy Group Definition Wizard - Capabilities Report page, click **Finish**. The QoS Properties page appears.
- Step 8** You have completed creation of the Campus Access Cat6000 Port policy group. Now you define its QoS properties. Continue with [Step 2: Defining the Campus Access Cat6000 Port Policy Group QoS Properties, page 2-12](#).

### Related Topics

- [Step 2: Defining the Campus Access Cat6000 Port Policy Group QoS Properties, page 2-12](#)

## Step 2: Defining the Campus Access Cat6000 Port Policy Group QoS Properties

This step assumes that you have completed [Step 1: Defining the Campus Access Cat6000 Port Policy Group](#), page 2-9.

In this step you assign the QoS Style=Port Based property to the policy group. The policies in this policy group are defined for individual switch ports and not for the VLAN, therefore the QoS style must be set to port-based.

### Procedure

---

**Step 1** In the QoS Properties page, click **Edit**. The QoS Properties Wizard - Congestion Management page appears.



**Note** If the QoS Properties page is not open, select **Configure > Policy Groups**, then click the QoS Properties link for the Campus Access Cat6000 Port policy group.

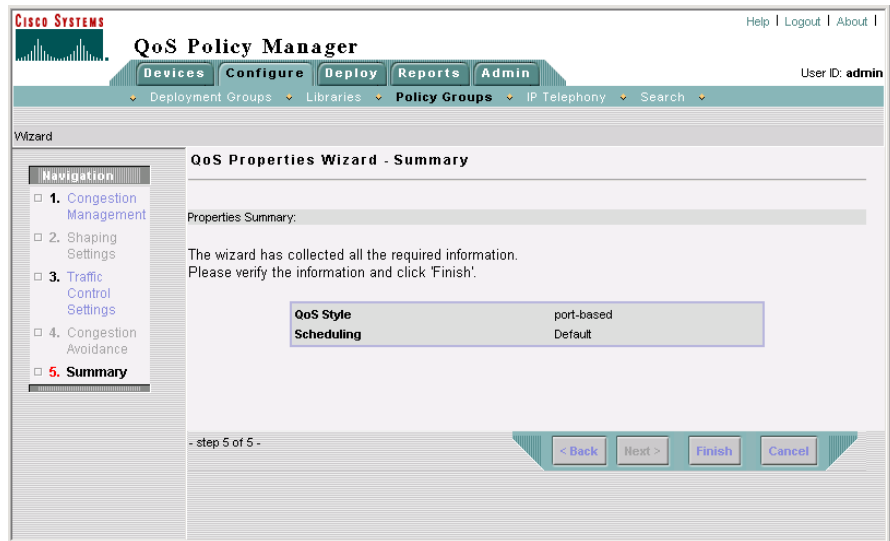
---

**Step 2** In the QoS Properties Wizard - Congestion Management page, click **Next** to accept the page defaults. The QoS Properties Wizard - Traffic Control Settings page appears.

**Step 3** In the QoS Properties Wizard - Traffic Control Settings page:

- Select the Enable QoS Style check box.
- Select the Port based radio button.
- Do not modify the other page fields.
- Click **Finish**. The QoS Properties Wizard - Summary page appears, where you can view a summary of the QoS properties for the policy group. [Figure 2-3](#) shows the QoS Properties Wizard - Summary page.

**Figure 2-3** Lesson 2-1—Campus Access Cat6000 Port Policy Group QoS Properties Wizard - Summary Page



**Step 4** In the QoS Properties Wizard - Summary page, click **Finish**. The QoS Properties page appears.

**Step 5** You have completed defining QoS properties for the Campus Access Cat6000 Port policy group. Now you assign elements to it. Continue with [Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy Group, page 2-14](#).

### Related Topics

- [Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy Group, page 2-14](#)

## Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy Group

This step assumes that you have completed [Step 2: Defining the Campus Access Cat6000 Port Policy Group QoS Properties](#), page 2-12.

In this step you assign the network element SC0 on switch Access-Cat6000-2 to the policy group.

### Procedure

---

**Step 1** Select **Assigned Network Elements** in the TOC. The Assigned Network Elements page appears.



**Note** If the Assigned Network Elements entry does not appear in the TOC, select **Configure > Policy Groups**, then click the Network Elements link for the Campus Access Cat6000 Port policy group.

---

**Step 2** In the Assigned Network Elements page, select **Add**. The Assignment dialog box opens.

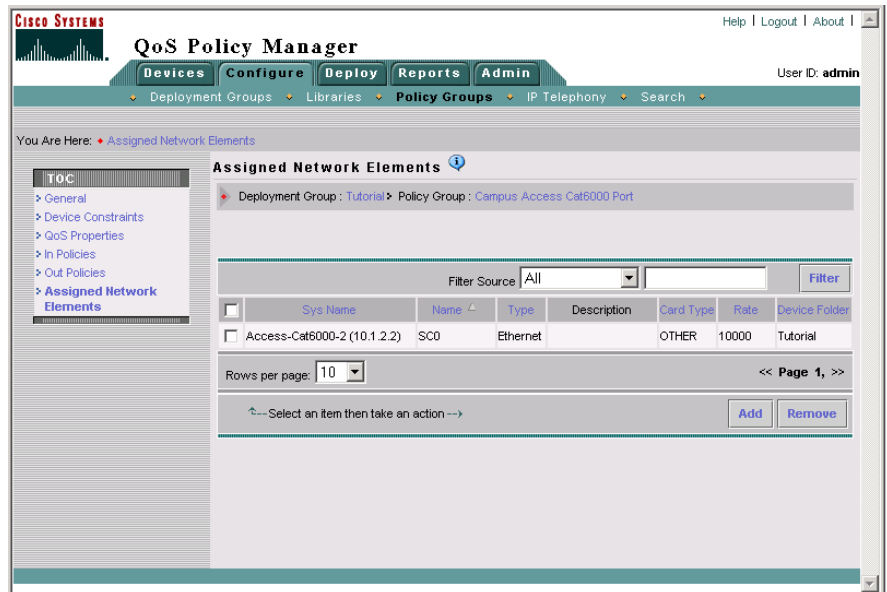
**Step 3** Do the following in the Assignment dialog box:

- a. Select the network element sc0 on switch Access-Cat6000-2 by selecting the check box next to it.
- b. Click **Assign**.

The dialog box closes. The selected network element appears in the Assigned Network Elements page.



**Figure 2-4 Lesson 2-1—Campus Access Cat6000 Port Policy Group Assigned Network Elements Page**



- Step 4** You have completed assigning elements to the Campus Access Cat6000 Port policy group. Now you create the ERP Traffic Coloring policy. Continue with [Step 4: Creating the ERP Traffic Coloring Policy, page 2-15](#).

#### Related Topics

- [Step 4: Creating the ERP Traffic Coloring Policy, page 2-15](#)

## Step 4: Creating the ERP Traffic Coloring Policy

This step assumes that you have completed [Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy Group, page 2-14](#).

In this step you create the ERP Traffic Coloring policy, which colors inbound ERP traffic to DSCP value 32.

## Procedure

---

**Step 1** Select **In Policies** in the TOC. The In Policies page appears.



**Note** If the In Policies entry does not appear in the TOC, select **Configure > Policy Groups**, then click the In Policies link for the Campus Access Cat6000 Port policy group.

---

**Step 2** In the In Policies page, click **Create**. The In Policy wizard opens, displaying the In Policy Wizard - General page.

**Step 3** Do the following in the In Policy Wizard - General page:

- a. Enter **Color ERP traffic** in the Policy Name field.
- b. Enter **Colors inbound ERP traffic** in the Enter Description for the Policy field.
- c. The QoS Policy check box is automatically selected.
- d. Click **Next**. The In Policy Wizard - Filter page appears.

**Step 4** Do the following in the In Policy Wizard - Filter page:

- a. The New Filter check box is automatically selected.
- b. Enter **ERP traffic** in the Filter name field.
- c. Click **Create** to define a filter condition. The Rule Settings page appears.

**Step 5** In the Rule Settings page, click **Edit** in the Protocol row of the Rule Setting table. The Protocol Editor dialog box opens.

**Step 6** Do the following in the Protocol Editor dialog box:

- a. Select the From Library radio button.
- b. Select **TCP** from the Source list box.
- c. Click **OK**. The Protocol Editor dialog box closes, and the Rule Settings page refreshes.

**Step 7** In the Rule Settings page, click **Edit** in the Source IP row of the Rule Setting table. The Source IP Editor dialog box opens.

- Step 8** Do the following in the Source IP Editor dialog box:
- Select the IP Address / Host name list radio button.
  - Enter **10.1.2.3** (the IP address of the ERP server) in the IP/Host field.
  - Enter **255.255.255.0** in the Mask field.
  - Click **Add**. The address is added to the Add a new value list.
  - Click **OK**. The Source IP Editor dialog box closes and the Rule Setting page refreshes.
- Step 9** In the Rule Setting page, click **Done**. The In Policy Wizard - Filter page appears.
- Step 10** In the In Policy Wizard - Filter page, click **Next**. The In Policy Wizard - Marking page appears.
- Step 11** Do the following in the In Policy Wizard - Marking page:
- Select the Value radio button.  
The Enable Marking check box is automatically selected.
  - Select **32 (cs4)** from the Value list box.
  - Click **Finish**. The In Policy Wizard - Summary page appears, where you can view a summary of the policy. [Figure 2-5](#) shows the summary page.

Figure 2-5 Lesson 2-1—Color ERP Traffic Policy Summary Page



**Step 12** In the In Policy Wizard - Summary page, click **Finish**. The In Policies page appears.

**Step 13** Select **Configure > Policy Groups**. The Policy Groups page appears.

Now that you have completed creating the Campus Access Cat6000 Port policy group to color ERP traffic that originates from the Campus application server, you can proceed with the next lesson, [Lesson 2-2: Defining Policy Groups and Policies To Color Campus Web Traffic](#), page 2-19.

#### Related Topics

- [Lesson 2-1: Creating the Campus Access Cat6000 Port Policy Group](#), page 2-9

# Lesson 2-2: Defining Policy Groups and Policies To Color Campus Web Traffic

The goal of this lesson is to apply QoS that colors web traffic that originates from the Campus web server so that the devices between this server and the Sales and Finance users can provide good response time for web traffic.

You will apply this QoS to VLAN20 on switch Access-Cat6000-1. Coloring the traffic at this network location allows the switch to queue the traffic on the egress interfaces before sending the traffic to the WAN. Coloring at the switch is more desirable than coloring at the router between the switch and the WAN because the processing is distributed among more devices, conserving resources on the edge router.

To apply QoS to a VLAN in QPM, you must create two policy groups. The first policy group is assigned to the VLAN network element, and contains the QoS policies. The second policy group is assigned to the member interfaces of the VLAN, and defines the QoS style as VLAN-based.

Therefore, this lesson is divided into two lessons, one for each policy group:

- [Lesson 2-2-1: Defining the Campus Access VLAN Policy Group, page 2-19](#)
- [Lesson 2-2-2: Defining the Campus Access VLAN Ports Policy Group, page 2-26](#)

## Lesson 2-2-1: Defining the Campus Access VLAN Policy Group

The Campus Access VLAN policy group, in combination with the Campus Access VLAN Ports policy group, colors web traffic that originates from the Campus web server so that the devices between this server and the Sales and Finance users can provide good response time for web traffic. It is applied to the VLAN20 interface on switch Access-Cat6000-1.

The details of the Campus Access VLAN policy group are as follows:

- Device constraints:
  - Catalyst 6000 VLAN interfaces
  - CatOS 6.3
- Network Element Assignments: VLAN20 on switch Access-Cat6000-1

- QoS Policies: Color web traffic DSCP 16

Marking web traffic as DSCP 16 (which corresponds to IP precedence value 2), indicates that it is lower priority than ERP traffic, which will be marked as DSCP 32 (which corresponds to IP precedence value 4).

The following topics describe how to create the Campus Access VLAN policy group. Each step assumes that you have just completed the previous step:

- [Step 1: Defining the Campus Access VLAN Policy Group, page 2-20](#)
- [Step 2: Assigning Elements to the Campus Access VLAN Policy Group, page 2-22](#)
- [Step 3: Creating the Web Traffic Coloring Policy, page 2-24](#)

## Step 1: Defining the Campus Access VLAN Policy Group

In this step you define the basic properties of the policy group, including:

- Name
- Description
- Device constraints:
  - Catalyst 6000 VLAN interfaces
  - CatOS 6.3

### Procedure

- 
- Step 1** Select **Configure > Policy Groups**. The Policy Groups page appears.
  - Step 2** Select **Tutorial** from the Deployment Group list box. The page refreshes to display the policy groups in the Tutorial deployment group.
  - Step 3** Click **Create**. The Policy Group Definition wizard starts.
  - Step 4** Do the following in the Policy Group Definition Wizard - General Definition page:
    - a. Enter **Campus Access VLAN** in the Policy Group Name field.
    - b. Enter **Colors outbound web traffic** in the Policy Group Description field.

- c. Do not modify the other page fields.
  - d. Click **Next**. The Policy Group Definition Wizard - Constraints Definition page appears.
- Step 5** Do the following in the Policy Group Definition Wizard - Constraints Definition page:
- a. Click **Define Manually**. The Manual Constraint Definition page appears.
  - b. Select **Cat6000\_PFC1** from the Model list.
  - c. Select **6.3** from the OS Version list.
  - d. Select **VLAN** from the Network Element Type list.
  - e. Click **OK**. The Policy Group Definition Wizard - Constraints Definition page appears. [Figure 2-6](#) shows the completed Policy Group Definition Wizard - Constraints Definition page.

**Figure 2-6 Lesson 2-2-1—Campus Access VLAN Policy Group Constraints Definition Page**



77960

- Step 6** In the Policy Group Definition Wizard - Constraints Definition page, click **Next**. The Policy Group Definition Wizard - Capabilities Report page appears, where you can view a summary of the QoS features that can be configured for the policy group, according to the device constraints.
- Step 7** In the Policy Group Definition Wizard - Capabilities Report page, click **Finish**. The QoS Properties page appears.
- This policy group uses the default QoS properties, so there is no need to edit them.
- Step 8** You have completed creation of the Campus Access VLAN Policy Group. Now assign network elements to it. Continue with [Step 2: Assigning Elements to the Campus Access VLAN Policy Group, page 2-22](#).
- 

#### Related Topics

- [Step 2: Assigning Elements to the Campus Access VLAN Policy Group, page 2-22](#)

## Step 2: Assigning Elements to the Campus Access VLAN Policy Group

This step assumes that you have completed [Step 1: Defining the Campus Access VLAN Policy Group, page 2-20](#).

In this step you assign the network element VLAN20 on switch Access-Cat6000-1 to the policy group.

#### Procedure

---

- Step 1** Select **Assigned Network Elements** in the TOC. The Assigned Network Elements page appears.



**Note** If the Assigned Network Elements entry does not appear in the TOC, select **Configure > Policy Groups**, then click the Network Elements link for the Campus Access VLAN policy group.

---

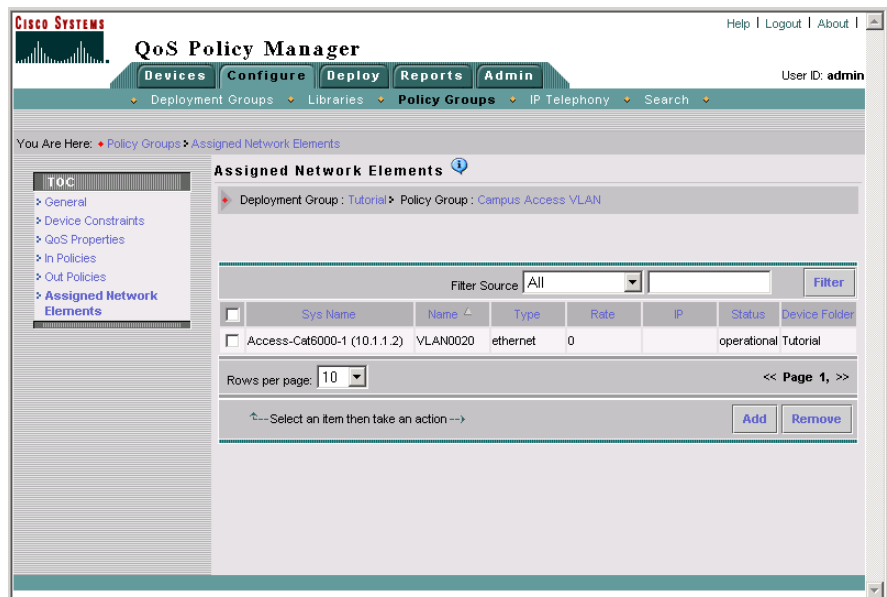
- Step 2** In the Assigned Network Elements page, select **Add**. The Assignment dialog box opens.



- Step 3** Do the following in the Assignment dialog box:
- Select the network element VLAN0020 on device Access-Cat6000-1 by selecting the check box next to it.
  - Click **Assign**.

The dialog box closes. The selected network element appears in the Assigned Network Elements page. [Figure 2-7](#) shows the completed Assigned Network Elements page.

**Figure 2-7 Lesson 2-2-1—Campus Access VLAN Policy Group Assigned Network Elements Page**



- Step 4** You have completed assigning elements to the Campus Access VLAN Policy Group. Now you create the Web Traffic Coloring policy. Continue with [Step 3: Creating the Web Traffic Coloring Policy, page 2-24](#).

### Related Topics

- [Step 3: Creating the Web Traffic Coloring Policy, page 2-24](#)

## Step 3: Creating the Web Traffic Coloring Policy

This step assumes that you have completed [Step 2: Assigning Elements to the Campus Access VLAN Policy Group, page 2-22](#).

In this step you create the Web Traffic Coloring policy, which colors inbound web traffic to DSCP value 16.

### Procedure

---

**Step 1** Select **In Policies** in the TOC. The In Policies page appears.



**Note** If the In Policies entry does not appear in the TOC, select **Configure > Policy Groups**, then click the In Policies link for the Campus Access VLAN policy group.

---

**Step 2** In the In Policies page, click **Create**. The Policy wizard opens, displaying the In Policy Wizard - General page.

**Step 3** Do the following in the In Policy Wizard - General page:

- Enter **Color web traffic** in the Policy Name field.
- Enter **Colors web traffic** in the Description field.
- The QoS Policy check box is automatically selected.
- Click **Next**. The In Policy Wizard - Filter page appears.

**Step 4** Do the following in the In Policy Wizard - Filter page:

- The New Filter check box is automatically selected.
- Enter **Web Traffic** in the Filter Name field.
- Click **Create**. The Rule Settings page appears.

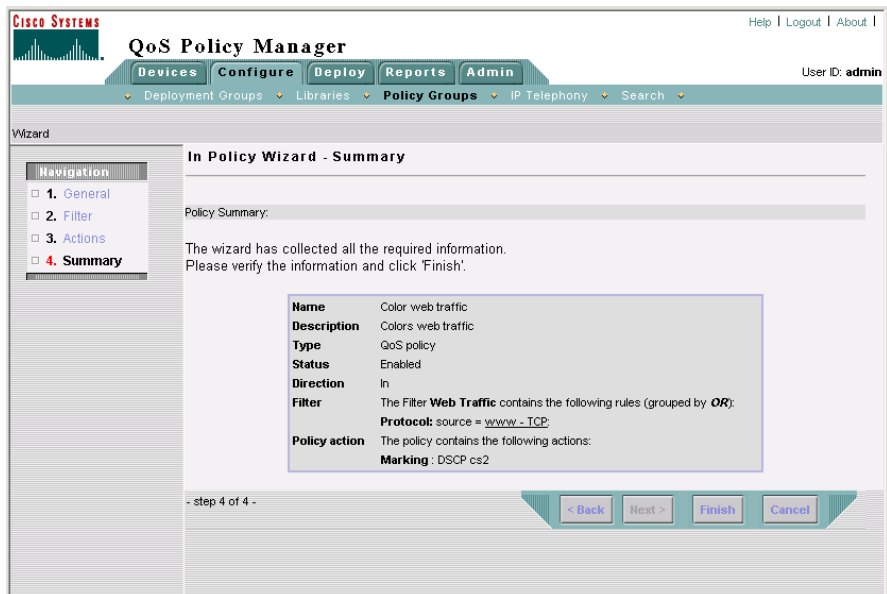
**Step 5** In the Rule Settings page, click **Edit** in the Protocol table row. The Protocol Editor dialog box opens.

**Step 6** Do the following in the Protocol Editor dialog box:

- Select the From Library radio button.
- Select **www-TCP** from the Source list box.

- c. Click **OK**. The Protocol Editor dialog box closes. The Rule Setting page updates in the main QPM window.
- Step 7** In the Rule Settings page, click **Done**. The In Policy Wizard - Filter page appears.
- Step 8** In the In Policy Wizard - Filter page, click **Next**. The In Policy Wizard - Marking page appears.
- Step 9** Do the following in the In Policy Wizard - Marking page:
- Select the Value radio button.  
The Enable Marking check box is automatically selected.
  - Select **16 (cs2)** from the Value list box.
  - Click **Finish**. The In Policy Wizard - Summary page appears, where you can view a summary of the policy. [Figure 2-8](#) shows the completed In Policy Wizard - Summary page.
  - Click **Finish**. The In Policies page appears.

**Figure 2-8 Lesson 2-2-1—Web Traffic Coloring Policy In Policy Wizard - Summary Page**



77961

**Step 10** Select **Configure > Policy Groups** to open the Policy Groups page.

---

Now that you have completed creating the Campus Access VLAN policy group to color web traffic that originates from the Campus web server, you can proceed with the next lesson, [Lesson 2-2-2: Defining the Campus Access VLAN Ports Policy Group](#), page 2-26.

#### Related Topics

- [Lesson 2-2-2: Defining the Campus Access VLAN Ports Policy Group](#), page 2-26

## Lesson 2-2-2: Defining the Campus Access VLAN Ports Policy Group

The Campus Access VLAN Ports policy group, in combination with the Campus Access VLAN policy group, colors web traffic that originates from the Campus web server so that the devices between this server and the Sales and Finance users can provide good response time for web traffic. It is applied to the interfaces that are members of VLAN20 on switch Access-Cat6000-1.

This policy group defines the QoS style for its assigned ports as VLAN-based. This means that the VLAN policies in the Campus Access VLAN policy group will be deployed to these ports. Therefore this policy group does not contain any policies.

The details of the Campus Access VLAN policy group are as follows.

- Device constraints:
  - Catalyst 6000 Ethernet interfaces
  - CatOS 6.3
- Network Element Assignments: Member interfaces of VLAN20 on switch Access-Cat6000-1
- QoS Properties: QoS style=VLAN-based

The following topics describe how to create the Campus Access VLAN Ports policy group. Each step assumes that you have just completed the previous step:

- [Step 1: Defining the Campus Access VLAN Ports Policy Group](#), page 2-27

- [Step 2: Defining the Campus Access VLAN Ports Policy Group QoS Properties, page 2-29](#)
- [Step 3: Assigning Elements to the Campus Access VLAN Ports Policy Group, page 2-31](#)

## Step 1: Defining the Campus Access VLAN Ports Policy Group

In this step you define the basic properties of the policy group, including:

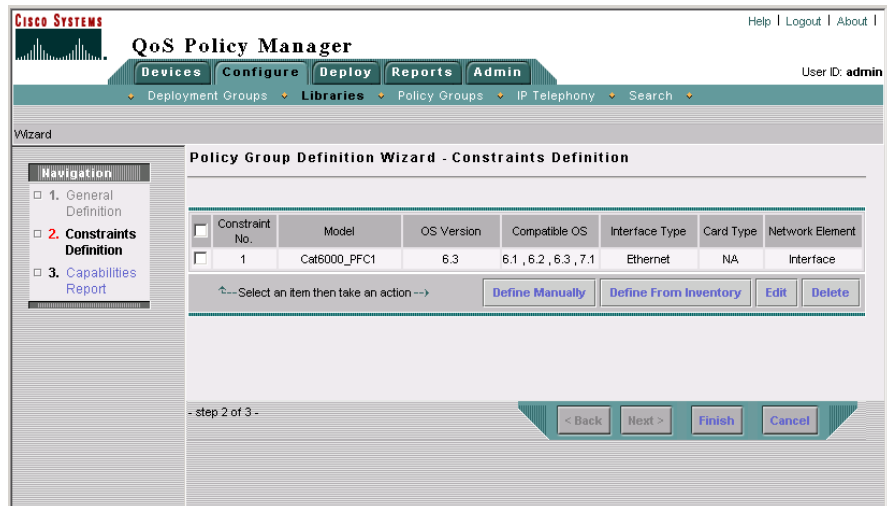
- Name
- Description
- Device constraints:
  - Catalyst 6000 Ethernet interfaces
  - CatOS 6.3

### Procedure

- 
- Step 1** Select **Configure > Policy Groups**. The Policy Groups page appears.
  - Step 2** Select **Tutorial** from the Deployment Group list box. The page refreshes to display the policy groups in the Tutorial deployment group.
  - Step 3** Click **Create**. The Policy Group Definition wizard starts.
  - Step 4** Do the following in the Policy Group Definition Wizard - General Definition page:
    - Enter **Campus Access VLAN Ports** in the Policy Group Name field.
    - Enter **Applies VLAN Based QoS Style** in the Policy Group Description field.
    - Do not modify the other page fields.
    - Click **Next**. The Policy Group Definition Wizard - Constraints Definition page appears.
  - Step 5** Do the following in the Policy Group Definition Wizard - Constraints Definition page:
    - Click **Define Manually**. The Manual Constraint Definition page appears.
    - Select **Cat6000\_PFC1** from the Model list.
    - Select **6.3** from the OS Version list.

- d. Select **Interface** from the Network Element Type list.
- e. Select **Ethernet** from the Interface Type list.
- f. Click **OK**. The Policy Group Definition Wizard - Constraints Definition page appears. [Figure 2-9](#) shows the completed Policy Group Definition Wizard - Constraints Definition page.

**Figure 2-9** Lesson 2-2-2—Campus Access VLAN Ports Policy Group Definition Wizard - Constraints Definition Page



- Step 6** In the Policy Group Definition Wizard - Constraints Definition page, click **Next**. The Policy Group Definition Wizard - Capabilities Report page appears, where you can view a summary of the QoS features that can be configured for the policy group, according to the device constraints.
- Step 7** In the Policy Group Definition Wizard - Capabilities Report page, click **Finish**. The QoS Properties page appears.
- Step 8** You have completed creation of the Campus Access VLAN Ports policy group. Now you define its properties. Continue with [Step 2: Defining the Campus Access VLAN Ports Policy Group QoS Properties](#), page 2-29.

### Related Topics

- [Step 2: Defining the Campus Access VLAN Ports Policy Group QoS Properties, page 2-29](#)

## Step 2: Defining the Campus Access VLAN Ports Policy Group QoS Properties

This step assumes that you have completed [Step 1: Defining the Campus Access VLAN Ports Policy Group, page 2-27](#).

In this step you assign the QoS Style=VLAN Based QoS property to the policy group.

### Procedure

- 
- Step 1** In the QoS Properties page, click **Edit**. The QoS Properties Wizard - Congestion Management page appears.



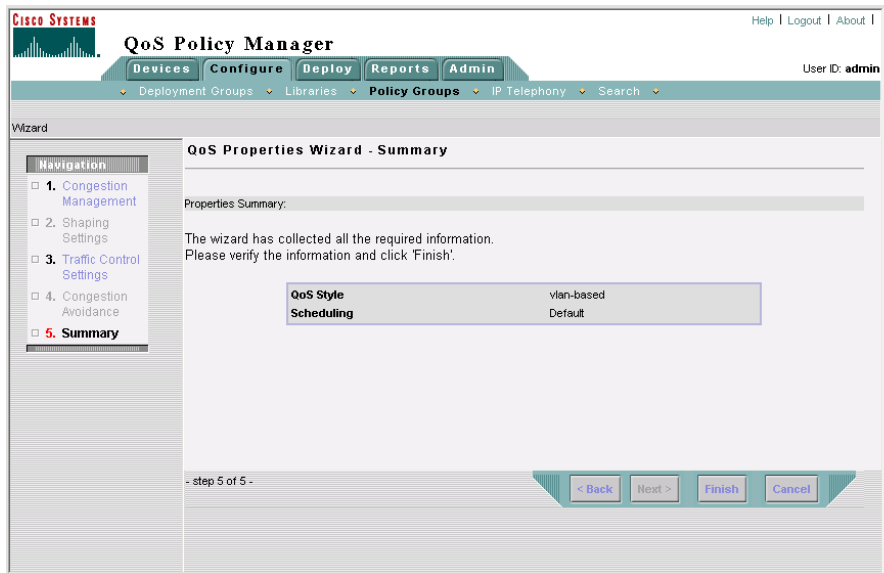
---

**Note** If the QoS Properties page is not open, select **Configure > Policy Groups**, then click the QoS Properties link for the Campus Access VLAN Ports policy group.

---

- Step 2** In the QoS Properties Wizard - Congestion Management page, click **Next** to accept the page defaults. The QoS Properties Wizard - Traffic Control Settings page appears.
- Step 3** Do the following in the QoS Properties Wizard - Traffic Control Settings page:
- Select the Enable QoS Style check box.
  - Select the VLAN based radio button.
  - Do not modify the other page fields.
  - Click **Next**. The QoS Properties Wizard - Summary page appears. [Figure 2-10](#) shows the QoS Properties Wizard - Summary page.

**Figure 2-10** Lesson 2-2-2—Campus Access VLAN Ports Policy Group QoS Properties Wizard - Summary Page



- Step 4** In the QoS Properties Wizard - Summary page, click **Finish**. The QoS Properties page appears.
- Step 5** You have completed defining the QoS properties of the Campus Access VLAN Ports policy group. Now you assign network elements to it. Continue with [Step 3: Assigning Elements to the Campus Access VLAN Ports Policy Group, page 2-31](#).

### Related Topics

- [Step 3: Assigning Elements to the Campus Access VLAN Ports Policy Group, page 2-31](#)



## Step 3: Assigning Elements to the Campus Access VLAN Ports Policy Group

This step assumes that you have completed [Step 2: Defining the Campus Access VLAN Ports Policy Group QoS Properties](#), page 2-29.

In this step you assign the interfaces that are assigned to VLAN20 on switch Access-Cat6000-1 to the policy group.

### Procedure

---

**Step 1** Select **Assigned Network Elements** in the TOC. The Assigned Network Elements page appears.



**Note** If the Assigned Network Elements entry does not appear in the TOC, select **Configure > Policy Groups**, then click the Network Elements link for the Campus Access VLAN Ports policy group.

---

**Step 2** In the Assigned Network Elements page, select **Add**. The Assignment dialog box opens.

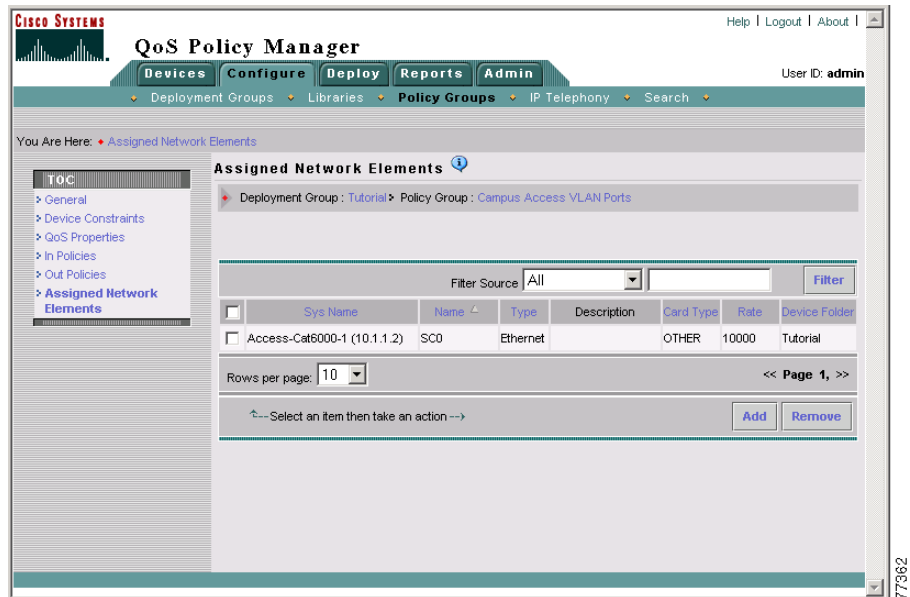
**Step 3** Do the following in the Assignment dialog box:

- a. Select the network element sc0 on device Access-Cat6000-1 by selecting the check box next to it.
- b. Click **Assign**.

The dialog box closes. The selected network element appears in the Assigned Network Elements page. [Figure 2-11](#) shows the completed Assigned Network Elements page.

---

**Figure 2-11** Lesson 2-2-2—Campus Access VLAN Ports Policy Group Assigned Network Elements Page



Now that you have completed defining policy groups and policies to color campus web traffic, you can proceed with the next lesson, [Lesson 2-3: Creating the Remote FastEthernet Policy Group](#), page 2-32.

#### Related Topics

- [Lesson 2-3: Creating the Remote FastEthernet Policy Group](#), page 2-32

## Lesson 2-3: Creating the Remote FastEthernet Policy Group

The Remote FastEthernet policy group colors web and ERP traffic originating from the remote sites so that the devices between these sites and the Campus web and application servers can provide good response time for these traffic types. It is applied to the ingress FastEthernet interfaces of routers Core-3600-1 and Core-2600-1.

Coloring this traffic at these interfaces allows the routers to queue these traffic types on the egress interfaces (based on color) before sending the traffic to the WAN. This policy group is necessary because the switches at the remote sites cannot color traffic, so the coloring must be done at the routers.

The details of the Remote FastEthernet policy group are as follows.

- Device Constraints:
  - 2600 Series and 3600 Series Ethernet interfaces
  - Cisco IOS 12.2
- Network Element Assignments:
  - FastEthernet interface 0/0 on router Core-3600-1
  - FastEthernet interface 0/0 on router Core-2600-1
- QoS Properties: Class-based QoS
- QoS Policies:
  - Color web traffic DSCP 16
  - Color ERP traffic DSCP 32

Marking web traffic as DSCP 16 (which corresponds to IP precedence value 2), indicates that it is lower priority than ERP traffic, which is marked as DSCP 32 (which corresponds to IP precedence value 4).

The following topics describe how to create the Remote FastEthernet policy group. Each step assumes that you have just completed the previous step:

- [Step 1: Defining the Remote FastEthernet Policy Group, page 2-34](#)
- [Step 2: Defining the Remote FastEthernet Policy Group QoS Properties, page 2-36](#)
- [Step 3: Assigning Elements to the Remote FastEthernet Policy Group, page 2-38](#)
- [Step 4: Creating the Web Traffic Coloring Policy, page 2-39](#)
- [Step 5: Creating the ERP Traffic Coloring Policy, page 2-42](#)

## Step 1: Defining the Remote FastEthernet Policy Group

In this step you define the basic properties of the policy group, including:

- Name
- Description
- Constraints:
  - 2600 Series and 3600 Series Ethernet interfaces
  - Cisco IOS 12.2

### Procedure

---

- Step 1** Select **Configure > Policy Groups**. The Policy Groups page appears.
- Step 2** Select **Tutorial** from the Deployment Group list box. The page refreshes to display the policy groups in the Tutorial deployment group.
- Step 3** Click **Create**. The Policy Group Definition wizard starts.
- Step 4** Do the following in the Policy Group Definition Wizard - General Definition page:
- a. Enter **Remote FastEthernet** in the Policy Group Name field.
  - b. Enter **Colors web and ERP traffic from remote sites** in the Policy Group Description field.
  - c. Do not modify the other page fields.
  - d. Click **Next**. The Policy Group Definition Wizard - Constraints Definition page appears.
- Step 5** Do the following in the Policy Group Definition Wizard - Constraints Definition page:
- a. Click **Define Manually**. The Manual Constraint Definition page appears.
  - b. Select **2600** from the Model list.
  - c. Select **12.2** from the OS Version list.
  - d. Select **Interface** from the Network Element Type list.

- e. Select **Ethernet** from the Interface Type list.
- f. Click **OK**. The Policy Group Definition Wizard - Constraints Definition page appears.

**Step 6** Do the following in the Policy Group Definition Wizard - Constraints Definition page:

- a. Click **Define Manually**. The Manual Constraint Definition page appears.
- b. Select **3600** from the Model list.
- c. Select **12.2** from the OS Version list.
- d. Interface is automatically entered in the Network Element Type list.
- e. Select **Ethernet** from the Interface Type list.
- f. Click **OK**. The Policy Group Definition Wizard - Constraints Definition page appears. [Figure 2-12](#) shows the completed Policy Group Definition Wizard - Constraints Definition page.

**Figure 2-12 Lesson 2-2-2—Remote FastEthernet Policy Group Definition Wizard - Constraints Definition Page**

The screenshot shows the QoS Policy Manager web interface. The main title is "QoS Policy Manager" with a navigation menu including "Devices", "Configure", "Deploy", "Reports", and "Admin". The user is logged in as "admin". The current page is the "Policy Group Definition Wizard - Constraints Definition" page. On the left, there is a "Navigation" sidebar with three items: "1. General Definition", "2. Constraints Definition" (which is selected), and "3. Capabilities Report". The main content area features a table with the following data:

Constraint No.	Model	OS Version	Compatible OS	Interface Type	Card Type	Network Element
<input type="checkbox"/> 1	2600	12.2	12.2, 12.2T	Ethernet	NA	Interface
<input type="checkbox"/> 2	3600	12.2	12.2, 12.2T	Ethernet	NA	Interface

Below the table, there is a prompt: "Select an item then take an action -->". To the right of this prompt are four buttons: "Define Manually", "Define From Inventory", "Edit", and "Delete". At the bottom of the page, there is a progress indicator: "- step 2 of 3 -" and four navigation buttons: "< Back", "Next >", "Finish", and "Cancel".

77368

- Step 7** In the Policy Group Definition Wizard - Constraints Definition page, click **Next**. The Policy Group Definition Wizard - Capabilities Report page appears, where you can view a summary of the QoS features that can be configured for the policy group, according to the device constraints.
- Step 8** In the Policy Group Definition Wizard - Capabilities Report page, click **Finish**. The QoS Properties page appears.
- Step 9** You have completed creation of the Remote FastEthernet policy group. Now you define its QoS properties. Continue with [Step 2: Defining the Remote FastEthernet Policy Group QoS Properties, page 2-36](#).
- 

#### Related Topics

- [Step 2: Defining the Remote FastEthernet Policy Group QoS Properties, page 2-36](#)

## Step 2: Defining the Remote FastEthernet Policy Group QoS Properties

This step assumes that you have completed [Step 1: Defining the Remote FastEthernet Policy Group, page 2-34](#).

In this step you define the Class-based QoS property to the policy group.

#### Procedure

---

- Step 1** In the QoS Properties page, click **Edit**. The QoS Properties Wizard - Congestion Management page appears.



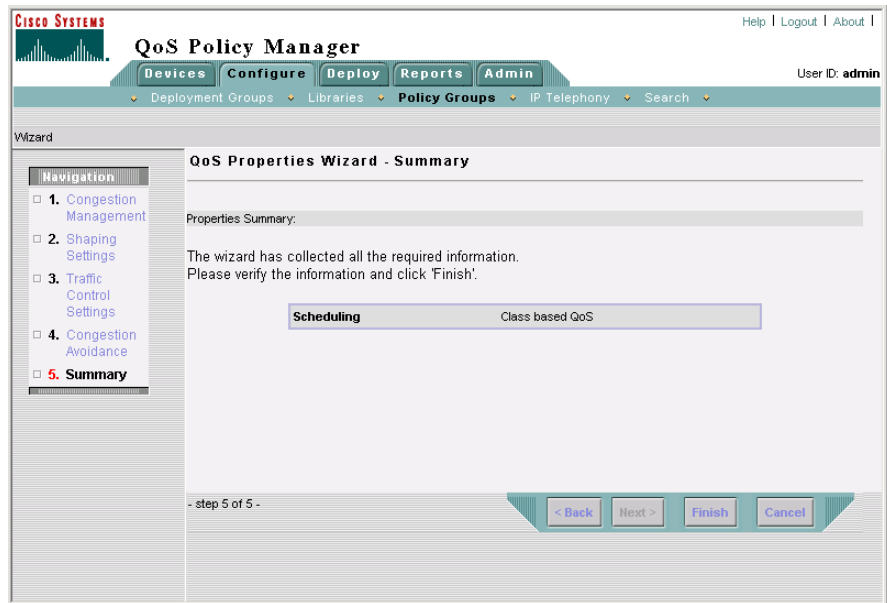
**Note** If the QoS Properties page is not open, select **Configure > Policy Groups**, then click the QoS Properties link for the Remote FastEthernet policy group.

---

- Step 2** Do the following in the QoS Properties Wizard - Congestion Management page:
- a. Select **Class Based QoS** from the Select a scheduling method list box.

- b. Click **Finish**. The QoS Properties Wizard - Summary page appears. [Figure 2-13](#) shows the QoS Properties Wizard - Summary page.

**Figure 2-13** Lesson 2-2-2—Remote FastEthernet Policy Group QoS Properties Wizard - Summary Page



- Step 3** In the QoS Properties Wizard - Summary page, click **Finish**. The QoS Properties page appears.
- Step 4** You have defined the QoS properties of the Remote FastEthernet policy group. Now you assign network elements to it. Continue with [Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy Group](#), page 2-14.

### Related Topics

- [Step 3: Assigning Elements to the Remote FastEthernet Policy Group](#), page 2-38

## Step 3: Assigning Elements to the Remote FastEthernet Policy Group

This step assumes that you have completed [Step 2: Defining the Remote FastEthernet Policy Group QoS Properties](#), page 2-36.

In this step you assign these network elements to the policy group:

- FastEthernet interface 0/0 on router Core-3600-1
- FastEthernet interface 0/0 on router Core-2600-1

### Procedure

---

**Step 1** Select **Assigned Network Elements** in the TOC. The Assigned Network Elements page appears.



**Note** If the Assigned Network Elements entry does not appear in the TOC, select **Configure > Policy Groups**, then click the Network Elements link for the Remote FastEthernet policy group.

---

**Step 2** In the Assigned Network Elements page, select **Add**. The Add Assignment dialog box opens.

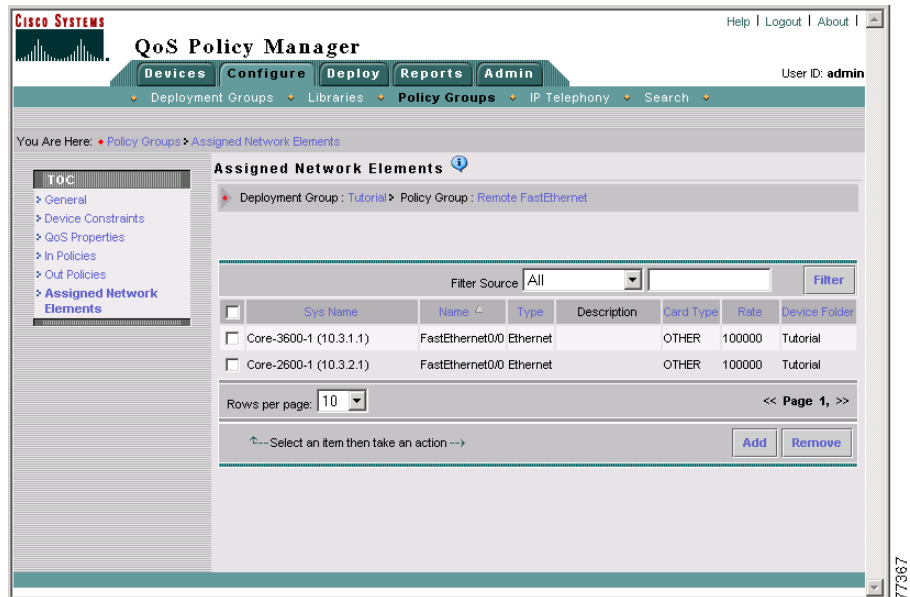
**Step 3** Do the following in the Add Assignment dialog box:

- a. Select the following network elements by selecting the check box next to them.
  - FastEthernet0/0 on device Core-2600-1
  - FastEthernet0/0 on device Core-3600-1
- b. Click **Assign**.

The dialog box closes. The selected network element appears in the Assigned Network Elements page. [Figure 2-14](#) shows the completed Assigned Network Elements page.



**Figure 2-14 Lesson 2-2-2—Remote FastEthernet Policy Group Assigned Network Elements Page**



- Step 4** You have completed assigning network elements to the Remote FastEthernet policy group. Now you create the Web Traffic Coloring policy. Continue with [Step 4: Creating the Web Traffic Coloring Policy, page 2-39](#).

#### Related Topics

- [Step 4: Creating the Web Traffic Coloring Policy, page 2-39](#)

## Step 4: Creating the Web Traffic Coloring Policy

This step assumes that you have completed [Step 3: Assigning Elements to the Remote FastEthernet Policy Group, page 2-38](#).

In this step you create the Web Traffic Coloring policy, which colors web traffic coming from the remote sites to DSCP 16.

## Procedure

---

**Step 1** Select **In Policies** in the TOC. The In Policies page appears.



**Note** If the In Policies entry does not appear in the TOC, select **Configure > Policy Groups**, then click the In Policies link for the Remote FastEthernet policy group.

---

**Step 2** In the In Policies page, click **Create**. The In Policy wizard opens, displaying the In Policy Wizard - General page.

**Step 3** Do the following in the In Policy Wizard - General page:

- a. Enter **Web Traffic Coloring** in the Policy Name field.
- b. Enter **Colors inbound web traffic** in the Enter Description for the Policy field.
- c. Leave the QoS Policy radio button selected.
- d. Click **Next**. The In Policy Wizard - Filter page appears.

**Step 4** Do the following in the In Policy Wizard - Filter page:

- a. Leave the Create a new filter radio button selected.
- b. Enter **Web traffic** in the Filter name field.
- c. Click **Create** to define a filter rule. The Rule Settings page appears.

**Step 5** In the Rule Settings page, click **Edit** in the Protocol table row. The Protocol Editor dialog box opens.

**Step 6** Do the following in the Protocol Editor dialog box:

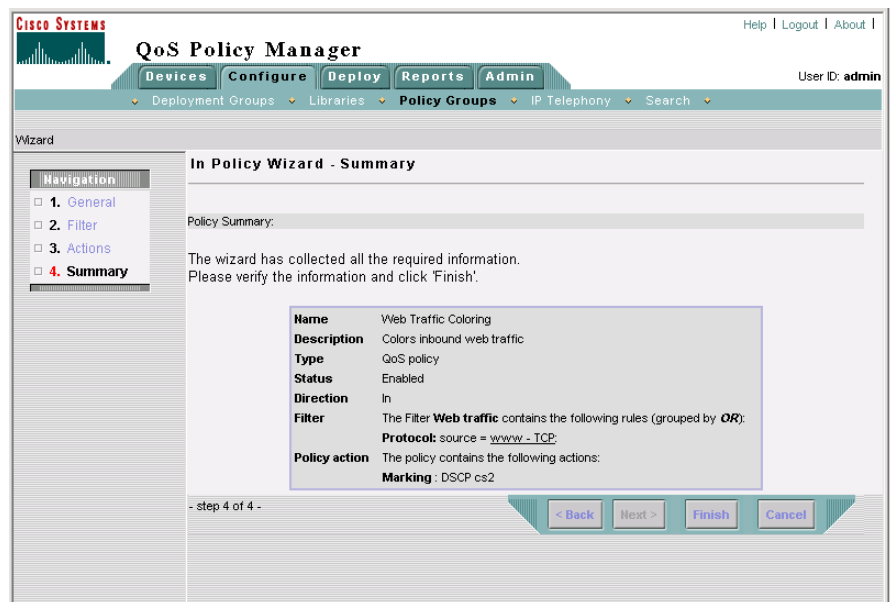
- a. Select the From Library radio button.
- b. Select **www-TCP** from the Source list box.
- c. Click **OK**. The Protocol Editor dialog box closes. The Rule Setting page updates in the main QPM window.

**Step 7** In the Rule Settings page, click **Done**. The In Policy Wizard - Filter page appears.

**Step 8** In the In Policy Wizard - Filter page, click **Next**. The In Policy Wizard - Marking page appears.

- Step 9** Do the following in the In Policy Wizard - Marking page:
- Select **16 (cs2)** from the Value list box.  
The Enable Marking check box is automatically selected.
  - Click **Finish**. The In Policy Wizard - Summary page appears, where you can view a summary of the policy. [Figure 2-15](#) shows the completed In Policy Wizard - Summary page.
  - Click **Finish**. The In Policies page appears.

**Figure 2-15 Lesson 2-2-2—Remote FastEthernet Policy Group In Policy Wizard - Summary Page**



- Step 10** You have completed creation of the Web Traffic Coloring policy. Continue with [Step 5: Creating the ERP Traffic Coloring Policy, page 2-42](#).

### Related Topics

- [Step 5: Creating the ERP Traffic Coloring Policy, page 2-42](#)

## Step 5: Creating the ERP Traffic Coloring Policy

This step assumes that you have completed [Step 4: Creating the Web Traffic Coloring Policy, page 2-39](#).

In this step you create the ERP Traffic Coloring policy, which colors ERP traffic coming from the remote sites to DSCP 32.

### Procedure

---

**Step 1** In the In Policies page, click **Create**. The In Policy wizard opens, displaying the In Policy Wizard - General page.



---

**Note** If the In Policies entry does not appear in the TOC, select **Configure > Policy Groups**, then click the In Policies link for the Remote FastEthernet policy group.

---

**Step 2** Do the following in the In Policy Wizard - General page:

- a. Enter **Color ERP traffic** in the Policy Name field.
- b. Enter **Colors inbound ERP traffic** in the Enter Description for the Policy field.
- c. Leave the QoS Policy check box selected.
- d. Click **Next**. The In Policy Wizard - Filter page appears.

**Step 3** Do the following in the In Policy Wizard - Filter page:

- a. The Create a new filter check box is automatically selected.
- b. Enter **ERP traffic** in the Filter name field.
- c. Click **Create** to define a filter condition. The Rule Settings page appears.

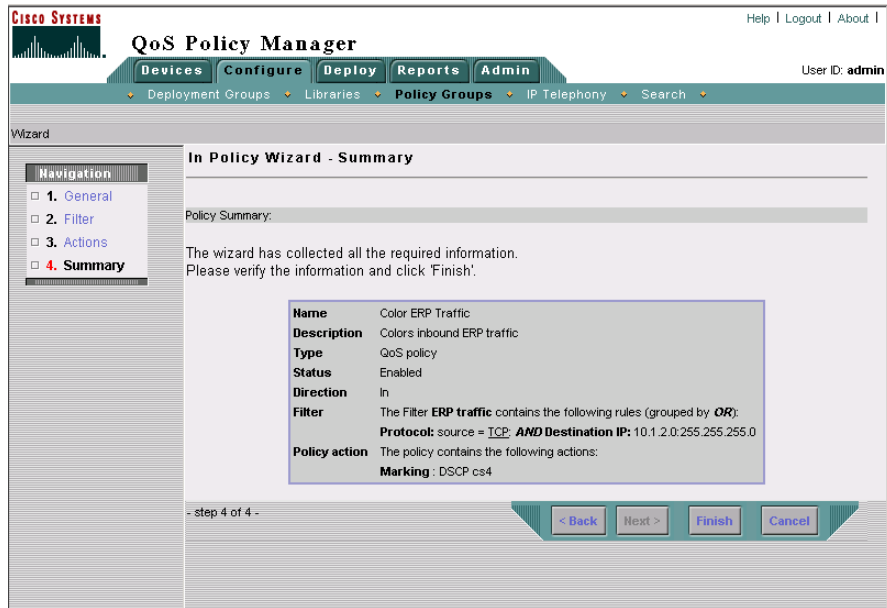
**Step 4** In the Rule Settings page, click **Edit** in the Protocol row of the Rule Setting table. The Protocol Editor dialog box opens.

**Step 5** Do the following in the Protocol Editor dialog box:

- a. Select the From Library radio button.
- b. Select **TCP** from the Source list box.



**Figure 2-16 Lesson 2-2-2—Remote FastEthernet Policy Group In Policy Wizard - Summary Page**



- Step 11** In the In Policy Wizard - Summary page, click **Finish**. The In Policies page appears.
- Step 12** Select **Configure > Policy Groups**. The Policy Groups page appears.

Now that you have completed creating the Remote FastEthernet policy group to color web and ERP traffic originating from the remote sites, you can proceed with the next lesson, [Lesson 2-4: Creating the WAN PPP Policy Group, page 2-45](#).

### Related Topics

- [Lesson 2-4: Creating the WAN PPP Policy Group, page 2-45](#)

## Lesson 2-4: Creating the WAN PPP Policy Group

The WAN PPP policy group queues web and ERP traffic that is exchanged between the web and application servers on the Campus and the remote Finance and Sales groups. It is applied to the egress interfaces of the core routers—Core-7200-1, Core-3600-1, and Core-2600-1.

These interfaces are the best network elements on which to apply queuing because they connect the Campus and remote LANs to the WAN. The bandwidth difference between the LAN and WAN creates a backlog of traffic at these interfaces, so a queuing policy will ensure that web and ERP traffic flows get the desired share of the available WAN bandwidth.

Only one queuing policy group is necessary because one policy group with the necessary properties and policies can be applied to all of the pertinent interfaces. This is unlike the situation with the coloring policy, in which two policy groups are necessary because coloring is applied at switch interfaces on the Campus LAN, but is applied at router interfaces on the remote LANs.

The details of the WAN PPP policy group are as follows.

- Device Constraints:
  - 7200 Series, 3600 Series, and 2600 Series serial interfaces
  - Cisco IOS 12.2
- Network Element Assignments:
  - Serial interfaces 4/0 and 4/1 on router Core-7200-1
  - Serial interface 1/0 on router Core-3600-1
  - Serial interface 1/0 on router Core-2600-1
- QoS Properties: MQC CBWFQ
- QoS Policies:
  - DSCP 32 (ERP traffic) 40%
  - DSCP 16 (web traffic) 20%
  - WFQ for default

The following topics describe how to create the WAN PPP policy group. Each step assumes that you have just completed the previous step:

- [Step 1: Defining the WAN PPP Policy Group, page 2-46](#)
- [Step 2: Defining the WAN PPP Policy Group QoS Properties, page 2-49](#)
- [Step 3: Assigning Elements to the WAN PPP Policy Group, page 2-50](#)
- [Step 4: Creating the MQC CBWFQ Queuing Policies, page 2-52](#)

## Step 1: Defining the WAN PPP Policy Group

In this step you define the basic properties of the policy group, including:

- Name
- Description
- Constraints:
  - 7200 Series, 3600 Series, and 2600 Series serial interfaces
  - Cisco IOS 12.2

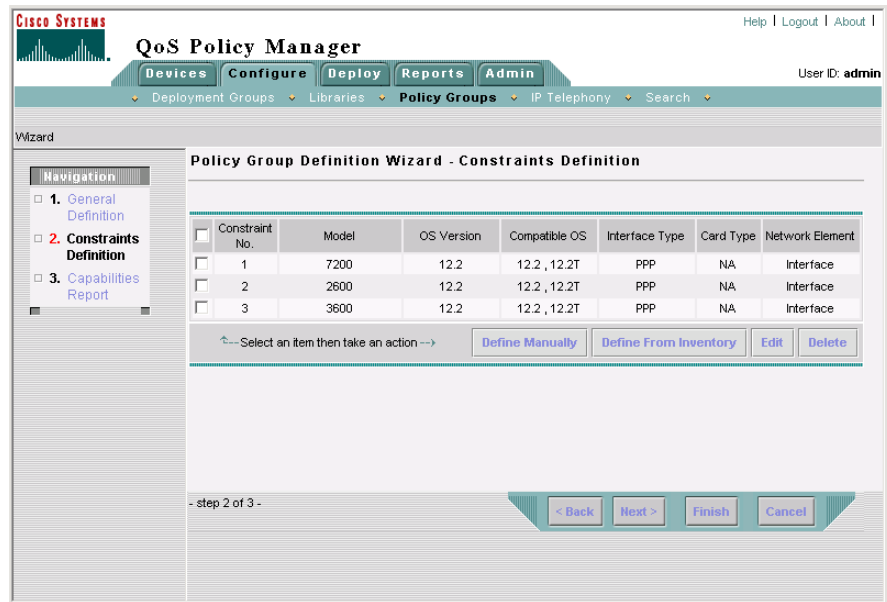
### Procedure

- 
- Step 1** Select **Configure > Policy Groups**. The Policy Groups page appears.
  - Step 2** Select **Tutorial** from the Deployment Group list box. The page refreshes to display the policy groups in the Tutorial deployment group.
  - Step 3** Click **Create**. The Policy Group Definition wizard starts.
  - Step 4** Do the following in the Policy Group Definition Wizard - General Definition page:
    - Enter **WAN PPP** in the Policy Group Name field.
    - Enter **Applies MQC CBWFQ to ERP and web traffic entering the WAN** in the Policy Group Description field.
    - Do not modify the other page fields.
    - Click **Next**. The Policy Group Definition Wizard - Constraints Definition page appears.



- Step 5** In the Policy Group Definition Wizard - Constraints Definition page, click **Define Manually**. The Manual Constraint Definition page appears.
- Step 6** Do the following in the Manual Constraint Definition page:
- Select **2600** from the Model list.
  - Select **12.2** from the OS Version list.
  - Select **Interface** from the Network Element Type list.
  - Select **PPP** from the Interface Type list.
  - Click **OK**. The Policy Group Definition Wizard - Constraints Definition page appears.
- Step 7** In the Policy Group Definition Wizard - Constraints Definition page, click **Define Manually**. The Manual Constraint Definition page appears.
- Step 8** Do the following in the Manual Constraint Definition page:
- Select **3600** from the Model list.
  - Select **12.2** from the OS Version list.
  - Interface** is automatically entered in the Network Element Type field.
  - Select **PPP** from the Interface Type list.
  - Click **OK**. The Policy Group Definition Wizard - Constraints Definition page appears.
- Step 9** In the Policy Group Definition Wizard - Constraints Definition page, click **Define Manually**. The Manual Constraint Definition page appears.
- Step 10** Do the following in the Manual Constraint Definition page:
- Select **7200** from the Model list.
  - Select **12.2** from the OS Version list.
  - Interface** is automatically entered in the from the Network Element Type field.
  - Select **PPP** from the Interface Type list.
  - Click **OK**. The Policy Group Definition Wizard - Constraints Definition page appears. [Figure 2-17](#) shows the completed Policy Group Definition Wizard - Constraints Definition page.

**Figure 2-17 Lesson 2-4—WAN PPP Policy Group Definition Wizard - Constraints Definition Page**



- Step 11** In the Policy Group Definition Wizard - Constraints Definition page, click **Next**. The Policy Group Definition Wizard - Capabilities Report page appears, where you can view a summary of the QoS features that can be configured for the policy group, according to the device constraints.
- Step 12** In the Policy Group Definition Wizard - Capabilities Report page, click **Finish**. The QoS Properties page appears.
- Step 13** You have completed creation of the WAN PPP policy group. Now you define its QoS properties. Continue with [Step 2: Defining the WAN PPP Policy Group QoS Properties, page 2-49](#).

### Related Topics

- [Step 2: Defining the WAN PPP Policy Group QoS Properties, page 2-49](#)

## Step 2: Defining the WAN PPP Policy Group QoS Properties

This step assumes that you have completed [Step 1: Defining the WAN PPP Policy Group](#), page 2-46.

In this step you assign the modular QoS CLI (MQC) class-based weighted fair queuing (CBWFQ) QoS property to the policy group.

### Procedure

---

**Step 1** In the QoS Properties page, click **Edit**. The QoS Properties Wizard - Congestion Management page appears.



---

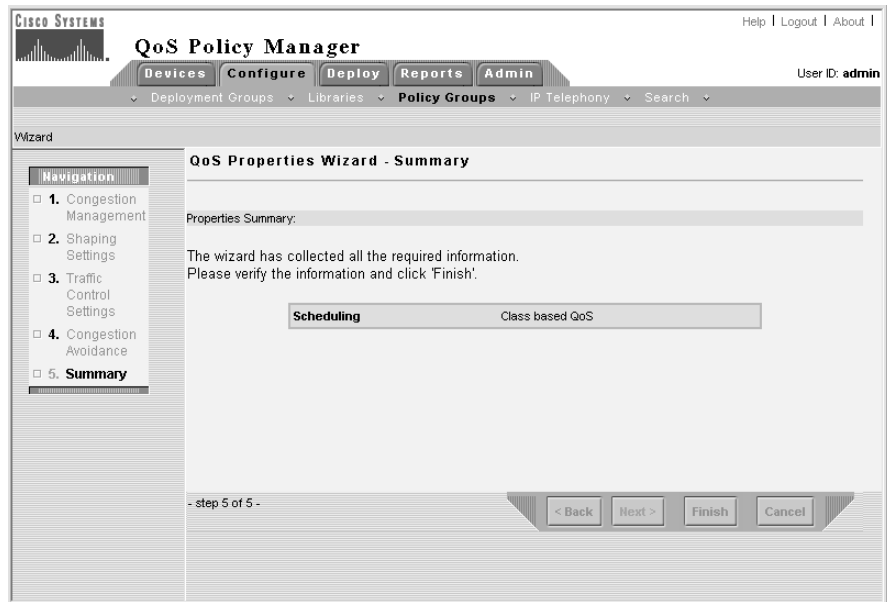
**Note** If the QoS Properties page is not open, select **Configure > Policy Groups**, then click the QoS Properties link for the WAN PPP policy group.

---

**Step 2** Do the following in the QoS Properties Wizard - Congestion Management page:

- Select **Class Based QoS** from the Select a scheduling method list box.
- Click **Finish**. The QoS Properties Wizard - Summary page appears. [Figure 2-18](#) shows the QoS Properties Wizard - Summary page.

**Figure 2-18 Lesson 2-4—WAN PPP Policy Group QoS Properties Wizard - Summary Page**



- Step 3** In the QoS Properties Wizard - Summary page, click **Finish**. The QoS Properties page appears.
- Step 4** You have completed defining QoS properties for the WAN PPP policy group. Now you assign network elements to it. Continue with [Step 3: Assigning Elements to the WAN PPP Policy Group, page 2-50](#).

#### Related Topics

- [Step 3: Assigning Elements to the WAN PPP Policy Group, page 2-50](#)

## Step 3: Assigning Elements to the WAN PPP Policy Group

This step assumes that you have completed [Step 2: Defining the WAN PPP Policy Group QoS Properties, page 2-49](#).

In this step you assign these network elements to the policy group:

- Serial interfaces 4/0 and 4/1 on router Core-7200-1.
- Serial interface 1/0 on router Core-3600-1.
- Serial interface 1/0 on router Core-2600-1.

### Procedure

---

**Step 1** Select **Assigned Network Elements** in the TOC. The Assigned Network Elements page appears.



**Note** If the Assigned Network Elements entry does not appear in the TOC, select **Configure > Policy Groups**, then click the Network Elements link for the WAN PPP policy group.

---

**Step 2** In the Assigned Network Elements page, select **Add**. The Assignment dialog box opens.

**Step 3** Do the following in the Assignment dialog box:

- a. Select the following network elements by selecting the check box next to them.
  - Serial4/0 on device Core-7200-1.
  - Serial4/1 on device Core-7200-1.
  - Serial1/0 on device Core-3600-1.
  - Serial1/0 on device Core-2600-1.
- b. Click **Assign**.

The dialog box closes. The selected network element appears in the Assigned Network Elements page. [Figure 2-19](#) shows the completed Assigned Network Elements page.

**Figure 2-19 Lesson 2-4—WAN PPP Policy Group Assigned Network Elements Page**

The screenshot shows the Cisco QoS Policy Manager interface. The main content area is titled "Assigned Network Elements" and shows a table of network elements assigned to the WAN PPP policy group. The table has the following data:

Sys Name	Name	Type	Description	Card Type	Rate	Device Folder
Core-3600-1 (10.3.1.1)	Serial1/0	PPP		OTHER	1544	Tutorial
Core-2600-1 (10.3.2.1)	Serial1/0	PPP		OTHER	512	Tutorial
Core-7200-1 (10.1.1.1)	Serial4/0	PPP		OTHER	1544	Tutorial
Core-7200-1 (10.1.1.1)	Serial4/1	PPP		OTHER	512	Tutorial

The interface also includes a "Filter Source" dropdown set to "All", a "Filter" button, and a "Rows per page" dropdown set to "10". The page number is "Page 1".

- Step 4** You have completed assigning network elements to the WAN PPP policy group. Now you create the MQC CBWFQ queuing policies. Continue with [Step 4: Creating the MQC CBWFQ Queuing Policies, page 2-52](#).

### Related Topics

- [Step 4: Creating the MQC CBWFQ Queuing Policies, page 2-52](#)

## Step 4: Creating the MQC CBWFQ Queuing Policies

In this step you create the three policies that are needed to apply MQC CBWFQ queuing to web and ERP traffic entering the WAN, and implement a class default policy for all traffic that does not match any of the traffic classes:

- The ERP Queuing policy allocates 40% of bandwidth to DSCP 32 (ERP traffic).

- The Web Queuing policy allocates 20% of bandwidth to DSCP 16 (web traffic).
- The Default Queuing policy assigns WFQ as the queuing mechanism for the default traffic class (all traffic that does not match the other classes).

The following sections describe how to create these policies:

- [Step 4a: Creating the ERP Traffic Queuing Policy, page 2-53](#)
- [Step 4b: Creating the Web Traffic Queuing Policy, page 2-56](#)
- [Step 4c: Creating the Class Default Policy, page 2-59](#)

## Step 4a: Creating the ERP Traffic Queuing Policy

This step assumes that you have completed [Step 3: Assigning Elements to the WAN PPP Policy Group, page 2-50](#).

In this step you create the ERP Traffic Queuing policy, which queues ERP traffic entering the WAN using MCQ CBWFQ. It works in conjunction with the DSCP marking that is done by other policies to allocate 40% of the link bandwidth to DSCP 32 (ERP) traffic.

### Procedure

---

**Step 1** Select **Out Policies** in the TOC. The Out Policies page appears.



**Note** If the Out Policies entry does not appear in the TOC, select **Configure > Policy Groups**, then click the Out Policies link for the WAN PPP policy group.

---

**Step 2** In the Out Policies page, click **Create**. The Out Policy wizard opens, displaying the Out Policy Wizard - General page.

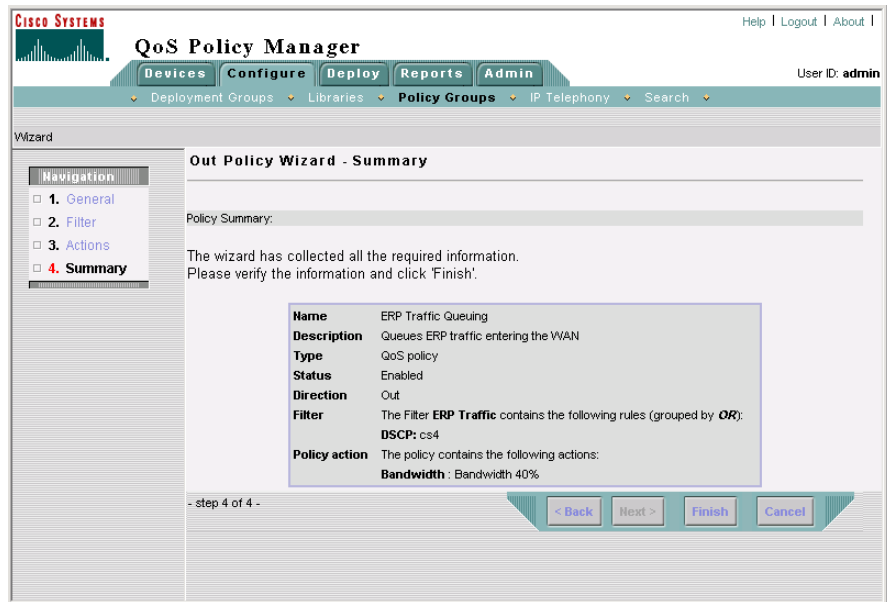
**Step 3** Do the following in the Out Policy Wizard - General page:

- a. Enter **ERP Traffic Queuing** in the Policy Name field.
- b. Enter **Queues ERP traffic entering the WAN** in the Enter Description for the Policy field.

- c. Leave the QoS Policy radio button selected.
  - d. Click **Next**. The Out Policy Wizard - Filter page appears.
- Step 4** Do the following in the Out Policy Wizard - Filter page:
  - a. Leave the Create a new filter radio button selected.
  - b. Enter **ERP Traffic** in the Filter Name field.
  - c. Click **Create**. The Rule Setting page appears.
- Step 5** In the Rule Setting page, click **Edit** in the Service table row. The Service Editor dialog box opens.
- Step 6** Do the following in the Service Editor dialog box:
  - a. Select **32 (cs4)** from the Value list box.
  - b. Click **OK**. The Service Editor dialog box closes, and the Rule Settings page refreshes.
- Step 7** In the Rule Settings page, click **Done**. The Out Policy Wizard - Filter page appears.
- Step 8** In the Out Policy Wizard - Filter page, click **Next**. The Out Policy Wizard - Marking page appears.
- Step 9** Click **Queuing** in the Navigation list (under step 3, Actions). The Out Policy Wizard - Queuing page appears.
- Step 10** Do the following in the Out Policy Wizard - Queuing page:
  - a. Enter **40** in the bandwidth field.  
The Enable Bandwidth Allocation (CBQ) check box is automatically selected.
  - b. Leave the Ratio radio button selected.
  - c. Click **Finish**. The Out Policy Wizard - Summary page appears, where you can view a summary of the policy. [Figure 2-20](#) shows the completed Out Policy Wizard - Summary page.



**Figure 2-20 Lesson 2-4—WAN PPP Policy Group Out Policy Wizard - Summary Page**



- Step 11** In the Out Policy Wizard - Summary page, click **Finish**. The Out Policies page appears.
- Step 12** You have completed creating the ERP Traffic Queuing policy. Now you create the Web Traffic Queuing policy. Continue with [Step 4b: Creating the Web Traffic Queuing Policy, page 2-56](#).

### Related Topics

- [Step 4b: Creating the Web Traffic Queuing Policy, page 2-56](#)

## Step 4b: Creating the Web Traffic Queuing Policy

This step assumes that you have completed [Step 4a: Creating the ERP Traffic Queuing Policy, page 2-53](#).

In this step you create the Web Traffic Queuing policy, which queues web traffic entering the WAN using MCQ CBWFQ. It works in conjunction with the DSCP marking that is done by other policies to allocate 20% of the link bandwidth to DSCP 16 (web) traffic.

### Procedure

**Step 1** In the Out Policies page, click **Create**. The Out Policy wizard opens, displaying the Out Policy Wizard - General page.

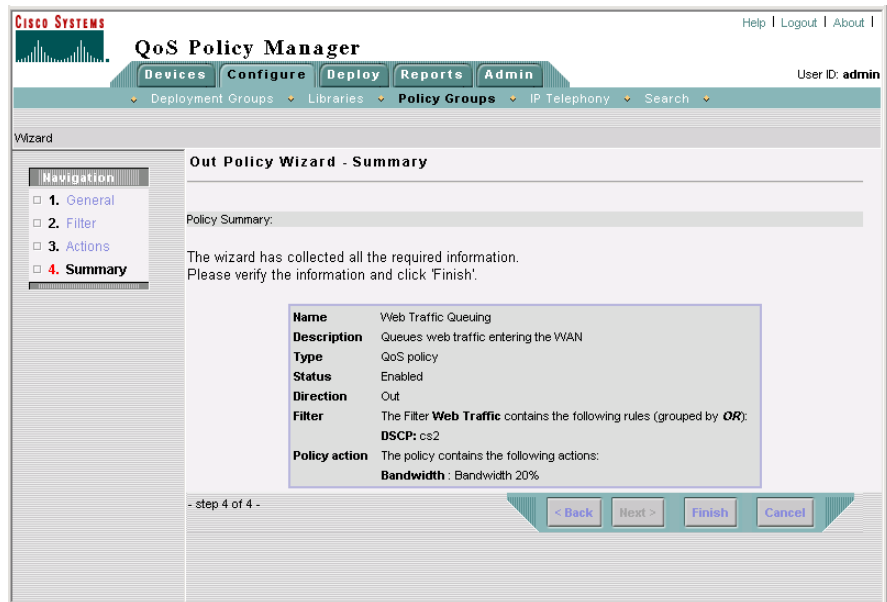


**Note** If the Out Policies page is not open and the Out Policies entry does not appear in the TOC, select **Configure > Policy Groups**, then click the Out Policies link for the WAN PPP policy group.

- Step 2** Do the following in the Out Policy Wizard - General page:
- Enter **Web Traffic Queuing** in the Policy Name field.
  - Enter **Queues web traffic entering the WAN** in the Enter Description for the Policy field.
  - Leave the QoS Policy radio button selected.
  - Click **Next**. The Out Policy Wizard - Filter page appears.
- Step 3** Do the following in the Out Policy Wizard - Filter page:
- Leave the Create a new filter radio button selected.
  - Enter **Web Traffic** in the Filter Name field.
  - Click **Create**. The Rule Setting page appears.
- Step 4** In the Rule Setting page, click **Edit** in the Service table row. The Service Editor dialog box opens.
- Step 5** Do the following in the Service Editor dialog box:
- Select **16 (cs2)** from the Value list box.



**Figure 2-21 Lesson 2-4—WAN PPP Policy Group Out Policy Wizard - Summary Page**



- Step 10** In the Out Policy Wizard - Summary page, click **Finish**. The Out Policies page appears.
- Step 11** You have completed creating the Web Traffic Queuing policy. Now you create the Class Default policy. Continue with [Step 4c: Creating the Class Default Policy, page 2-59](#).

### Related Topics

- [Step 4c: Creating the Class Default Policy, page 2-59](#)

## Step 4c: Creating the Class Default Policy

This step assumes that you have completed [Step 4b: Creating the Web Traffic Queuing Policy](#), page 2-56.

In this step you create the class default policy, which assigns weighted fair queuing (WFQ) as the queuing method for all traffic that does not match the filters of the other policies.

### Procedure

---

**Step 1** In the Out Policies page, click **Create**. The Out Policy wizard opens, displaying the Out Policy Wizard - General page.



**Note** If the Out Policies page is not open and the Out Policies entry does not appear in the TOC, select **Configure > Policy Groups**, then click the Out Policies link for the WAN PPP policy group.

---

**Step 2** Do the following in the Out Policy Wizard - General page:

- a. Enter **WAN PPP Default** in the Policy Name field.
- b. Enter **Queues default traffic using WFQ** in the Enter Description for the Policy field.
- c. Leave the QoS Policy radio button selected.
- d. Click **Next**. The Out Policy Wizard - Filter page appears.

**Step 3** Do the following in the Out Policy Wizard - Filter page:

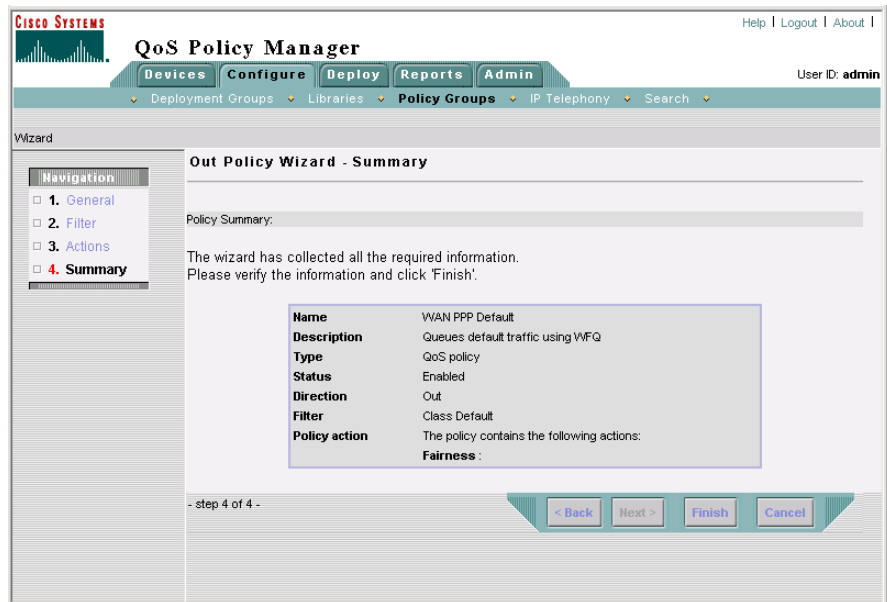
- a. Click the Class Default radio button.
- b. Click **Next**. The Out Policy Wizard - Marking page appears.

**Step 4** Click **Queuing** in the Navigation list (under step 3, Actions). The Out Policy Wizard - Queuing page appears.

**Step 5** Do the following in the Out Policy Wizard - Actions page:

- a. Select the Enable WFQ check box.
- b. Click **Finish**. The Out Policy Wizard - Summary page appears, where you can view a summary of the policy. [Figure 2-22](#) shows the completed Out Policy Wizard - Summary page.

**Figure 2-22 Lesson 2-4—WAN PPP Policy Group Out Policy Wizard - Summary Page**



**Step 6** In the Out Policy Wizard - Summary page, click **Finish**. The Out Policies page appears.

Now that you have completed creating the WAN PPP policy group to queue web and ERP traffic that is exchanged between the web and application servers on the Campus and the remote Finance and Sales groups, you can proceed with the next lesson, [Lesson 2-5: Adding FTP Policing To the Campus Access VLAN Policy Group](#), page 2-61.

#### Related Topics

- [Lesson 2-5: Adding FTP Policing To the Campus Access VLAN Policy Group](#), page 2-61

# Lesson 2-5: Adding FTP Policing To the Campus Access VLAN Policy Group

This lesson demonstrates how you can add additional functionality to an existing policy group. In this case, you will add a policing policy to police FTP traffic, limiting FTP bandwidth usage to 128 Kbps, to the Campus Access VLAN policy group.

This lesson assumes that you have completed [Lesson 2-2: Defining Policy Groups and Policies To Color Campus Web Traffic, page 2-19](#).

## Procedure

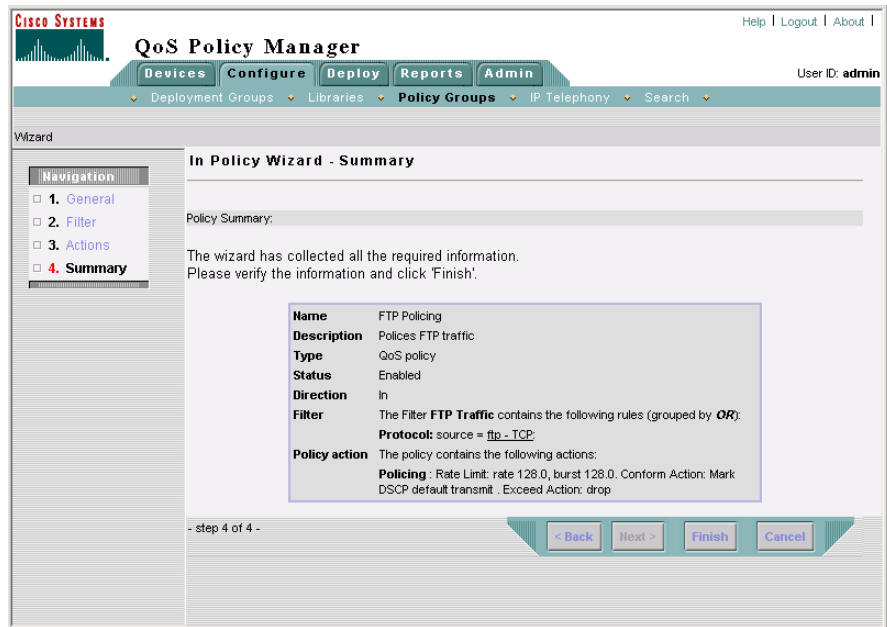
---

- Step 1** Select **Configure > Policy Groups**. The policy groups page appears.
- Step 2** Select **Tutorial** from the Deployment Group list box.
- Step 3** Click the number in the In Policies column of the of the Campus Access VLAN policy group table entry. The In Policies page appears.
- Step 4** In the In Policies page, click **Create**. The In Policy Wizard - General page appears.
- Step 5** Do the following in the In Policy Wizard - General page:
  - a. Enter **FTP Policing** in the Policy Name field.
  - b. Enter **Polices FTP traffic** in the Enter Description for the Policy field.
  - c. Click **Next**. The In Policy Wizard - Filter page appears.
- Step 6** Do the following in the In Policy Wizard - Filter page:
  - a. The New Filter check box is automatically selected.
  - b. Enter **FTP Traffic** in the Filter name field.
  - c. Click **Create**. The Rule Setting page appears.
- Step 7** In the Rule Setting page, click **Edit** in the Protocol table row. The Protocol Editor dialog box opens.
- Step 8** Do the following in the Protocol Editor dialog box:
  - a. Leave the From Library radio button selected.
  - b. Select **ftp-TCP** from the Source list box.





**Figure 2-23 Lesson 2-5—Campus Access VLAN Policy Group In Policy Wizard - Summary Page**



**Step 13** In the In Policy Wizard - Summary page, click **Finish**. The In Policies page appears.

**Step 14** Select **Configure > Policy Groups**. The Policy Groups page appears.

Now that you have added FTP policing to the Campus Access VLAN policy group, you can proceed with the next lesson, [Lesson 2-6: Deploying the Data Network Tutorial Policies, page 2-64](#).

### Related Topics

- [Lesson 2-6: Deploying the Data Network Tutorial Policies, page 2-64](#)

# Lesson 2-6: Deploying the Data Network Tutorial Policies

This lesson describes how to deploy the QoS policies that were saved in your deployment group to the devices in the network, where they will be implemented.

**Note**

---

Although you can follow all the steps in this lesson, the actual deployment of the “Tutorial” deployment group will fail, since you cannot deploy to virtual devices in the network. However, if you are using real devices in your data network, you should be able to deploy your QoS policies to your devices successfully.

---

To distribute your QoS policies to your physical network devices, QPM translates your policies into device commands and enters the commands through the device’s command line interface (CLI). You can choose whether or not to deploy your QoS configurations directly to the network devices through Telnet. QPM automatically deploys your QoS configurations to configuration files. This procedure does not configure your devices but generates configuration files that can be sent manually to the devices. QoS configurations can be deployed to the device through any application that downloads configuration files to the devices.

**Before You Begin**

To do this lesson you should have completed lessons 2-1 through 2-5.

**Procedure**

- 
- Step 1** Select **Deploy > Deployment**. The first step of the Deployment wizard is displayed—Deployment Group Selection.
  - Step 2** Select the Current version of a deployment group radio button, and select Tutorial from the list box (if it isn’t already selected).
  - Step 3** Click **Next** to move to the next step of the wizard—the Device Selection and Preview page.

This page displays a list of all the devices that are available for deployment. In this step of the wizard, you select the devices you want to deploy to. You can also preview your device configurations prior to deployment.

- Step 4** If you are using virtual devices, select the check boxes next to the virtual devices in your data network example. If you are using real devices, select the check boxes next to the devices to which you want to deploy your policies. Deselect those you do not want to deploy to.
- Step 5** If you want to preview the CLI configuration commands for a device, click its configuration link in the table. A preview window opens, letting you view the Backup ShowRun configuration commands and any incremental Telnet script commands that will be written to the device.
- Step 6** When you have finished previewing the device's configuration, click **Close** to close the Preview window.
- Step 7** Click **Next** to move to the next step of the wizard—the Job Details page.
- Step 8** Enter **Data\_Tutorial** in the Job Name field.
- Step 9** If required, you can enter a description for the job in the Job Description field.
- Step 10** Make sure the Deploy configuration to the devices using Telnet check box is selected. (The configuration will also be saved to files.)
- Step 11** Click **Next** to move to the final step of the wizard. This page presents a summary of the data collected through the wizard for you to verify.
- Step 12** After you have verified the job information, click **Deploy** to deploy the deployment group to the network.

The Active Jobs page opens, enabling you to monitor the deployment process, as described in the next lesson, [Lesson 2-7: Monitoring the Deployment Process, page 2-66](#).

---

### Related Topics

- [Understanding the Data Network Tutorial Example Network, page 2-2](#)
- [Lesson 2-7: Monitoring the Deployment Process, page 2-66](#)

# Lesson 2-7: Monitoring the Deployment Process

QPM allows you to monitor the deployment process, by viewing the activity and status of your deployment job, in real-time. The Active Jobs page provides a dynamic view of all the currently active deployments and their status. For each job, the start time of configuration for each job, the job's status, and a summary of the number of devices deployed according to their status, is displayed.

The status of a job deployment or a device deployment may be Pending, In Progress, Completed, or Failed. A job deployment may also have the status of Aborted or Paused. For your deployment job to be "Completed", all the devices must be successfully configured. If the deployment of one device fails, the entire deployment fails.

## Before You Begin

To do this lesson you should have completed Lessons 2-1 through 2-6.

## Procedure

---

### Step 1 Select **Deploy > Jobs > Active Jobs**.

The Active Jobs page appears, displaying your current deployment job and its status.



#### Tip

The display is automatically refreshed every ten seconds. You can refresh manually by clicking the Refresh button.

---

### Step 2 View the status of your deployment job.

During the deployment process, a status of "In Progress" will be displayed for your job. The status will change to Failed, since the devices in your network are virtual and you cannot deploy to virtual devices in a network.



#### Note

If you are using real devices in your network, the status should change to "Completed", indicating that your deployment job was completed successfully.

---

### Related Topics

- [Understanding the Data Network Tutorial Example Network, page 2-2](#)
- [Lesson 2-6: Deploying the Data Network Tutorial Policies, page 2-64](#)





## IP Telephony Network Tutorial

---

Real-time voice over IP (VoIP) traffic in a network is directly affected by packet loss, packet delay, and delay variation. In an enterprise environment, network congestion can occur at any time in any portion of the network campus, branch office, or WAN. For successful deployment of IP telephony, you must ensure end-to-end network quality for voice traffic.

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

In this chapter, you will learn how to use the IP Telephony wizard to deploy QoS for VoIP over the Campus, WAN, and Branch Office segments of a network, using an example network scenario. The tutorial describes the process of configuring QoS for VoIP traffic, from selecting the devices that are in the network example, through deployment to the network and monitoring the activity and status of a deployment job.

The IP Telephony wizard creates voice policy groups that contain the QoS properties and policies required at each relevant point in your IP telephony network. The wizard determines the QoS features that can be configured in a voice policy group according to voice policy group templates which are based on the IP Telephony QoS guide. Each voice policy group contains a “voice role” attribute, which specifies the role of the interface on the network, such as, IP phone, Switch to WAN Router.

### Before You Begin

For the purpose of this tutorial, a file has been created containing the IP addresses and configuration details of the virtual devices that are in the IP telephony network configuration example. By using these virtual devices, you can follow the lessons without affecting your network. You must import the devices before you begin working on this tutorial. See [Lesson 1-2: Importing the Tutorial Virtual Devices, page 1-7](#).



---

**Note**

If you want to create policies and deploy them using actual devices that exist in your network, you must obtain the IP addresses of the appropriate devices.

---

The IP telephony network tutorial assumes that all the virtual devices in the IP telephony example network shown in [Figure 3-1](#) have already been imported into your device inventory. [Table 3-1 on page 3-6](#) provides the network device information for these devices in the IP telephony network example.

This chapter includes the following sections:

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard, page 3-8](#)
- [Lesson 3-2: Modifying the Voice Policies, page 3-32](#)
- [Lesson 3-3: Deploying the IP Telephony QoS Policies, page 3-45](#)
- [Lesson 3-4: Monitoring the Deployment Process, page 3-47](#)

### Related Topics

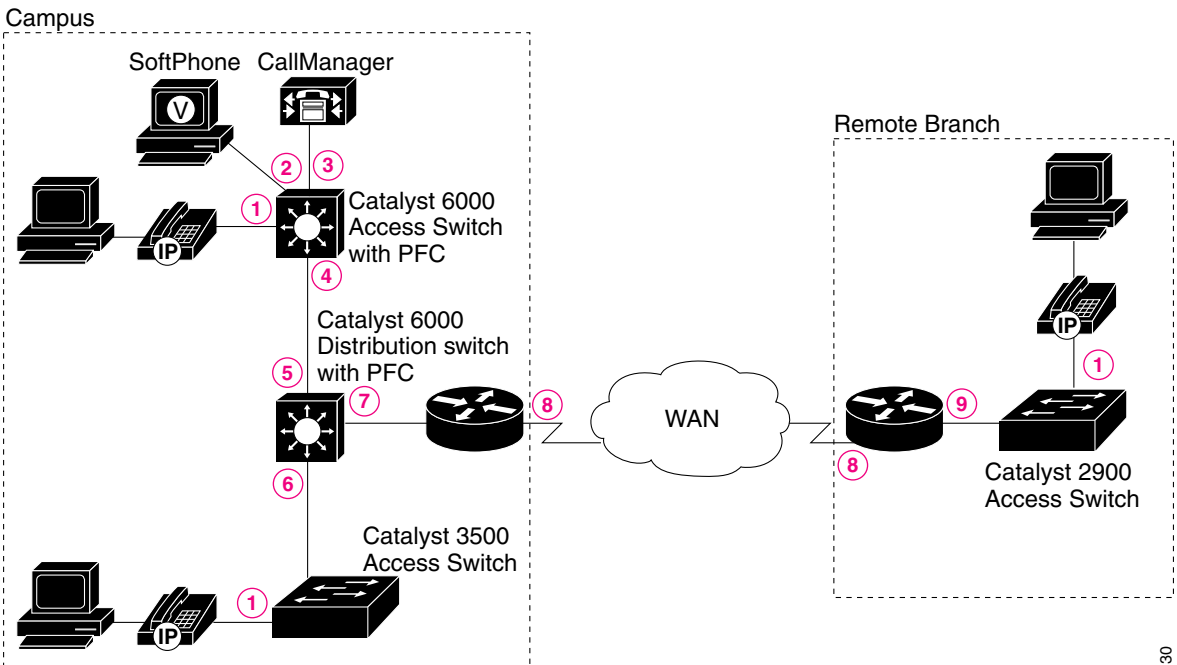
- [Lesson 1-2: Importing the Tutorial Virtual Devices, page 1-7](#).



# Understanding the IP Telephony Network Example

Figure 3-1 shows a typical network example for configuring QoS policies for IP telephony in an enterprise environment.

Figure 3-1 Configuring QoS for IP Telephony Network Example



63130

Based on this network configuration example, the following topics describe:

- [Configuring QoS for the Campus Site, page 3-4](#)
- [Configuring QoS for the WAN, page 3-5](#)
- [Configuring QoS for the Remote Branch, page 3-5](#)
- [Network Example Device Information, page 3-6](#)

## Configuring QoS for the Campus Site

The campus site includes a Cisco CallManager, an IP phone, and a SoftPhone that are connected to a QoS-aware Layer 3 access switch (with PFC). An additional IP phone is connected to a Layer 2 access switch (without PFC). The IP phone ports are configured to use an auxiliary voice VLAN on the switches. Both the access switches are connected to a Catalyst 6000 PFC Layer 3 distribution switch, running IOS version 12.1. Voice data from the campus site enters the WAN from a Cisco 7200 router running IOS version 12.2.

In the campus site, you must configure QoS for IP telephony at the following network points, shown in [Figure 3-1](#):

- The IP phone connections to the access switches ports (network points **1**).
- The SoftPhone connection to the access switch port (network point **2**).
- The CallManager connection to the access switch port (network point **3**).
- The uplink port on the Layer 3 access switch connection to the Layer 3 distribution switch port (network point **4**).
- The downlink ports on the Layer 3 distribution switch connections to the Layer 3 and Layer 2 access switches ports (network points **5** and **6**).
- The LAN connection from the Layer 3 distribution switch to the WAN router (network point **7**).

### Related Topics

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Step 3: Selecting the IP Phone Connections, page 3-15](#)
- [Step 4: Selecting the SoftPhone Connection, page 3-17](#)
- [Step 5: Selecting the CallManager Port, page 3-19](#)
- [Step 6: Selecting the IntraLAN Connections, page 3-21](#)
- [Step 7: Selecting the Voice VLAN Connections, page 3-23](#)

## Configuring QoS for the WAN

Because link speed in the WAN is much slower than in the LAN, QoS configuration for WAN links is needed to prevent delay. In the WAN segment of a network, the interface connections could support Serial Point-To-Point configuration or Frame Relay configuration. In this tutorial, the interface connections in the WAN segment of your network support Frame Relay configuration.

In a Frame Relay WAN configuration, you must configure the following QoS features for IP telephony on the devices interfaces (network points 8 in [Figure 3-1](#)):

- Frame Relay Fragmentation (FRF)
- Low Latency Queue (LLQ)
- IP RTP Header Compression (cRTP)
- Frame Relay Traffic Shaping (FRTS)

### Related Topics

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Step 8: Selecting the Switch to WAN Router Connection, page 3-25](#)
- [Step 9: Selecting the Router WAN to Switch Connection, page 3-27](#)
- [Step 10: Selecting the WAN Frame Relay Connections, page 3-29](#)

## Configuring QoS for the Remote Branch

The remote site includes an IP phone that is connected by means of a Layer 2 QoS-aware access switch to a Cisco 3600 router in the WAN. You must configure QoS on the IP phone port (network point 1) and on the branch office router interface to the access switch (network point 9 in [Figure 3-1](#)).

### Related Topics

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Step 3: Selecting the IP Phone Connections, page 3-15](#)
- [Step 9: Selecting the Router WAN to Switch Connection, page 3-27](#)

## Network Example Device Information

Table 3-1 shows the technical details of the devices in the IP telephony network example in Figure 3-1. These configuration details have already been imported into your device inventory so that you can follow these lessons. Interfaces that do not have QoS applied to them in the tutorial are not listed.

**Table 3-1 Sample Network Device Information for IP Telephony Network Tutorial**

Device Name	Device Model and IP Address	Software Version	Interfaces	IP Address	Mask
Core-7200-1	7200 10.9.1.1	12.2	FastEthernet0/0 FastEthernet 100,000 Kbit/sec (100 Mb/sec)	10.9.1.1	255.255.255.0
			Serial5/0 Frame Relay line at 512 Kbit/second Serial 5/0.1 DLCI 40	10.9.2.1	255.255.255.0
Core-3600-2	3600 10.8.1.1	12.2T	FastEthernet0/1 FastEthernet 100,000 Kbit/sec (100 Mb/sec)	10.8.1.1	255.255.255.0
			Serial2/0 Frame Relay line at 512 Kbit/second Serial 2/0.1 DLCI 40	10.8.2.2	255.255.255.0

**Table 3-1 Sample Network Device Information for IP Telephony Network Tutorial (continued)**

<b>Device Name</b>	<b>Device Model and IP Address</b>	<b>Software Version</b>	<b>Interfaces</b>	<b>IP Address</b>	<b>Mask</b>
Access-Cat6 000-3	6509 10.6.1.2	6.3	VLAN5	10.6.1.2	255.255.255.0
			propVirtual		
			Ethernet2/0 Standard Ethernet (10/100 Mbit/sec)		
			Ethernet2/1 Standard Ethernet (10/100 Mbit/sec)		
			Ethernet2/2 Standard Ethernet (10/100 Mbit/sec)		
Access-Cat6 000-4	6509 10.7.2.2	12.1E	GigabitEthernet1/1 gigabitEthernet	10.7.2.2	255.255.255.0
			GigabitEthernet1/2 gigabitEthernet		
			FastEthernet2/1 FastEthernet 100,000 Kbit/sec (100 Mb/sec)		
Access-Cat3 500-2	3524-PWR -XL 10.4.1.2	12.0	Ethernet2/3 Standard Ethernet (10/100 Mbit/sec)	10.4.1.2	255.255.255.0
			GigabitEthernet0/1 gigabitEthernet		

**Table 3-1** Sample Network Device Information for IP Telephony Network Tutorial (continued)

Device Name	Device Model and IP Address	Software Version	Interfaces	IP Address	Mask
Access-Cat2 900-2	2900-XL 10.4.2.2	12.0	FastEthernet0/1	10.4.2.2	255.255.255.0
			FastEthernet 100,000 Kbit/sec (100 Mb/sec)		
			Ethernet3/1  Standard Ethernet (10/100 Mbit/sec)		

**Related Topics**

- [Understanding the IP Telephony Network Example, page 3-3](#)

## Lesson 3-1: Assigning Voice Policies Using 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 point (interface) where QoS is a concern. 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.

The steps of the wizard that you must follow for this lesson include:

- [Step 1: Introduction, page 3-11](#)
- [Step 2: Selecting Devices for QoS Configuration, page 3-12](#)
- [Step 3: Selecting the IP Phone Connections, page 3-15](#)
- [Step 4: Selecting the SoftPhone Connection, page 3-17](#)
- [Step 5: Selecting the CallManager Port, page 3-19](#)
- [Step 6: Selecting the IntraLAN Connections, page 3-21](#)
- [Step 7: Selecting the Voice VLAN Connections, page 3-23](#)
- [Step 8: Selecting the Switch to WAN Router Connection, page 3-25](#)

- [Step 9: Selecting the Router WAN to Switch Connection, page 3-27](#)
- [Step 10: Selecting the WAN Frame Relay Connections, page 3-29](#)
- [Step 11: End, page 3-31](#)

### Before you Begin

To run the wizard, the following preconditions must be met:

- Voice VLANs have been configured on all the relevant ports on your devices to enable the wizard to attach QoS properties to these VLANs.
- All the relevant devices were imported to QPM. See [Lesson 1-2: Importing the Tutorial Virtual Devices, page 1-7](#).
- The “Tutorial” deployment group has been created. See [Lesson 1-4: Creating the Tutorial Deployment Group, page 1-11](#).

### Related Topics

- [Using the IP Telephony Wizard, page 3-9](#)

## Using the IP Telephony Wizard

This topic will help you understand the main features of the IP Telephony wizard and how to use them.

### Description

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.

### Advanced

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

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

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

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

### Selection Table

In each configuration step, you select the network elements that require QoS configuration. The available network elements are presented in a table. You can hide this table by clicking the arrow button next to **Selection Table**. By default, the selection table is open.

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

### Assignment Summary

As you work through the wizard, you can see a summary of the voice policy groups that were created for the current voice role, and the number of network elements that were assigned to them in the current configuration step. This summary page also includes detailed information about the network elements assignments.

### Saving Your Assignments

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

If the Display Configuration Info. check box is selected, clicking Next opens the assignments summary page for that configuration step. The voice policy groups will be saved in the deployment group, but the assignment of interfaces to them



will not be saved. After reviewing your assignments summary, clicking Next in this page saves both the voice policy groups and the interface assignments, and opens the next step of the wizard.

### Related Topics

- [Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard, page 3-8](#)

## Step 1: Introduction

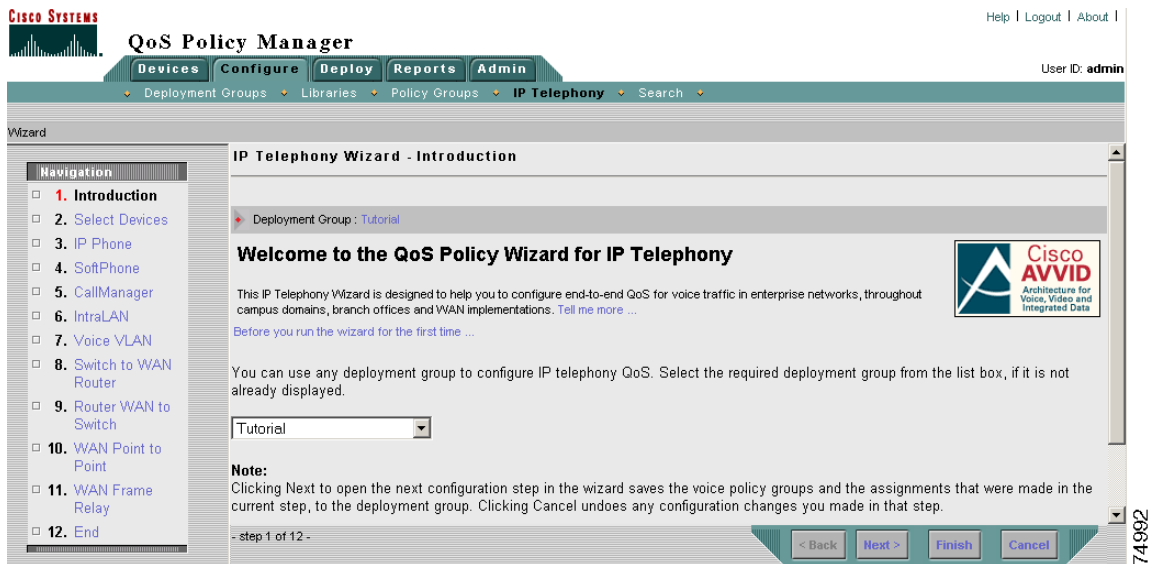
The first step of the wizard includes an overview of why QoS configuration is necessary for VoIP networks, and how the wizard will guide you to configure QoS for IP telephony.

This step also displays the name of the deployment group that is currently open, and will be used by the wizard for defining the IP telephony policies. If the displayed deployment group is not the one you require, you can change it.

### Procedure

- 
- Step 1** Select **Configure > IP Telephony**. The Introduction page of the wizard appears.
- Step 2** If the displayed deployment group is not “Tutorial”, select it from the deployment group list box.

Figure 3-2 Lesson 3-1—Selecting a Deployment Group



**Step 3** Click **Next** or select **Select Devices** in the Navigation TOC, to move to Step 2 of the wizard.

### Related Topics

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Configuring QoS for the Campus Site, page 3-4](#)
- [Using the IP Telephony Wizard, page 3-9](#)
- [Step 2: Selecting Devices for QoS Configuration, page 3-12](#)

## Step 2: Selecting Devices for QoS Configuration

In this step of the wizard, you select the devices you want to configure for voice QoS. All the devices that you imported from your virtual devices file, that support IP telephony features (according to model and OS), are displayed in a table. By default, the wizard selects all the devices.

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

**Note**

---

If you opened the IP Telephony wizard before you imported your devices, no devices will be displayed. You should click Cancel to exit the wizard, and open the Import Devices wizard. See [Lesson 1-2: Importing the Tutorial Virtual Devices, page 1-7](#).

---

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

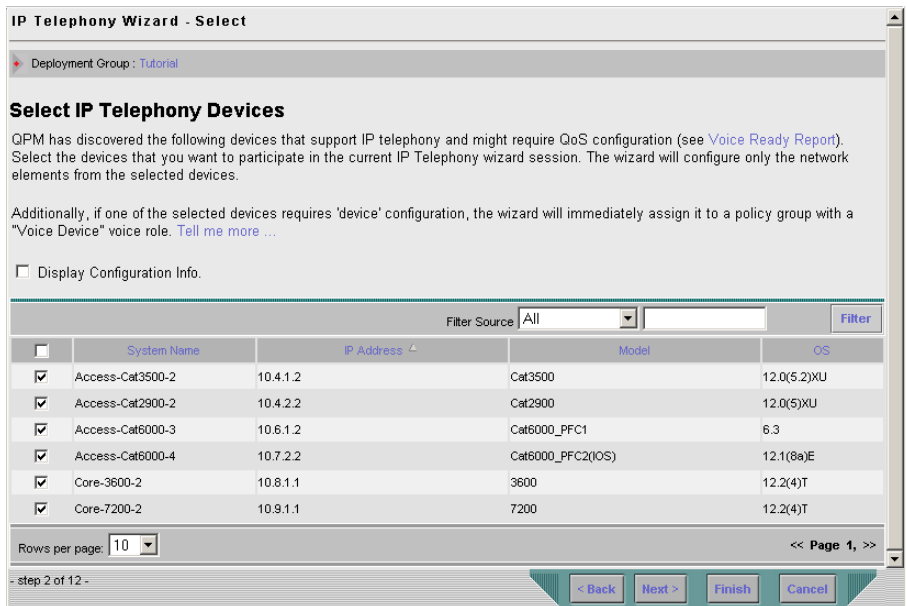
**Procedure**

---

**Step 1** Select the following devices by selecting the check boxes next to them:

- Access-Cat2900-2
- Access-Cat3500-2
- Access-Cat6000-3
- Access-Cat6000-4
- Core-3600-2
- Core-7200-1

Figure 3-3 Lesson 3-1—Selecting IP Telephony Devices



**Step 2** To see all the devices in your device group, and whether they support QoS for voice, click the Voice Ready Report link. The Voice Ready report appears.

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

- If you want to view summary information about the assignments made at each configuration step of the wizard, select the Display Configuration Info. check box, and click **Next**. The Assignment Summary page appears.
- If you don't want to view the assignments summary at each configuration step of the wizard, deselect the Display Configuration Info. check box.

**Step 4** Click **Next** or select **IP Phone** in the Navigation TOC.

The wizard saves the assignment of the selected devices to the appropriate voice policy groups with a Voice Device voice role, and the next configuration step of the wizard appears.

After you have selected all the devices in your IP telephony network that require QoS configuration, you must define the connections for each voice role.

**Related Topics**

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Configuring QoS for the Campus Site, page 3-4](#)
- [Using the IP Telephony Wizard, page 3-9](#)
- [Step 3: Selecting the IP Phone Connections, page 3-15](#)

## Step 3: Selecting the IP Phone Connections

In this step of the wizard, you select the switch ports on which the wizard will configure the QoS settings for all your IP phone connections in the network (network points **1** in [Figure 3-1](#)).

**Procedure**

- 
- Step 1** Select the check box next to the Et2/0 port to configure QoS on the IP phone port connection to the Catalyst 6000 Layer 3 access switch in the campus.
- Step 2** Select the check box next to the Ethernet2/3 port to configure QoS on the IP phone port connection to the Catalyst 3500 Layer 2 access switch in the campus.
- Step 3** Select the check box next to the Ethernet3/1 port to configure QoS on the IP phone port connection to the Catalyst 2900 Layer 2 access switch in the remote branch.

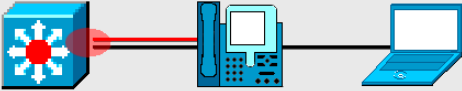
Figure 3-4 Lesson 3-1—Selecting IP Phone Connections

IP Telephony Wizard - Select

Deployment Group: Tutorial

### Select IP Phone Connections

Select the switch ports on which the wizard will configure the QoS settings for the IP phone connections.



**Description**

**Advanced**

**Selection Table**

Display Configuration Info.

Filter Source: All

<input type="checkbox"/>	Name	Type	Description	Card Type	Rate	Device Name	Voice Role	Peer Model
<input type="checkbox"/>	FastEthernet0/1	Ethernet		OTHER	100000	Access-Cat2900-2		
<input checked="" type="checkbox"/>	Ethernet3/1	Ethernet		OTHER	10000	Access-Cat2900-2		
<input checked="" type="checkbox"/>	Ethernet2/3	Ethernet		OTHER	10000	Access-Cat3500-2		
<input type="checkbox"/>	GigabitEthernet0/1	Ethernet		OTHER	1000000	Access-Cat3500-2		
<input checked="" type="checkbox"/>	Et2/0	Ethernet		OTHER	10000	Access-Cat6000-3		
<input type="checkbox"/>	Et2/1	Ethernet		OTHER	10000	Access-Cat6000-3		
<input type="checkbox"/>	Et2/2	Ethernet		OTHER	10000	Access-Cat6000-3		
<input type="checkbox"/>	GigabitEthernet1/0	Ethernet		OTHER	1000000	Access-Cat6000-3		

Rows per page: 10 << Page 1, >>

- step 3 of 12 -

**Step 4** Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next** or select **SoftPhone** in the Navigation TOC.

The selected IP phone ports will be assigned to the appropriate voice policy groups with an IP Phone voice role. The wizard saves the assignment and the next configuration step of the wizard appears.

**Related Topics**

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Configuring QoS for the Campus Site, page 3-4](#)
- [Using the IP Telephony Wizard, page 3-9](#)
- [Step 4: Selecting the SoftPhone Connection, page 3-17](#)

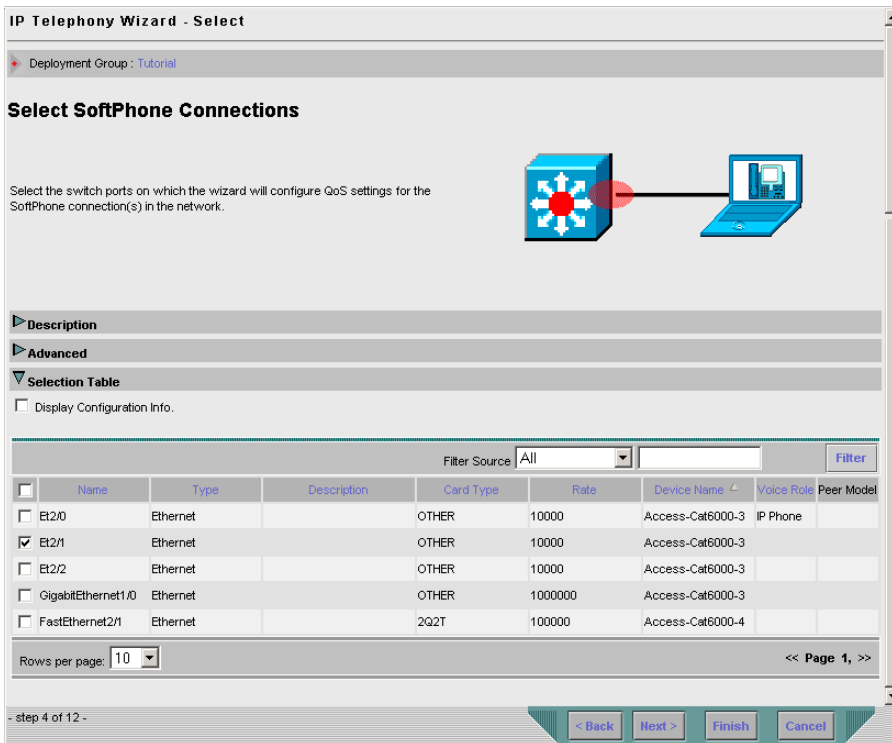
## Step 4: Selecting the SoftPhone Connection

This step allows you to select the switch port on which the wizard will configure the QoS settings for the SoftPhone connection in your network (network point 2 in [Figure 3-1](#)).

**Procedure**

- 
- Step 1** Select the check box next to the Et2/1 Ethernet port on which to configure QoS for the SoftPhone connection to the Catalyst 6000 Layer 3 access switch in the campus.

Figure 3-5 Lesson 3-1—Selecting the SoftPhone Connection

**Step 2** Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next** or select **CallManager** in the Navigation TOC.

The selected SoftPhone port will be assigned to the appropriate voice policy group(s) with a SoftPhone voice role. The wizard saves the assignment and the next configuration step of the wizard appears.

**Related Topics**

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Configuring QoS for the Campus Site, page 3-4](#)



- [Using the IP Telephony Wizard, page 3-9](#)
- [Step 5: Selecting the CallManager Port, page 3-19](#)

## Step 5: Selecting the CallManager Port

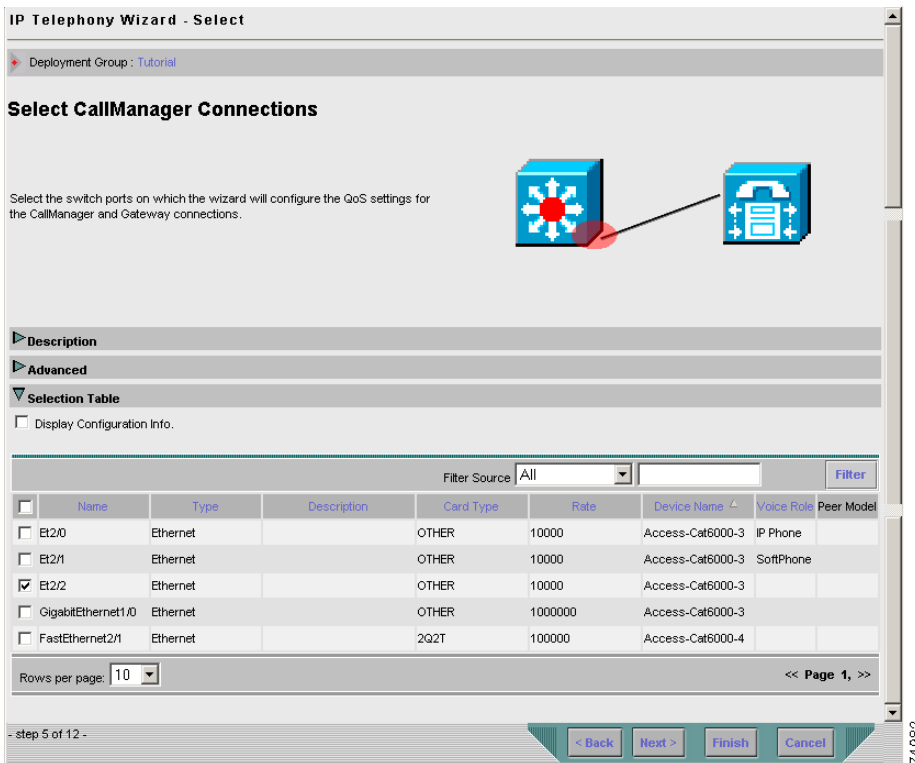
This step allows you to select the switch port on which the wizard will configure the QoS settings for the CallManager connection in your network (network point 3 in [Figure 3-1](#)).

### Procedure

---

- Step 1** Select the check box next to the Et2/2 Ethernet port on which to configure QoS for the CallManager connection to the Layer 3 Catalyst 6000 access switch in the campus.

Figure 3-6 Lesson 3-1—Selecting the CallManager Connection

**Step 2** Click Next.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next** or select **IntraLAN** in the Navigation TOC.

The selected CallManager port will be assigned to the appropriate voice policy group(s) with a CallManager voice role. The wizard saves the assignment and the next configuration step of the wizard appears.

**Related Topics**

- [Understanding the IP Telephony Network Example, page 3-3](#)

- [Configuring QoS for the Campus Site](#), page 3-4
- [Using the IP Telephony Wizard](#), page 3-9
- [Step 6: Selecting the IntraLAN Connections](#), page 3-21

## Step 6: Selecting the IntraLAN Connections

After configuring the QoS access interfaces, you must configure QoS throughout the LAN.

In this step, the wizard helps you define the appropriate QoS for the internal LAN ports—the uplinks and downlinks (network points 4, 5 and 6 in [Figure 3-1](#)).



### Note

---

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

---

The correct QoS for LAN switches connection is to trust DSCP from Layer 3 devices and trust CoS from Layer 2 devices. The wizard will configure the QoS automatically according to the type of neighboring switch. If there is no neighboring switch (or if the switch is of unknown type), QPM will configure trust CoS.

### Procedure

---

**Step 1** Select the check boxes next to the following switch interfaces to configure QoS for the LAN connections in the network:

- GigabitEthernet1/0 (on the Catalyst 6000 access switch)
- GigabitEthernet1/2 (on the Catalyst 6000 distribution switch)
- GigabitEthernet1/1 (on the Catalyst 6000 distribution switch)

Figure 3-7 Lesson 3-1—Selecting the IntraLAN Connections

IP Telephony Wizard - Select

Deployment Group: Tutorial

### Select IntraLAN Connections

After QoS configuration of the access interfaces, QoS must be configured throughout the LAN. Select the uplink and downlink interfaces 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 L2 switches. The wizard will not configure QoS policies on these interfaces.

**Description**

**Advanced**

**Selection Table**

Display Configuration Info.

Filter Source: All

<input type="checkbox"/>	Name	Type	Description	Card Type	Rate	Device Name	Voice Role	Peer Model
<input type="checkbox"/>	E12/0	Ethernet		OTHER	10000	Access-Cat6000-3	IP Phone	
<input type="checkbox"/>	E12/1	Ethernet		OTHER	10000	Access-Cat6000-3	SoftPhone	
<input type="checkbox"/>	E12/2	Ethernet		OTHER	10000	Access-Cat6000-3	CallManager	
<input checked="" type="checkbox"/>	GigabitEthernet1/0	Ethernet		OTHER	1000000	Access-Cat6000-3		
<input checked="" type="checkbox"/>	GigabitEthernet1/1	GigabitEthernet		1P2Q2T	1000000	Access-Cat6000-4		
<input checked="" type="checkbox"/>	GigabitEthernet1/2	GigabitEthernet		1P2Q2T	1000000	Access-Cat6000-4		
<input type="checkbox"/>	FastEthernet2/1	Ethernet		2Q2T	100000	Access-Cat6000-4		

Rows per page: 10

<< Page 1, >>

- step 6 of 12 -

< Back Next > Finish Cancel

744933

**Step 2** Click Next.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next** or select **Voice VLAN** in the Navigation TOC.

The selected interfaces will be assigned to the appropriate voice policy groups with an IntraLAN voice role. The wizard saves the assignment and the next configuration step of the wizard appears.

---

#### Related Topics

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Configuring QoS for the Campus Site, page 3-4](#)
- [Using the IP Telephony Wizard, page 3-9](#)
- [Step 7: Selecting the Voice VLAN Connections, page 3-23](#)

## Step 7: Selecting the Voice VLAN Connections

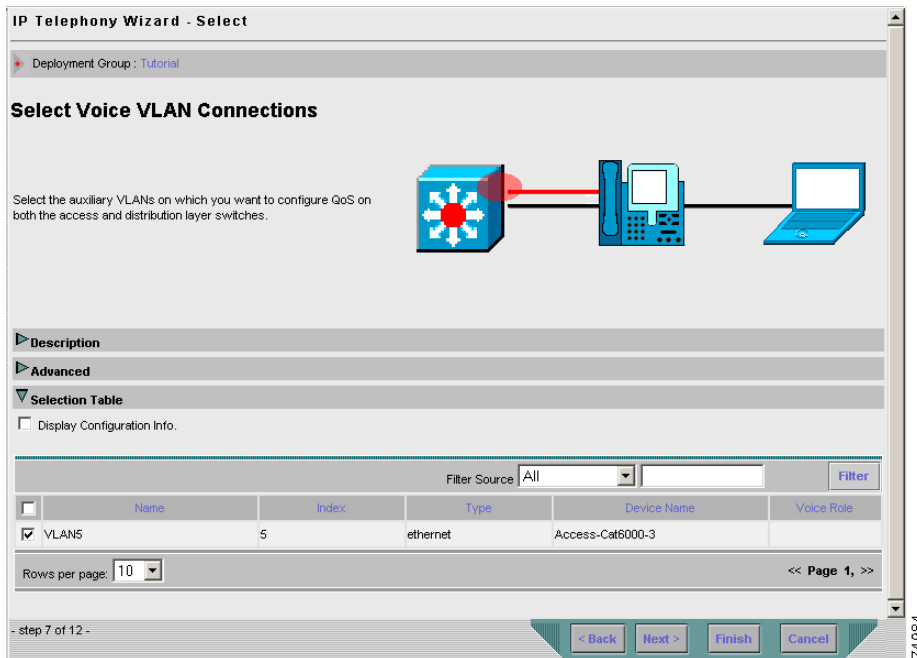
Since the IP phone ports are configured to use an auxiliary voice VLAN on the switches, and the QoS style on the IP phone ports is set to VLAN-based, it is essential to configure the appropriate policies on the voice VLAN. In this step, the wizard configures VLAN based QoS for the VLAN on which the IP phone ports and the Layer 2 switch to Layer 3 switch connections are configured.

#### Procedure

---

- Step 1** Select the check box next to the VLAN5 network element to configure VLAN based policies for the voice VLANs.

Figure 3-8 Lesson 3-1—Selecting the Voice VLAN Connections

**Step 2** Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next** or select **Switch to WAN Router** in the Navigation TOC.

The selected VLAN will be assigned to the appropriate voice policy groups with a Voice VLAN voice role. The wizard saves the assignment and the next configuration step of the wizard appears.

**Related Topics**

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Configuring QoS for the Campus Site, page 3-4](#)
- [Using the IP Telephony Wizard, page 3-9](#)
- [Step 8: Selecting the Switch to WAN Router Connection, page 3-25](#)

## Step 8: Selecting the Switch to WAN Router Connection

In this step, the wizard sets QoS for the Catalyst 6000 distribution switch interface to the Core-7200 WAN router (network point 7 in [Figure 3-1](#)).

Because traffic coming from the WAN side is already classified, the QoS configuration for the distribution switch interface to the router will be to trust the layer 3 DSCP bits.

### Procedure

---

- Step 1** Select the check box next to the FastEthernet2/1 interface in the table, to configure QoS for the distribution switch connection to the WAN router.

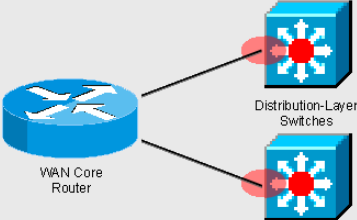
Figure 3-9 Lesson 3-1—Selecting the Switch to WAN Router Connection

IP Telephony Wizard - Select

Deployment Group: Tutorial

### Select Switch to WAN Router Connections

Select the switch interface on which to configure QoS for the distribution switch connection to the WAN router.



**Description**

**Advanced**

**Selection Table**

Display Configuration Info.

Filter Source: All

<input type="checkbox"/>	Name	Type	Description	Card Type	Rate	Device Name	Voice Role	Peer Model
<input type="checkbox"/>	Et2/0	Ethernet		OTHER	10000	Access-Cat6000-3	IP Phone	
<input type="checkbox"/>	Et2/1	Ethernet		OTHER	10000	Access-Cat6000-3	SoftPhone	
<input type="checkbox"/>	Et2/2	Ethernet		OTHER	10000	Access-Cat6000-3	CallManager	
<input type="checkbox"/>	GigabitEthernet1/0	Ethernet		OTHER	1000000	Access-Cat6000-3		
<input type="checkbox"/>	GigabitEthernet1/1	GigabitEthernet		1P2Q2T	1000000	Access-Cat6000-4	IntraLAN	
<input type="checkbox"/>	GigabitEthernet1/2	GigabitEthernet		1P2Q2T	1000000	Access-Cat6000-4	IntraLAN	
<input checked="" type="checkbox"/>	FastEthernet2/1	Ethernet		2Q2T	100000	Access-Cat6000-4		

Rows per page: 10

<< Page 1, >>

- step 8 of 12 -

< Back Next > Finish Cancel

**Step 2** Click Next.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, click **Next** or select **Router WAN to Switch** in the Navigation TOC.



The selected interface will be assigned to the appropriate voice policy groups with a Switch to WAN Router voice role. The wizard saves the assignment and the next configuration step of the wizard appears.

---

#### Related Topics

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Configuring QoS for the WAN, page 3-5](#)
- [Using the IP Telephony Wizard, page 3-9](#)
- [Step 9: Selecting the Router WAN to Switch Connection, page 3-27](#)

## Step 9: Selecting the Router WAN to Switch Connection

In this step, the wizard sets QoS for the router connection to the Catalyst 3500 access (layer 2 QoS aware) switch in the branch office (network point 9 in [Figure 3-1](#)).

By default, a router trusts the interface to a distribution (layer 3 QoS aware) switch, so there is no need to set QoS for the router connection to the Catalyst 6000 distribution switch in the campus.

#### Procedure

---

- Step 1** Select the check box next to the FastEthernet0/1 interface to configure QoS for the Core-3600-2 router interface to the Catalyst 2900 access switch.

Figure 3-10 Lesson 3-1—Selecting the Router WAN to Switch Connection

IP Telephony Wizard - Select

Deployment Group: Tutorial

### Select Router WAN to Switch Connections

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.

**Description**

**Advanced**

**Selection Table**

Display Configuration Info.

Filter Source: All

<input type="checkbox"/>	Name	Type	Description	Card Type	Rate	Device Name	Voice Role	Peer Model
<input checked="" type="checkbox"/>	FastEthernet0/1	Ethernet		OTHER	100000	Core-3600-2		
<input type="checkbox"/>	FastEthernet0/0	Ethernet		OTHER	100000	Core-7200-2		

Rows per page: 10

- step 9 of 12 -

74986

**Step 2** Click **Next**.

- If the Display Configuration Info. check box is selected, the Configuration Info page appears. After reviewing the assignments summary, select **WAN Frame Relay** in the Navigation TOC.
- If the Display Configuration Info. check box is not selected, the WAN Point-to-Point Connections page appears. Click **Next**, or select **WAN Frame Relay** in the Navigation TOC.

The selected interfaces will be assigned to the appropriate voice policy groups with a Router WAN to Switch voice role. The wizard saves the assignment and the next step that you must configure in the wizard will open.



---

**Note** Since the IP telephony network example is configured with Frame Relay and does not support Serial Point-to-Point configuration, you will skip the WAN Point-to-Point Connections configuration step.

---

### Related Topics

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Configuring QoS for the WAN, page 3-5](#)
- [Configuring QoS for the Remote Branch, page 3-5](#)
- [Using the IP Telephony Wizard, page 3-9](#)
- [Step 10: Selecting the WAN Frame Relay Connections, page 3-29](#)

## Step 10: Selecting the WAN Frame Relay Connections

In this step of the wizard, you select the Frame Relay DLCI's WAN links (network points **8** in [Figure 3-1](#)). When you assign a role to a DLCI, the role will also be assigned to the main interface to which the DLCI belongs. QPM configures both the DLCIs and the interfaces.

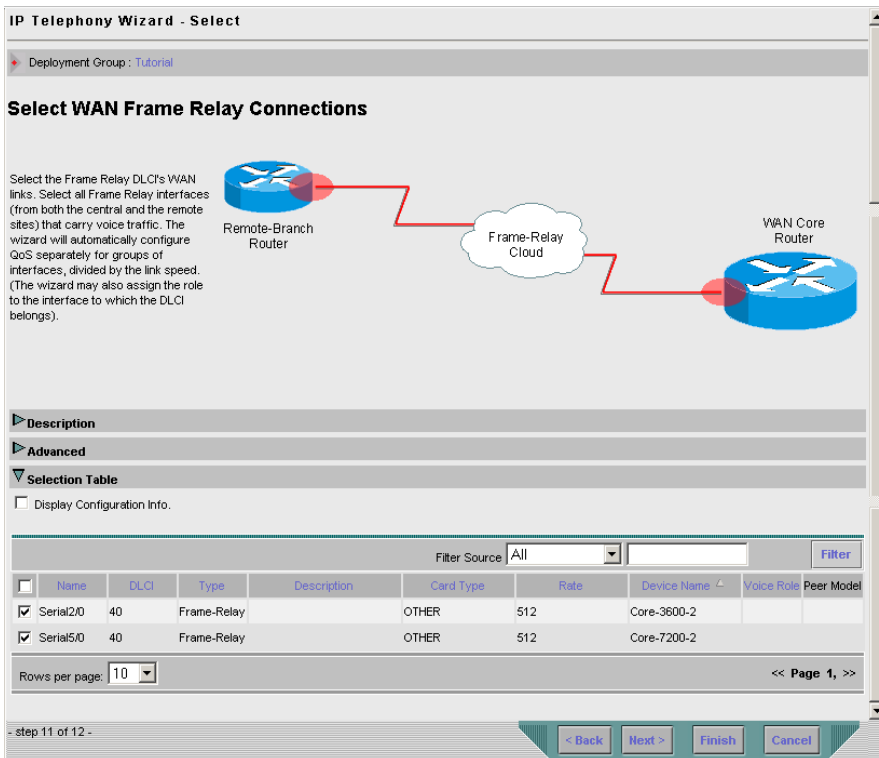
You must select all the Frame Relay interfaces (from both the central and the remote sites) that carry voice traffic. The wizard will automatically configure QoS separately for groups of interfaces, according to their link speed.

### Procedure

---

- Step 1** Select the check box next to the Serial2/0 interface to configure QoS for the Frame Relay DLCI WAN link in the remote site.
- Step 2** Select the check box next to the Serial5/0 interface to configure QoS for the Frame Relay DLCI WAN link in the campus site.

Figure 3-11 Lesson 3-1—Selecting the Frame Relay WAN Links



**Step 3** Click **Next** or select **End** in the Navigation TOC.

The selected interfaces will be assigned to the appropriate voice policy groups with a WAN Frame Relay voice role. The wizard saves the assignment and the final step of the wizard appears.

### Related Topics

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Configuring QoS for the WAN, page 3-5](#)
- [Using the IP Telephony Wizard, page 3-9](#)

- [Step 11: End, page 3-31](#)
- [Lesson 3-2: Modifying the Voice Policies, page 3-32](#)

## Step 11: End

The final step of the wizard informs you that all the QoS settings have been completed and that the wizard has added and saved the policies in your deployment group.

From this page, you can go directly to the Deployment wizard to deploy the deployment group, or to the Policy Groups page to view a detailed summary of all the voice policy groups that you created in the wizard. From the Policy Groups page, you can modify the properties and policies configured in the voice policy groups.

For the purpose of this tutorial, you should select to go to the Policy Groups page and follow the next lesson, which describes how to modify one of the voice policy groups that you created in this lesson.

### Procedure

---

**Step 1** Select the No radio button in the End page of the wizard.

**Step 2** Click **Finish** to close the wizard.

The Policy Groups page appears.

---

### Related Topics

- [Using the IP Telephony Wizard, page 3-9](#)
- [Lesson 3-2: Modifying the Voice Policies, page 3-32](#)

## Lesson 3-2: Modifying the Voice Policies

QPM allows you to customize policies to suit specific network configurations by modifying the voice policy groups. After you have completed the IP Telephony wizard, you can modify properties and policies of the voice policy groups created by the wizard. QPM allows you to modify any of the properties and policies of a voice policy group, except for its device constraints. Changing the device constraints will cause the voice policy group to lose its voice role. In this case, the IP Telephony wizard will be unable to assign network elements to the voice policy group.

**Note**

---

You cannot modify a policy group that is linked to a policy group template. Whenever you want to modify a policy group created by the IP Telephony wizard, you must first disconnect the policy group from the template, or modify the template.

---

In this lesson, you will learn how to modify the following WAN Frame Relay voice policy groups that were created in [Step 10: Selecting the WAN Frame Relay Connections](#) of the wizard:

- **WAN-FR- Main-Interface**—This voice policy group is for a main Frame Relay interface that has DLCI interfaces for voice traffic. In this voice policy group, IP RTP Header Compression (cRTP) is not configured on the Frame Relay links. Although cRTP reduces the consumption of available bandwidth for voice traffic, resulting in a reduction in traffic delay, it utilizes a lot of CPU in routers, which might cause performance problems. If CPU utilization is less than 75%, cRTP might be enabled. In this lesson, you will learn how to enable cRTP for this voice policy group.
- **WAN-FR-DLCI-Slow**—This voice policy group is for low speed Frame Relay interfaces. To ensure that real-time, delay-sensitive voice traffic can be carried over Frame Relay links, you must configure the bandwidth reserved for voice traffic. In this lesson, you will learn how to configure the percentage of bandwidth that should be reserved for the voice traffic.

**Before You Begin**

To do this lesson you should have completed [Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard](#), page 3-8.

After you have completed the IP Telephony wizard and you selected not to deploy your QoS policies, as described in [Step 11: End, page 3-31](#), the Policy Groups page automatically appears. The Policy Groups page displays all the voice policy groups that were created by the wizard. For each voice policy group, its associated voice role is displayed.

**Tip**

---

You can also open the Policy Groups page by selecting **Configure > Policy Groups**.

---

This lesson is divided into the following two lessons:

- [Lesson 3-2-1: Enabling cRTP for the WAN-FR-Main-Interface Voice Policy Group, page 3-33](#)
- [Lesson 3-2-2: Configuring the Voice Traffic Bandwidth for the WAN-FR-DLCI-Slow Voice Policy Group, page 3-37](#)

## Lesson 3-2-1: Enabling 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. In this lesson, you will learn how to enable cRTP for the WAN-FR-Main-Interface voice policy group.

### Procedure

- 
- Step 1** In the Policy Groups page, click the WAN-FR-Main-Interface policy group name in the table (you might need to open page 2 to find it). The General page appears, displaying general definitions for the selected policy group.

Figure 3-12 General Page for the WAN-FR-Main-Interface Policy Group

General ⓘ

Deployment Group : Tutorial > Policy Group : WAN-FR-Main-Interface

This policy group is connected to template WAN-FR-Main-Interface

Policy Group	
Name:	WAN-FR-Main-Interface
Description:	This policy group is for a main, Frame Relay interface that has DLCI interfaces for voice traffic, running IOS 12.1(3T) and later. (There are separate templates for the DLCI subinterfaces themselves.)
Total policies and properties:	2
Assigned to:	2 interfaces
Attached to template:	WAN-FR-Main-Interface <a href="#">Disconnect</a>
Voice Role:	WAN Frame Relay
<a href="#">Edit</a>	

- Step 2** Click **Disconnect** to disconnect the voice policy group from the template. The Edit button at the bottom of the page becomes active.
- Step 3** In the Policy Group TOC, select **QoS Properties**. The QoS Properties page appears.

Figure 3-13 QoS Properties Page for the WAN-FR-Main-Interface Policy Group

QoS Properties ⓘ

Deployment Group : Tutorial > Policy Group : WAN-FR-Main-Interface

QoS Properties	
Scheduling	Class based QoS
FRTS	
CRTP	not configured
Modular Shaping	not configured
IP RTP	not configured
FRF	not configured
WRED	not configured
<a href="#">Edit</a>	





**Note** cRTP is not configured.

**Step 4** Click **Edit** in the QoS Properties page. The QoS Properties wizard—Congestion Management page appears.

**Step 5** Select **Traffic Control Settings** in the Navigation TOC.

The QoS Properties wizard—Traffic Control Settings page appears, displaying the traffic control parameters that were configured by the IP Telephony wizard for the WAN-FR-Main-Interface voice policy group.

**Figure 3-14** Traffic Control Settings for the WAN-FR-Main-Interface Policy Group

QoS Properties Wizard - Traffic Control Settings

Configure the IP RTP Priority properties:

Set the IP RTF Header Compression properties:

**Enable IP RTP Header Compression**

**Passive**

Set the voice configuration properties:

**Enable Voice Configuration**

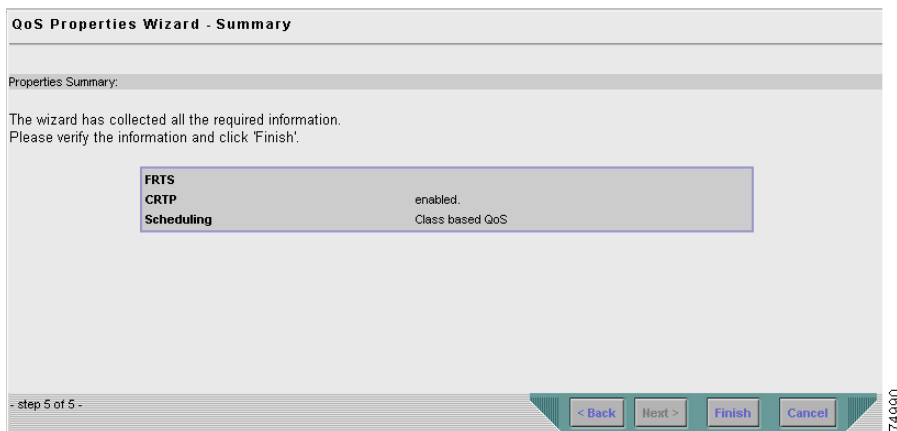
Bandwidth(%):

Fragment (optional):   Bytes  MSec

- step 3 of 5 -

74991

**Step 6** Select the Enable IP RTP Header Compression check box, and click **Finish**. The QoS Properties Wizard Summary page appears, in which you can view a summary of the QoS properties defined for the voice policy group.

**Figure 3-15 Summary Page for the WAN-FR-Main-Interface Policy Group**

**Note** cRTP is now enabled for the voice policy group.

**Step 7** Click **Finish** to save the changes.

The QoS Properties page appears, displaying the modified configuration. cRTP is now configured for this voice policy group.

**Step 8** Select **Configure > Policy Groups**. The Policy Groups page appears.

**Step 9** Continue with [Lesson 3-2-2: Configuring the Voice Traffic Bandwidth for the WAN-FR-DLCI-Slow Voice Policy Group, page 3-37](#).

### Related Topics

- [Lesson 3-2: Modifying the Voice Policies, page 3-32](#)
- [Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard, page 3-8](#)
- [Step 10: Selecting the WAN Frame Relay Connections, page 3-29](#)

## Lesson 3-2-2: Configuring the Voice Traffic Bandwidth for the WAN-FR-DLCI-Slow Voice Policy Group

In this lesson, you will learn how to modify the WAN-FR-DLCI-Slow voice policy group, by creating a QoS policy that configures the percentage of bandwidth on the interface that should be reserved for your voice traffic.

You can create policies in a policy group, or in a policy group template. This lesson describes how to modify the WAN-FR-DLCI-Slow policy group template to create the QoS policy. Changes made in the policy group template will also apply to the attached voice policy group—WAN-FR-DLCI-Slow.

A QoS policy contains a filter and actions, so you will need to define the filter for the policy, and then the policy action(s). A filter can contain filter condition(s) which you must also define for the filter rule. After it is created, the new QoS policy will be added to the outbound policies currently defined for the template.

### Procedure

---

- Step 1** In the Policy Groups page, click the WAN-FR-DLCI-Slow policy group template name in the table (you might need to open page 2 to find it). The General page for the policy group template appears, displaying general definitions for the selected template.

Figure 3-16 General Page for the WAN-FR-DLCI-Slow Policy Group Template

General ⓘ

Policy Group Template : WAN-FR-DLCI-Slow

Policy Group Template	
Name:	WAN-FR-DLCI-Slow
Description:	This policy group is for low-speed (<=768K) Frame Relay subinterfaces. The QoS configuration for these subinterfaces use FRTS with CIR, and because a different configuration is required for each speed, there are few templates. When you use these templat
Total policies and properties:	7
Voice Role:	WAN Frame Relay

Edit

**Step 2** In the Policy Group TOC, select **Out Policies**. The Out Policies page appears, displaying the current outbound policies defined for the template.

Figure 3-17 Out Policies Page for the WAN-FR-DLCI-Slow Policy Group Template

Out Policies ⓘ

Policy Group Template : WAN-FR-DLCI-Slow

Filter Source: All Filter

<input type="checkbox"/>	Policy Order ↕	Enable	Policy Name	Filter	Action
<input type="checkbox"/>	1	✓	VoIP gets LLQ 40 percent	OR DSCP: ef OR IP Precedence: critical	Bandwidth Bandwidth 40%, Priority LLQ enabled, ,
<input type="checkbox"/>	2	✓	VoIP cntrl 10percent BW	OR DSCP: af31 OR IP Precedence: flash	Bandwidth Bandwidth 10%,
<input type="checkbox"/>	3	✓	Class-Default-Out	Class Default	Fairness ,

Rows per page: 10 << Page 1, >>

↑-- Select an item then take an action -->

Create Disable Enable Reorder Edit Delete

**Step 3** Click **Create** in the Out Policies page. The General page of the Out Policy wizard appears.

**Figure 3-18 Out Policy Wizard - General Page**

Out Policy Wizard - General

Enter the policy's name: ⓘ

Policy Name: My data gets 20 percent

Enter description for the policy: ⓘ

This policy configures the percentage of bandwidth to be reserved for my voice traffic data.

QoS policy

QoS Policy

- step 1 of 4 -

< Back Next > Finish Cancel

74989

- Step 4** Do the following in the Out Policy wizard - General page:
- Enter **My data gets 20 percent BW** in the Policy Name field.
  - Enter **This policy configures the percentage of bandwidth to be reserved for my voice traffic data** in the description field.
  - Select the QoS Policy check box to define the type of policy you want to create.
  - Click **Next**. The Out Policy wizard - Filter page appears.

Figure 3-19 Out Policy Wizard - Filter Page

Out Policy Wizard - Filter

Select how to define the traffic type of the policy:

Create a new filter  Class Default

Enter name for the filter (optional):

Filter name:

Add and edit rules for the current filter.

<input type="checkbox"/> Not	Rules
No Records Found	

← Select an item then take an action →

- step 2 of 4 -

75000

- Step 5** Define a filter to specify the traffic to which the policy should be applied:
- In the Out Policy wizard - Filter page, select the **Create a new filter** check box. This enables the policy to be applied to traffic that matches any of the filter conditions.
  - Enter **MyDataFilter** in the Filter name field.
  - Click **Create**. The Rule Setting page appears, displaying the conditions you can define for each filter rule.
- Step 6** Define the condition for the filter rule:
- In the Rule Setting page, click **Edit** next to the Service filter condition. The Service Editor dialog box opens.
  - From the Value list box, select **18 (af21)**—the DSCP value of the packet. (For this example, it is assumed that data traffic was already marked at the edge.)
  - Click **OK**. The Service Editor dialog box closes, and the Rule Settings page refreshes to display the new Service condition.
  - Click **Done**. The Out Policy Wizard - Filter page reappears, displaying the filter rule you have defined.

**Figure 3-20 Out Policy Wizard - Filter Page**

Out Policy Wizard - Filter

Select how to define the traffic type of the policy:

Create a new filter  Class Default

Enter name for the filter (optional):

Filter name:

Add and edit rules for the current filter.

<input type="checkbox"/> Not	Rules
<input checked="" type="checkbox"/>	DSCP: sf21

Select an item then take an action -->

Create Edit Delete

- step 2 of 4 -

< Back Next > Finish Cancel

81004

**Step 7** Click **Next** in the Out Policy Wizard - Filter page. The Out Policy Wizard - Actions page for Marking appears.

**Step 8** Define the QoS policy action:

- a. Select **Actions > Queuing** in the wizard navigation TOC. The Out Policy Wizard - Queuing Actions page appears. (Queuing actions manage congestion for outbound traffic.)
- b. Select the Enable Bandwidth Allocation (CBQ) check box.
- c. Enter **20** in the Bandwidth field to define the percentage of the interface's bandwidth you want to allocate to your traffic.

Figure 3-21 Out Policy Wizard - Queuing Actions Page

Out Policy Wizard - Queuing

Specify the priority of the traffic:

Enable Priority (LLQ) Optional Burst:  bytes

Specify the bandwidth to allocate to the traffic:

Enable Bandwidth Allocation (CBO)

Bandwidth  Ratio

- step 3 of 4 -

< Back Next > Finish Cancel

81005

**Step 9** Click **Finish** to complete the wizard. The Summary page appears.

Figure 3-22 Out Policy Wizard - Summary Page

Out Policy Wizard - Summary

Policy Summary:

The wizard has collected all the required information.  
Please verify the information and click 'Finish'.

<b>Name</b>	My data gets 20 percent BW
<b>Description</b>	This policy configures the percentage of bandwidth to be reserved for my voice traffic data.
<b>Type</b>	QoS policy
<b>Status</b>	Enabled
<b>Direction</b>	Out
<b>Filter</b>	The Filter <b>MyDataFilter</b> contains the following rules (grouped by <b>OR</b> ): <b>DSCP</b> : af21
<b>Policy action</b>	The policy contains the following actions: <b>Bandwidth</b> : Bandwidth 20%

- step 4 of 4 -

< Back Next > Finish Cancel

74994

**Step 10** In the Summary page, view the details of the QoS policy you defined. Then click **Finish** to complete the policy and exit the wizard.

The Out Policies page reappears, displaying the new policy you defined for the selected template.



Figure 3-23 Out Policies Page with New Policy

<input type="checkbox"/>	Policy Order	Enable	Policy Name	Filter	Action
<input type="checkbox"/>	1	✓	VoIP gets LLQ 40 percent	OR DSCP: ef OR IP Precedence: critical	Bandwidth Bandwidth 40%, Priority LLQ enabled.,
<input type="checkbox"/>	2	✓	VoIP cntrl 10percent BW	OR DSCP: af31 OR IP Precedence: flash	Bandwidth Bandwidth 10%,
<input type="checkbox"/>	3	✓	Class-Default-Out	Class Default	Fairness ,
<input type="checkbox"/>	4	✓	My data gets 20 percent	OR DSCP: af21	Bandwidth Bandwidth 20%,

Since policies on an interface are executed top-down according to the list displayed in the table, they should appear in order of importance to ensure they get the required priority. In [Figure 3-23](#), the Class Default policy precedes your new QoS policy. Since this policy is applied to all traffic that does not match any of the filters, you must reorder the policies so that it appears last in the list.

**Step 11** Change the order of the policies in the policy group template:

- a. Click **Reorder** in the Out Policies page. The Reorder Policies dialog box opens.
- b. In the Reorder Policies dialog box, select **My data gets 20 percent BW** and click the Up button.
- c. Click **OK**. The dialog box closes, and the Out Policies page reappears displaying the new policies order.

Figure 3-24 Out Policies Page with New Policy Reordered

Out Policies i

Policy Group Template : WAN-FR-DLCI-Slow

Filter Source: All Filter

<input type="checkbox"/>	Policy Order	Enable	Policy Name	Filter	Action
<input type="checkbox"/>	1	✓	VoIP gets LLQ 40 percent	OR DSCP: ef OR IP Precedence: critical	Bandwidth Bandwidth 40%, Priority LLQ enabled.,
<input type="checkbox"/>	2	✓	VoIP cntrl 10percent BW	OR DSCP: af31 OR IP Precedence: flash	Bandwidth Bandwidth 10%,
<input type="checkbox"/>	3	✓	My data gets 20 percent	OR DSCP: af21	Bandwidth Bandwidth 20%,
<input type="checkbox"/>	4	✓	Class-Default-Out	Class Default	Fairness ,

Rows per page: 10 << Page 1, >>

Select an item then take an action-->

- Step 12** Check that the QoS policy you defined in the WAN-FR-DLCI-Slow policy group template was also created in the attached voice policy group:
- Select **Configure > Policy Groups**. The Policy Groups page appears.
  - Click the WAN-FR-DLCI-Slow voice policy group name in the table (you might need to open page 2 to find it). The General page appears.
  - In the Policy Group TOC, select **Out Policies**. The Out Policies page appears, displaying the newly defined QoS policy in the list with all the outbound policies for the WAN-FR-DLCI-Slow voice policy group.
- Step 13** Continue with [Lesson 3-3: Deploying the IP Telephony QoS Policies, page 3-45](#).

### Related Topics

- [Lesson 3-2: Modifying the Voice Policies, page 3-32](#)
- [Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard, page 3-8](#)
- [Step 10: Selecting the WAN Frame Relay Connections, page 3-29](#)

# Lesson 3-3: Deploying the IP Telephony QoS Policies

This lesson describes how to deploy the QoS policies that were saved in your deployment group to the devices in the network, where they will be implemented.



## Note

---

Although you can follow all the steps in this lesson, the actual deployment of the “Tutorial” deployment group will fail, since you cannot deploy to virtual devices in the network. However, if you are using real devices in your IP telephony network, you should be able to deploy your QoS policies to your devices successfully.

---

To distribute your QoS policies to your physical network devices, QPM translates your policies into device commands and enters the commands through the device’s command line interface (CLI). You can choose whether or not to deploy your QoS configurations directly to the network devices using Telnet. QPM automatically deploys your QoS configurations to configuration files. This procedure does not configure your devices but generates configuration files that can be sent manually to the devices. QoS configurations can be deployed to the device using any application that downloads configuration files to the devices.

## Before You Begin

To do this lesson you should have completed [Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard, page 3-8](#).

## Procedure

- 
- Step 1** Select **Deploy > Deployment**. The first step of the Deployment wizard appears—Deployment Group Selection.
  - Step 2** Select the Current version of a deployment group radio button, and select **Tutorial** from the list box (if it isn’t already selected).
  - Step 3** Click **Next** to move to the next step of the wizard—the Device Selection and Preview page.

This page displays a list of all the devices that are available for deployment. In this step of the wizard, you select the devices you want to deploy to. You can also preview your device configurations prior to deployment.

- Step 4** If you are using virtual devices, select the check boxes next to the virtual devices in your IP Telephony network example. If you are using real devices, select the check boxes next to the devices to which you want to deploy your policies. Deselect those you do not want to deploy to.
- Step 5** If you want to preview the CLI configuration commands for a device, click its configuration link in the table. A preview window opens, in which you can view the Backup ShowRun configuration commands and any incremental Telnet script commands that will be written to the device.
- Step 6** After you have finished previewing the device's configuration, click **Close** to close the Preview window.
- Step 7** Click **Next** to move to the next step of the wizard—the Job Details page.
- Step 8** Enter **IPT\_Tutorial** in the Job Name field.
- Step 9** If required, you can enter a description for the job in the Job Description box.
- Step 10** Make sure the Deploy configuration to the devices using Telnet check box is selected. (The configuration will also be saved to files.)
- Step 11** Click **Next** to move to the final step of the wizard. This page presents a summary of the data collected through the wizard for you to verify.
- Step 12** After you have verified the job information, click **Deploy** to deploy the deployment group to the network.
- The Active Jobs page appears, enabling you to monitor the deployment process, as described in the next lesson.
- 

### Related Topics

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Lesson 3-4: Monitoring the Deployment Process, page 3-47](#)

## Lesson 3-4: Monitoring the Deployment Process

QPM allows you to monitor the deployment process, by viewing the activity and status of your deployment job, in real-time. The Active Jobs page provides a dynamic view of all the currently active deployments and their status. For each job, the start time of configuration for each job, the job's status, and a summary of the number of devices deployed according to their status, is displayed.

The status of a job deployment or a device deployment may be Pending, In Progress, Completed, or Failed. A job deployment may also have the status of Aborted or Paused. For your deployment job to be "Completed", all the devices must be successfully configured. If the deployment of one device fails, the entire deployment fails.

### Before You Begin

To do this lesson you should have completed Lessons 3-1 and 3-3.

### Procedure

---

#### Step 1 Select **Deploy > Jobs > Active Jobs**.

The Active Jobs page appears, displaying your current deployment job and its status.



#### Tip

The display is automatically refreshed every ten seconds. You can refresh manually by clicking the Refresh button.

---

#### Step 2 View the status of your deployment job.

During the deployment process, a status of In Progress will be displayed for your job. The status will change to Failed, since the devices in your network are virtual and you cannot deploy to virtual devices in a network.



#### Note

If you are using real devices in your network, the status should change to Completed, indicating that your deployment job was completed successfully.

---

**Related Topics**

- [Understanding the IP Telephony Network Example, page 3-3](#)
- [Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard, page 3-8](#)
- [Lesson 3-3: Deploying the IP Telephony QoS Policies, page 3-45](#)



## QoS Analysis Tutorial

---

These topics help you understand how to use QPM monitoring to analyze the effect of your QoS policies on your network traffic. By graphing traffic based on how it matches the filters in your policies, QPM helps you see the types of traffic on your network as well as how the traffic is modified by the policies. This can help you adjust your policy definitions to obtain the desired impact on traffic.

- [Understanding QPM Monitoring, page 4-1](#)
- [Lesson 4-1: Doing a Baseline Traffic Analysis, page 4-5](#)
- [Lesson 4-2: Monitoring QoS, page 4-18](#)
- [Lesson 4-3: Monitoring QoS in Real Time, page 4-28](#)

## Understanding QPM Monitoring

QPM monitors traffic based on the QoS policies that have been distributed to network interfaces using QPM. QPM cannot monitor traffic on interfaces that do not have QoS policies, or on interfaces where QoS policies have been defined by other means.

These topics help you understand QPM's monitoring capabilities.

- [What is the Purpose of QoS Analysis?, page 4-2](#)
- [What Can You Monitor Using QPM?, page 4-2](#)
- [What Is the Difference Between Historical and Real-Time Monitoring?, page 4-3](#)
- [How Much Disk Space Is Required for Historical Monitoring?, page 4-4](#)

## What is the Purpose of QoS Analysis?

QoS Analysis serves these main purposes:

- **Baseline Traffic Analysis**—The analysis of your existing traffic patterns before they are affected by QoS policies. Creating a baseline traffic analysis helps you understand your existing traffic, based on DiffServ classes or applications, so that you can develop QoS policies that are meaningful for the actual traffic on your network. [Lesson 4-1: Doing a Baseline Traffic Analysis, page 4-5](#) describes how to do baseline traffic analysis.
- **QoS Analysis**—The analysis of how your QoS policies are affecting network traffic. By monitoring QoS policies, you can determine if they are affecting traffic in the desired way, or if the policies need to be adjusted. [Lesson 4-2: Monitoring QoS, page 4-18](#) describes how to do QoS analysis.
- **QoS Troubleshooting**—The real-time analysis of traffic on an interface, based on QoS policy, to help you determine if a problem you are having on an interface is related to the QoS policies that are active on the interface. [Lesson 4-3: Monitoring QoS in Real Time, page 4-28](#) describes how to do real-time monitoring.

## What Can You Monitor Using QPM?

You can monitor the traffic on any interface on which you have distributed QoS policies using QPM. These policies do not have to be created using QPM. If you already have QoS policies defined on your interfaces, you can use QPM to import the policies, and then have QPM redistribute the policies to the interfaces. This action does not change the policies on the interface; it simply makes QPM aware of the policies. It also lets you thenceforth use QPM to modify and redistribute these policies.

If you do not already have QoS policies defined, you can use QPM to create a set of QoS policies that do not affect traffic to categorize traffic and help you establish a baseline for the traffic on your network, as described in [Lesson 4-1: Doing a Baseline Traffic Analysis, page 4-5](#). Or, if you already know what you want to do with QoS, you can create QoS policies that do affect network traffic and monitor the results, as described in [Lesson 4-2: Monitoring QoS, page 4-18](#).



## What Is the Difference Between Historical and Real-Time Monitoring?

QPM has two types of monitoring: historical and real-time. Historical monitoring is best used when you want to collect a lot of data over several hours, days, or even months. Real-time monitoring is best used for immediate troubleshooting.

[Table 4-1](#) shows some differences between the types of monitoring.

**Table 4-1 Differences Between Historical and Real-Time Monitoring**

Characteristic	Historical	Real-Time
Maximum number of interfaces monitored per task	12	1
Disk space requirements	Substantial. See <a href="#">How Much Disk Space Is Required for Historical Monitoring?</a> , page 4-4	No disk space used. Data is only presented on web page; it is not saved.
Polling interval for data collection	From 1 to 60 minutes.	From 10 to 30 seconds.
Length of task	Up to several months, depending on polling interval. QPM enforces a duration limit based on polling interval. See the <i>User Guide for CiscoWorks QoS Policy Manager 3.0</i> for the specific limits.	As long as you want, but you must be at the computer to see the data.
Reuse of monitoring task	Can only be run once, because you set a start and end time.	Can be rerun any time desired, because there is no set start or end time.
Reviewing results	Can review the results as many times as you want.	Results must be reviewed as they are collected.

## How Much Disk Space Is Required for Historical Monitoring?

Historical monitoring tasks can create a large amount of data. For example, an historical monitoring task for two interfaces that each have three policies (each with two conditions in the filter and one action), with a polling interval of 10 minutes, would generate approximately 600KB if run for 32 hours. The same task would generate 3000KB if the polling interval was reduced to 2 minutes.

These would both be considered small tasks. An historical monitoring task for 12 interfaces that each have six policies (each with one condition in the filter and two actions), with a polling interval of 10 minutes, would generate 66MB if run for ten days.

These are the factors that increase disk space usage for each historical monitoring task:

- Number of interfaces monitored—The more interfaces, the more data is collected.
- Number of policies—The policies on each interface are considered unique policies. For example, if you deploy the same five policies to ten interfaces, the total number of policies is 50, not five.
- Number of filters—Separate statistics are collected for each filter condition in a policy.
- Number and type of actions—Separate statistics are collected for each action in a policy. The amount of data also differs based on the type of action; for example, complex actions like policing (three counters) or WRED (21 counters) generate more data than simple queuing (one counter).
- Polling interval and duration—QPM collects a complete set of data during each polling interval, so the more frequent the polling interval, and the longer the task is run, the more data is collected. Due to the amount of data that can be generated, QPM limits the duration of tasks based on the polling interval; QPM will tell you if you select a duration too long for the polling interval. See *User Guide for CiscoWorks QoS Policy Manager 3.0* for the specific limitations.

The polling interval and duration can also affect how many concurrent tasks you can run. In general, you should run concurrent tasks on a representative sample of your WAN interfaces. If you choose a polling period of 1 minute, you should not collect data on more than 50 interfaces. If you select longer polling periods, you can analyze more interfaces.

When you install QPM, you specify how much free disk space should be maintained for database backups. If you leave insufficient space, monitoring tasks might use up your disk space. If this happens, all historical monitoring tasks stop and you must delete them. Thus, you should manage the disk space used by historical monitoring tasks by:

- Selecting realistic polling intervals and durations
- Periodically deleting old tasks when you are finished analyzing the data
- Exporting old tasks if you want to save the data

## Lesson 4-1: Doing a Baseline Traffic Analysis

Before you develop QoS policies, you might want to analyze your existing network traffic to help you determine the types of policies from which your network might benefit. To monitor your existing network traffic using QPM, you must first deploy QoS policies to the interfaces you want to monitor. These policies should filter traffic into meaningful groups, but they should not affect the traffic.

These topics explain how to set up a baseline traffic analysis in more detail:

- [Understanding How to Monitor Traffic for Baseline Analysis, page 4-5](#)
- [Step 1: Filtering Traffic for Analysis, page 4-6](#)
- [Step 2: Setting Up an Historical Monitoring Task, page 4-11](#)
- [Step 3: Reading the Historical Monitoring Graphs, page 4-13](#)

## Understanding How to Monitor Traffic for Baseline Analysis

QPM can only monitor traffic if the traffic meets the filter requirements of a QoS policy. Thus, to create graphs that show your existing network traffic, you must deploy QoS policies to each network interface where you want to take a baseline reading. These QoS policies should filter traffic without affecting the traffic.

You can use class-based policing policies to accomplish this type of filtering. Specifically, the policing policies should have these characteristics:

- **QoS Property for the policy group**—Select Class-Based QoS for the scheduling method for the policy group.
- **Filters**—Try to isolate types of traffic on your network that you will want to treat the same way. For example, you might create a filter for applications that require real-time performance (such as voice and video), another filter for important data-intensive applications (such as database, CRM, or other ERP traffic), and another filter for traffic that is not critical to your business (such as Gnutella traffic). Each network has its own definition of critical versus non-critical traffic, so use your knowledge of the network to filter traffic into meaningful groups.
- **Actions**—Set the Rate, Burst Size, and Exceed Burst policing rates to 8.0 Kbps. Set both the Conform and Exceed actions to Transmit. This ensures that all traffic is transmitted without the policies affecting the traffic.

#### Related Topics

- [Step 1: Filtering Traffic for Analysis, page 4-6](#)
- [Understanding QPM Monitoring, page 4-1](#)

## Step 1: Filtering Traffic for Analysis

Before you can do a baseline analysis of the traffic on an interface, you must create a policy group with the interfaces and an appropriate set of policies. The policies filter traffic into analyzable groups.

#### Before You Begin

This step assumes you have already added devices and interfaces to QPM, and that you have created a deployment group. The lessons in [Introduction, page 1-1](#) and [Data Network Tutorial, page 2-1](#) describe how to define these items in QPM.

As you follow this procedure, you must substitute your own device names and constraints for the example names and constraints. Also, modify the policy filters to make them meaningful for your network; the examples shown might not provide you with meaningful baseline information for your network.

## Procedure

---

- Step 1** Select **Configure > Policy Groups**. The Policy Groups page appears.
- Step 2** Select your deployment group from the Deployment Group list box.  
The page refreshes to display the policy groups in the deployment group, if any.
- Step 3** Create the policy group:
- Click **Create**. The Policy Group Definition wizard starts.
  - In the Policy Group Definition Wizard - General Definition page, enter a name and optionally a description for the policy group. For this example, the policy group name is **BaselineMonitoringDemo**.  
Click **Next**. The Policy Group Definition Wizard - Constraints Definition page appears.
  - In the Policy Group Definition Wizard - Constraints Definition page, click **Define Manually**, and enter the device constraints for the devices and interfaces you want to monitor. For this example, the device constraints are:
    - Model**—1720
    - OS Version**—12.2T
    - Network Element Type**—Interface
    - Interface Type**—HDLCClick **OK** to save the device constraints. The Policy Group Definition Wizard - Constraints Definition page appears.  
If you want to add other device constraints, click **Define Manually** and add them.
  - After you are finished defining device constraints, click **Next** in the Policy Group Definition Wizard - Constraints Definition page.  
The Policy Group Definition Wizard - Capabilities Report page appears, where you can view a summary of the QoS features that can be configured for the policy group, according to the device constraints.
  - In the Policy Group Definition Wizard - Capabilities Report page, click **Finish**. The QoS Properties page appears.

- Step 4** Select Class-based QoS as the QoS property for the policy group:
- a. In the QoS Properties page, click **Edit**. The QoS Properties Wizard - Congestion Management page appears.
  - b. In the QoS Properties Wizard - Congestion Management page, select **Class-based QoS** for the scheduling method and click **Finish**. The QoS Properties Wizard - Summary page appears, where you can view a summary of the QoS properties for the policy group.
  - c. Click **Finish** again to save your changes. The QoS Properties page appears.
- Step 5** Assign network elements to the policy group:
- a. Select **Assigned Network Elements** in the TOC. The Assigned Network Elements page appears.
  - b. In the Assigned Network Elements page, select **Add**. The Assignment dialog box opens.
  - c. In the Assignment dialog box, select the network elements that you want to monitor. In this example, we are selecting the single interface Serial0 on 10.51.116.154.
  - d. Click **Assign**. The dialog box closes and the selected network elements appear on the Assigned Network Elements page.
- Step 6** Create the policies to filter traffic into meaningful groups. In this example, we will create five policies. The policy characteristics are described in [Table 4-2](#). This procedure will show you how to create the EF policy. Repeat the process to create the other policies.

Table 4-2 Baseline Monitoring Demo Policies

Policy Order	Policy Name	Filter	Action
1	EF	<ul style="list-style-type: none"> <li>• or DSCP: ef</li> </ul>	<b>Policing:</b> <ul style="list-style-type: none"> <li>• Rate Limit: rate 8.0, burst 8.0, exceed 8.0.</li> <li>• Conform action: transmit</li> <li>• Exceed action: transmit</li> </ul>
2	AF3	<ul style="list-style-type: none"> <li>• or DSCP: af31</li> <li>• or DSCP: af32</li> <li>• or DSCP: af33</li> </ul>	<b>Policing:</b> <ul style="list-style-type: none"> <li>• Rate Limit: rate 8.0, burst 8.0, exceed 8.0.</li> <li>• Conform action: transmit</li> <li>• Exceed action: transmit</li> </ul>
3	AF2	<ul style="list-style-type: none"> <li>• or DSCP: af21</li> <li>• or DSCP: af22</li> <li>• or DSCP: af23</li> </ul>	<b>Policing:</b> <ul style="list-style-type: none"> <li>• Rate Limit: rate 8.0, burst 8.0, exceed 8.0.</li> <li>• Conform action: transmit</li> <li>• Exceed action: transmit</li> </ul>
4	AF1	<ul style="list-style-type: none"> <li>• or DSCP: af11</li> <li>• or DSCP: af12</li> <li>• or DSCP: af13</li> </ul>	<b>Policing:</b> <ul style="list-style-type: none"> <li>• Rate Limit: rate 8.0, burst 8.0, exceed 8.0.</li> <li>• Conform action: transmit</li> <li>• Exceed action: transmit</li> </ul>
5	BestEffort	Class Default	<b>Policing:</b> <ul style="list-style-type: none"> <li>• Rate Limit: rate 8.0, burst 8.0, exceed 8.0.</li> <li>• Conform action: transmit</li> <li>• Exceed action: transmit</li> </ul>

- a. Select **In Policies** in the TOC. The In Policies page appears.
- b. In the In Policies page, click **Create**. The In Policy wizard opens, displaying the In Policy Wizard - General page.

- c. In the In Policy Wizard - General page:
  - Enter **EF** in the Policy Name field.
  - Select the QoS Policy radio button.Click **Next**. The In Policy Wizard - Filter page appears.
- d. In the In Policy Wizard - Filter page:
  - Select **Create a new filter**.
  - Enter **EF** in the Filter name field.
- e. In the In Policy Wizard - Filter page, click **Create** to define a filter condition. The Rule Settings page appears. Create the filter as follows:
  - In the Rule Settings page, click **Edit** in the Service row of the Rule Setting table. The Service Editor dialog box opens.
  - In the Service Editor dialog box, select **46 (ef)**. Click **OK** to save the setting and return to the Rule Settings page.
  - In the Rule Setting page, click **Done**. The In Policy Wizard - Filter page appears.In the In Policy Wizard - Filter page, click **Next**. The In Policy Wizard - Marking page appears.
- f. Without making a selection in the Marking page, select **Policing** from the TOC. The In Policy Wizard - Policing page appears. Make these selections to define the policing policy:
  - Select **Enable Policing**.
  - Enter **8** in the Rate, Burst Size, and Exceed Burst fields.
  - Select **Transmit** in both the Conform Action and Exceed Action fields.
- g. Click **Finish**. The In Policy Wizard - Summary page appears, where you can view a summary of the policy.
- h. In the In Policy Wizard - Summary page, click **Finish** to save the policy. The In Policies page appears. Repeat the process to define the other policies.



- Step 7** Select **Deploy > Deployment** and follow the wizard to deploy the policy group. See [Lesson 2-6: Deploying the Data Network Tutorial Policies, page 2-64](#) and [Lesson 2-7: Monitoring the Deployment Process, page 2-66](#) for more detailed information on deploying policies and monitoring the deployment.
- Proceed with [Step 2: Setting Up an Historical Monitoring Task, page 4-11](#).
- 

### Related Topics

- [Understanding How to Monitor Traffic for Baseline Analysis, page 4-5](#)

## Step 2: Setting Up an Historical Monitoring Task

This step describes how to set up and run an historical monitoring task.

### Before You Begin

You must use QPM to deploy policies to an interface before you can use QPM to monitor the interface. The policies you deploy do not have to affect the traffic, they just have to filter the traffic. [Step 1: Filtering Traffic for Analysis, page 4-6](#), describes how to create QoS policies that do not affect traffic.

### Procedure

---

- Step 1** Select **Reports > Analysis**. The Historical Monitoring Tasks page appears. This page lists all the historical monitoring tasks that you have defined.
- Step 2** Click **Create**. The Monitoring Task Wizard starts at Step 1, Task Definition.
- Step 3** On the Monitoring Task Wizard - Task Definition page, fill in these fields to define the historical monitoring task:
- **Name**—A name you find meaningful.  
For this example, the name is **Baseline remote demo**.
  - **Polling Interval**—How often you want to collect data from the devices. The more frequent you poll the devices, the more effect the monitoring task might have on device performance. Also, the more frequent you poll the devices, the larger amount of data will be collected (thus filling up your disk space). See [How Much Disk Space Is Required for Historical Monitoring?, page 4-4](#) for a more detailed discussion of the implications of polling intervals.

For this example, the polling interval is 10 minutes.

- **Start and End Time**—The date and time you want the monitoring task to start and end. Click the calendar icon to choose dates from a calendar. The start time must use the 24-hour clock notation (that is, midnight is 00:00:00, noon is 12:00:00, 11 PM is 23:00:00, and so forth).

For this example, start time is 15 August 2002, 19:34:00 (7:34 PM), and end time is 15 September 2002, 19:34:00.

- **Enabled**—Check Enabled to identify that the task should be started at the selected start time. The task cannot run until you enable it.
- **Description**—Optionally, enter a description for the task.

When you are finished defining the task, click **Next**. The Monitoring Task Wizard - Select Devices page appears.

- Step 4** On the Monitoring Task Wizard - Select Devices page, select each device you want to include in this monitoring task by checking the box next to the device. Keep in mind that each monitoring task can have a maximum of 12 interfaces, so do not select more devices than you can use in this task.

When you are finished selecting devices, click **Next**. The Monitoring Task Wizard - Select Interfaces page appears.

- Step 5** On the Monitoring Task Wizard - Select Interfaces page, select the interfaces you want to include in the monitoring task. You can select a maximum of 12 interfaces.

When you are finished selecting interfaces, click **Next**. The Monitoring Task Wizard - Select Policies page appears.

- Step 6** On the Monitoring Task Wizard - Select Policies page, select the policies you want to include in the monitoring task. To select all policies, you can check the box in the table heading.

When you are finished selecting policies, click **Next**. The Monitoring Task Wizard - Summary page appears.

- Step 7** On the Monitoring Task Wizard - Summary page, review your task settings. If you want to make changes, click the links in the TOC to go to the page in the wizard that you want to change.

When you are satisfied with the task definition, click **Finish**. The task is saved and the Historical Monitoring Task page appears (Figure 4-1). Your task should be added to the list.

**Figure 4-1** Lesson 4-1, Step 2, Historical Monitoring Tasks Page After Defining Task

The screenshot displays the Cisco QoS Policy Manager interface. At the top, there are navigation tabs: Devices, Configure, Deploy, Reports, and Admin. Below these are sub-menus: IP Telephony, Upload, Analysis, Import Policy Groups, Conflicts, and Restore. The user ID is 'admin'. The main content area is titled 'Historical Monitoring Tasks' and shows a table of tasks. The table has columns for Name, Description, and Status. The 'MonDemoTask' is listed with a status of 'Finished'. The page also includes a 'Filter Source' dropdown, a 'Filter' button, and a 'Refresh Rate' dropdown.

Name	Description	Status
Baseline remote demo		Running
MonDemoTask	1 minute interval, 2 days, WAN Edge demo	Finished

If the status of your task is “Processing,” QPM is still analyzing your task. Select **Reports > Analysis** to refresh the page. When the status changes to “Running,” the task is ready to run at the start date and time. A task with a status of “Running” will not contain data until the start date and time has passed.

Proceed with [Step 3: Reading the Historical Monitoring Graphs, page 4-13](#).

### Related Topics

- [Understanding How to Monitor Traffic for Baseline Analysis, page 4-5](#)

## Step 3: Reading the Historical Monitoring Graphs

This step describes how to view an historical monitoring task, and how to read the graphs.

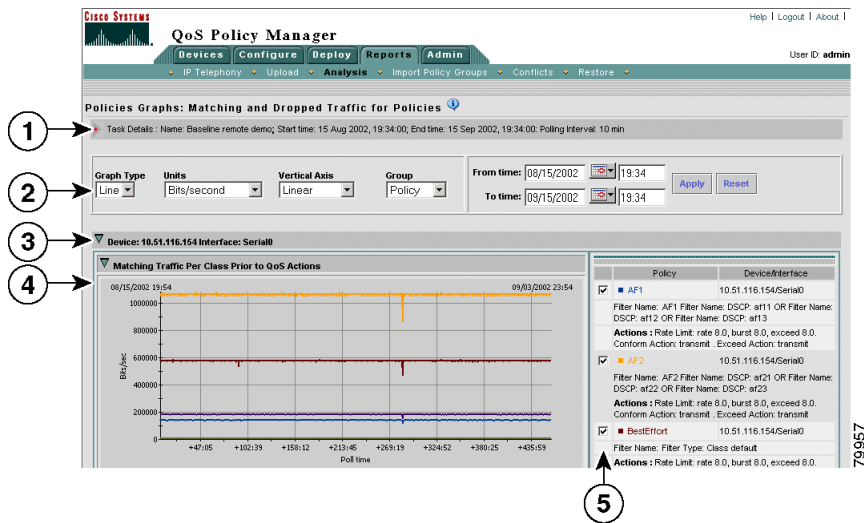
### Before You Begin

You can view any historical monitoring task, but a task will not have any data to display until the start date and time has been reached, QPM has polled the device three times, and at least one hour has passed. If you view a task before it is finished running, you can see the data that has been collected up to the latest polling period.

## Procedure

- Step 1** Select **Reports > Analysis**. The Historical Monitoring Tasks page appears. This page lists all the historical monitoring tasks that you have defined.
- Step 2** Select the task you want to view by checking the box next to the task. For this example, the task is **Baseline remote demo**.
- Step 3** Click **View Report**. The Policies Graphs page appears (Figure 4-2).

**Figure 4-2** Baseline Demo—Policies Graphs Page, Initial View



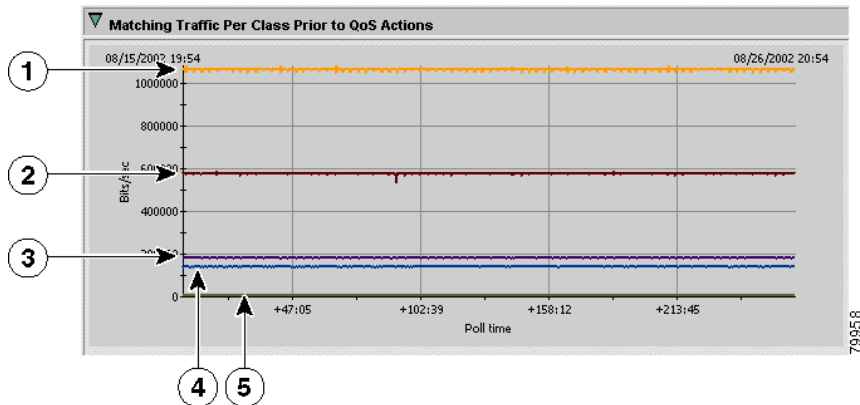
- 1** **Task details**—The historical monitoring task details, including name, duration, and polling interval. Use this information to help you understand the displayed data.

- 
- 2 Customization controls**—Fields that let you change how the data is displayed:
- **Graph Type**—Whether the graph is linear or bar. A linear graph displays all the collected data points, whereas a bar graph groups data points and displays averages for them (the time groupings are identified).
  - **Units**—The unit of measure for the graph, either bits per second or packets per second.
  - **Vertical Axis**—The scale used for the vertical axis: linear keeps the scale constant; logarithmic reduces the distance between numbers as the numbers get larger; and percentage shows the sale as the percentage of the available bandwidth. If you intend to create policies using bandwidth percentages, viewing the data in percentages can make it easier for you to develop your policies.
  - **Group**—Whether to group information on the graphs based on policies or interfaces (see number 3 below).
  - **From time and To time**—The start date and time and end date and time of the displayed data. By entering start and end times that are shorter than the start and end times of the collected data, you can zoom in on interesting traffic patterns to see more clearly what happened at that time. When you change the times, click **Apply** to change the graphs. Click **Reset** to change the times back to the original ones.
- 
- 3 Group folders**—Folders that you can open or close to see the graphs related to that item.
- If you select **Policy** for group in the customization controls, these folders are for interfaces. Each interface folder contains subfolders of matching traffic before applying QoS, matching traffic after applying QoS, and dropped traffic, based on each policy applied to the interface.
  - If you select **Interface** for Group in the customization controls, these folders are for policies. Each policy folder contains subfolders of matching traffic before applying QoS, matching traffic after applying QoS, and dropped traffic, based on each interface on which the policy is applied.
-

- |          |  |
|----------|--|
| <b>4</b> | <b>Graphs</b> —The collected data displayed according to your customization selections. You can open or close each graph by clicking the arrow to the left of the graph’s name. The colors used on the graphs are the colors used in the graphed items list (number 5 below).  |
| <b>5</b> | <b>Graphed items</b> —The items that can be displayed on the graphs (either policies or interfaces, depending on your selection in the Group customization control). In this example, the items graphed are policies. You can control which policies are graphed by checking or unchecking the associated box and clicking <b>Show Graphs</b> (not shown in this figure; the button is at the bottom of this group). If you have trouble seeing the data for an item (for example, because two lines occupy the same space), deselect the other items until you see the desired line. Switching between line and bar graphs can also help you identify overlapping data. |

Figure 4-3 shows the matching traffic per class prior to QoS actions graph from Figure 4-2.

**Figure 4-3** Baseline Demo—Matching Traffic Per Class Prior to QoS Actions Graph

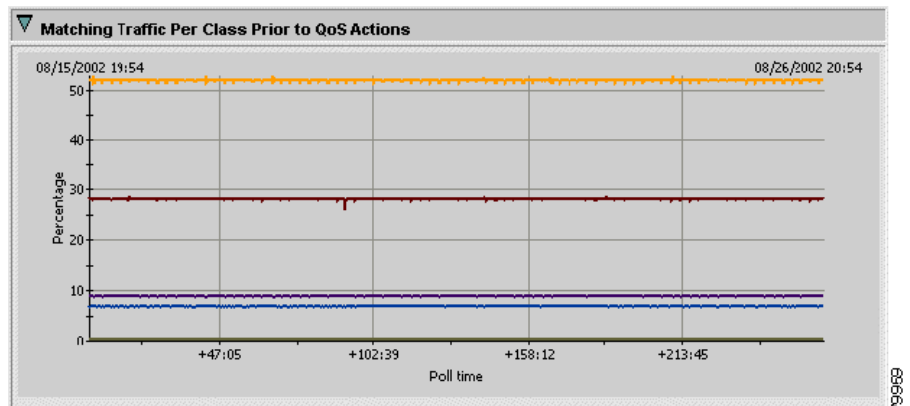


- |          |   |
|----------|---|
| <b>1</b> | Policy AF2. This policy matches DSCP af 21, af22, or af23.  |
| <b>2</b> | Policy BestEffort. This is the default class policy. Any traffic not matching the other policies matches this policy. |
| <b>3</b> | Policy EF. This policy matches DSCP ef.   |

4	Policy AF1. This policy matches DSCP af11, af12, or af13.
5	Policy AF3. This policy matches DSCP af31, af32, or af33.

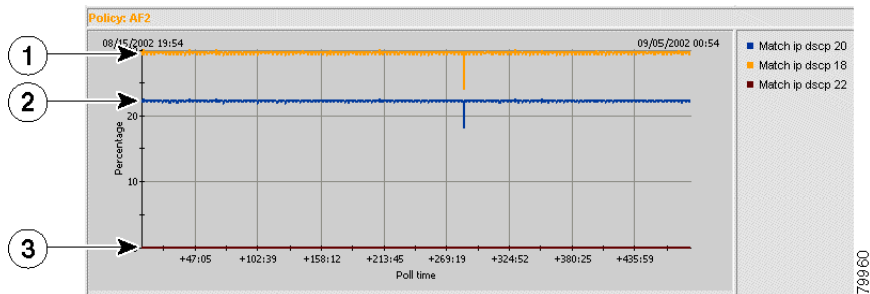
From the information in [Figure 4-3](#), you can see that traffic that matches the AF2 policy's filter consumes approximately 1050 Kbps of the interface's bandwidth. If you select **Percentage** from the Vertical Axis list box, you can see that this is approximately 52% of the interface's bandwidth ([Figure 4-4](#)). Policy AF3, on the other hand, accounts for almost no traffic.

**Figure 4-4** Baseline Demo—Matching Traffic Per Class Prior to QoS Actions Graph, Percentage Format



If a policy has more than one filter condition, like policy AF2 in this example, you can further analyze the traffic by looking at the filter graphs. The filter graphs show how much traffic matched each filter in a policy. To see the filter graphs, click the **Filters Graphs** button at the bottom of the page. [Figure 4-5](#) shows the filter graph for policy AF2. In this case, no traffic matched DSCP 22 (af23). DSCP 20 (af22) used approximately 22% of the bandwidth; DSCP 18 (af21) used approximately 30%.

Figure 4-5 Baseline Demo—Filter Graph for Policy AF2



1	Match IP DSCP 18 (af21)
2	Match IP DSCP 20 (af22)
3	Match IP DSCP 22 (af23)

The graphs also include ones that show the matching traffic after applying QoS, and the traffic that was dropped due to QoS action. However, because this is a baseline traffic analysis, the QoS policies do not affect traffic, so these graphs do not contain interesting information.

After you apply QoS policies that do affect traffic, you can monitor how the policies affect the traffic using the same techniques discussed in this section. Proceed with [Lesson 4-2: Monitoring QoS, page 4-18](#) for a detailed example of monitoring QoS.

### Related Topics

- [Understanding How to Monitor Traffic for Baseline Analysis, page 4-5](#)

## Lesson 4-2: Monitoring QoS

Monitoring QoS is similar to baseline monitoring, as described in [Lesson 4-1: Doing a Baseline Traffic Analysis, page 4-5](#). The only difference is that the QoS policies you are monitoring are designed to affect the traffic on the interfaces. Thus, you should see some evidence of your policies reducing the bandwidth used by some applications, with subsequent packet dropping for those applications.



### Before You Begin

This lesson assumes you have already created and deployed QoS policies to some devices using QPM. This lesson uses a specific interface and set of policies deployed on a Cisco test network. Replace the sample device and interface names with names from your network to create a monitoring task that can run on your network. These examples are meant to help you understand how to analyze the data QPM produces.

This example monitors 10.51.116.60 Serial 1/1, an HDLC 2048 Kbps interface on a Catalyst 3600, running IOS 12.2T. [Table 4-3](#) shows the policies deployed to the interface for outbound traffic. The policy group uses Class-based QoS scheduling. The policies have these purposes:

- **RealTime and VoiceControl**—These policies are meant for voice over IP traffic. Their purpose is to ensure low packet loss and delay.
- **Gold**—This policy is for high-priority data traffic. Its purpose is to provide fast response time.
- **Silver**—This policy is for secondary-priority traffic. Its purpose is to provide a bandwidth guarantee to ensure that the traffic is not starved for bandwidth, yet not allow the traffic to overwhelm gold or voice traffic.
- **BestEffort**—This policy is the default policy that applies to all traffic not covered by other policies. Its purpose is to ensure that the traffic is treated fairly, but the traffic is dropped if needed to ensure the service levels required by voice, gold, or silver traffic.

**Table 4-3 QoS Monitoring Demo Policies**

Policy Order	Policy Name	Filter	Action
1	RealTime	<ul style="list-style-type: none"> <li>• or <b>Protocol:</b> UDP and destination = Ports 16384 to 32767</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Priority:</b> LLQ enabled (a type of queuing)</li> <li>• <b>Bandwidth:</b> 33% (CBQ bandwidth allocation, a type of queuing)</li> </ul>
2	VoiceControl	<ul style="list-style-type: none"> <li>• or <b>Protocol:</b> TCP and destination = Ports 11000 to 11999</li> <li>• or <b>Protocol:</b> TCP and destination = Port 1720</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bandwidth:</b> 2%</li> </ul>

Table 4-3 QoS Monitoring Demo Policies (continued)

Policy Order	Policy Name	Filter	Action
3	Gold	<ul style="list-style-type: none"> <li>• or <b>Protocol:</b> TCP and destination = Ports 3300 to 3301</li> <li>• or <b>Protocol:</b> TCP and destination = Ports 1809</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bandwidth:</b> 25%</li> </ul>
4	Silver	<ul style="list-style-type: none"> <li>• or <b>Source NBAR application:</b> HTTP</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bandwidth:</b> 15%</li> </ul>
5	BestEffort	Class Default	<ul style="list-style-type: none"> <li>• <b>Fairness</b> (WFQ queuing enabled without specifying a number of queues)</li> </ul>

### Procedure

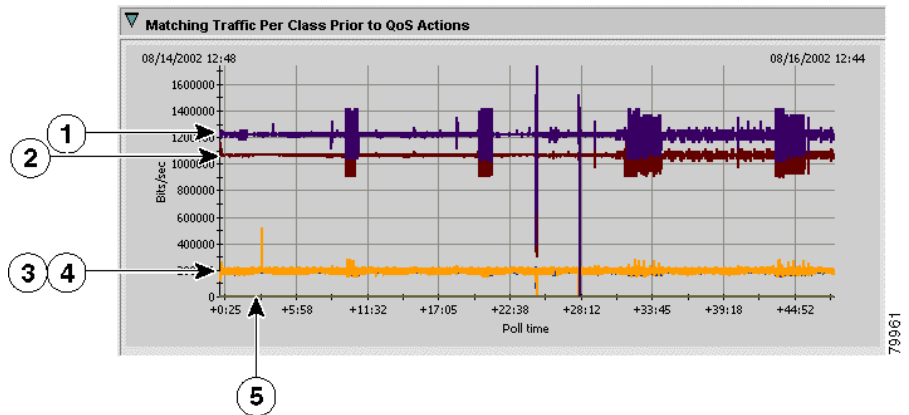
- 
- Step 1** Select **Reports > Analysis**, and click **Create**, to set up a new historical monitoring task. [Step 2: Setting Up an Historical Monitoring Task, page 4-11](#) explains in detail how to set up an historical monitoring task using this wizard. For this example, the historical monitoring task has these characteristics. The task you create will differ based on the devices and policies in your network:
- **Name**—MonDemoTask.
  - **Polling Interval**—1 minute.
  - **Start and End Time**—14 August 2002 12:45:00 to 16 August 2002 12:45:00 (2 day duration).
  - **Device and Interface**—10.51.116.60 Serial 1/1.
  - **Policies**—All policies described in [Table 4-3](#).
- Step 2** After the task has run long enough to poll the device at least 3 times (and at minimum one hour has passed), you can view the task and start analyzing the graphs. From the Historical Monitoring Tasks page (**Reports > Analysis**), check the box next to the task and click **View Report**. The Policies Graphs page appears and shows the graphs of the data collected by the task.

[Step 3: Reading the Historical Monitoring Graphs, page 4-13](#) explains some of the basics of reading these graphs. This discussion assumes you have already read that information.

Because this monitoring task is monitoring QoS policies that are intended to affect the network traffic on the interface, you should see a difference between the “Matching Traffic Per Class Prior to QoS Actions” (Figure 4-6) and the “Matching Traffic Per Class After QoS Actions” (Figure 4-7) graphs.

In this example, notice that traffic matching the BestEffort policy (number 1 in the figures) is approximately 1200 Kbps before QoS actions (roughly 60% of the interface’s bandwidth), but only 600 Kbps after QoS actions. If you open the “Matching Traffic Per Class Discarded by QoS Drop Actions” graph (Figure 4-8), you can see that roughly 600 Kbps of BestEffort traffic is being dropped. Also note that there is some Silver traffic dropping, but that no RealTime, VoiceControl, or Gold traffic is dropped. This is exactly the desired result for this set of policies.

**Figure 4-6** *MonDemoTask—Matching Traffic Per Class Prior to QoS Actions*



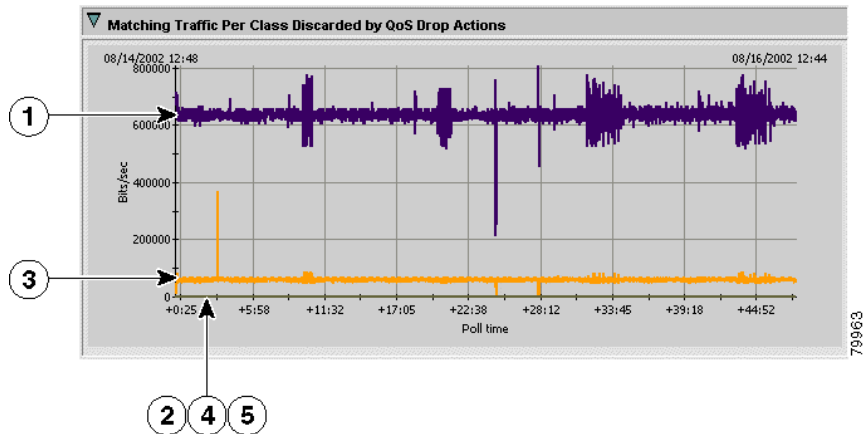
1	BestEffort
2	Gold
3	Silver
4	RealTime. The line for RealTime is behind the line for Silver.
5	VoiceControl. This line is just above the zero line.

Figure 4-7 MonDemoTask—Matching Traffic Per Class After QoS Actions



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl

**Figure 4-8** *MonDemoTask—Matching Traffic Per Class Discarded by QoS Drop Actions*



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl. Gold, VoiceControl, and RealTime overlap and are all 0 (no dropped traffic.)

**Step 3** Because linear graphs display all collected data points, the lines can be difficult to read if you are trying to analyze a portion of the data. To get a clearer view, you can zoom in on a specific time period.

For example, in [Figure 4-6](#), you can see some significant spikes approximately 25 hours into the task. To zoom in on the first spike, modify the From Time and To Time fields to approximate this period, and click **Apply**. In this case, change the From Time to 08/15/2002 13:20:00 and the To Time to 08/15/2002 13:50:00 ([Figure 4-9](#)).

Figure 4-9 Zooming In On Linear Graphs

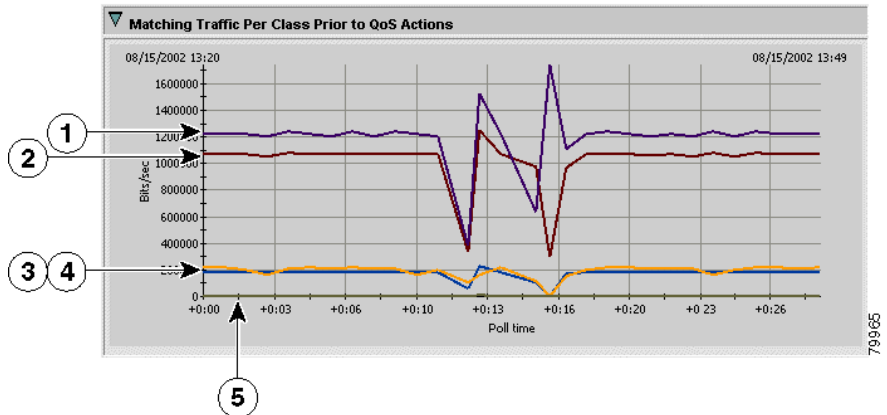
From time: 08/15/2002 13:20

To time: 08/15/2002 13:50

79964

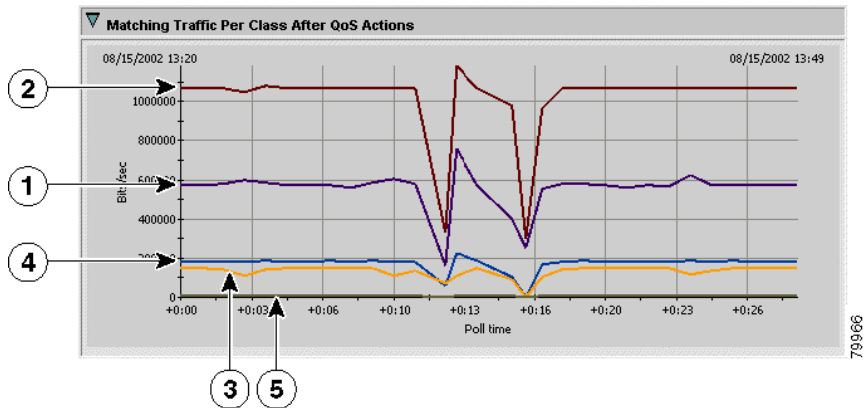
The resulting graphs show the network activity much more clearly for this time period.

Figure 4-10 MonDemoTask—Matching Traffic Per Class Prior to QoS Actions (After Zoom)



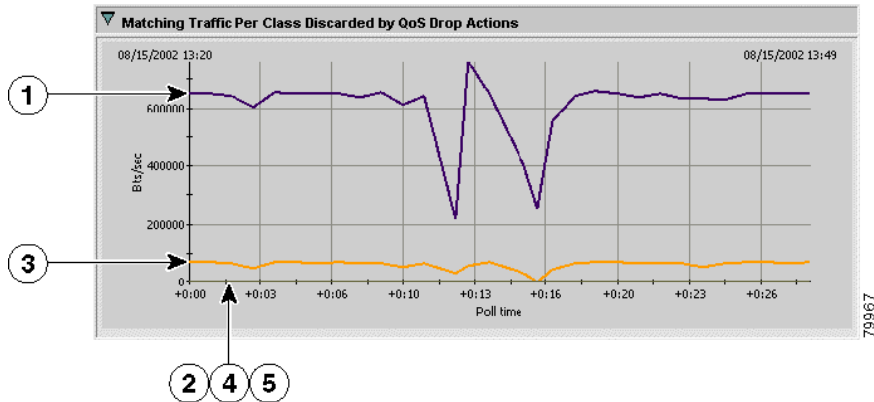
1	BestEffort
2	Gold
3	Silver
4	RealTime. The line for RealTime is mostly below the line for Silver. The lines occasionally cross.
5	VoiceControl. This line is just above the zero line.

**Figure 4-11** *MonDemoTask—Matching Traffic Per Class After QoS Actions (After Zoom)*



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl

**Figure 4-12** *MonDemoTask—Matching Traffic Per Class Discarded by QoS Drop Actions (After Zoom)*



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl. Gold, VoiceControl, and RealTime overlap and are all 0 (no dropped traffic.)

**Step 4** To get a simplified view of the network traffic, you can select Bar for **Graph Type** to see bar graphs.

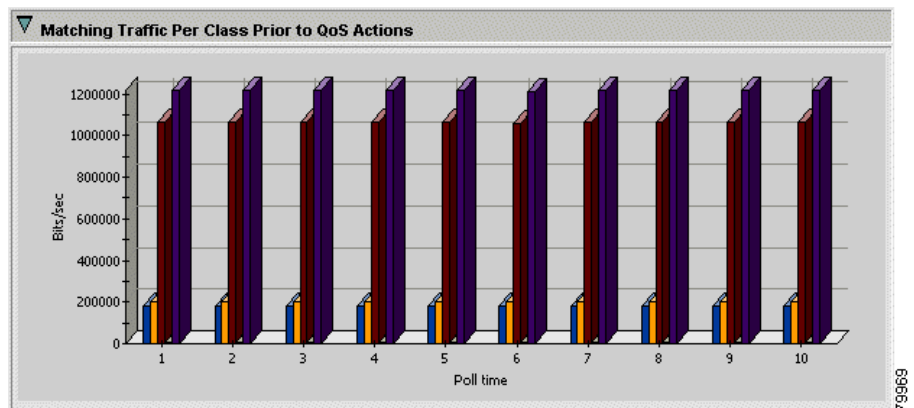
Unlike linear graphs, bar graphs do not show every data point collected. Instead, bar graphs show 10 data points, each one an average of the data collected over one tenth of the task's duration. The collection periods are shown in the lower right of the Policies Graphs page ([Figure 4-13](#)).



**Figure 4-13 Periods for Bar Graph Data Points**

Graphs X-axis Values	
Poll Time	Time From - Time To
1	08/14/2002 12:48--08/14/2002 17:36
2	08/14/2002 17:37--08/14/2002 22:23
3	08/14/2002 22:24--08/15/2002 03:10
4	08/15/2002 03:11--08/15/2002 07:58
5	08/15/2002 07:59--08/15/2002 12:47
6	08/15/2002 12:48--08/15/2002 17:36
7	08/15/2002 17:37--08/15/2002 22:25
8	08/15/2002 22:26--08/16/2002 03:13
9	08/16/2002 03:14--08/16/2002 08:00
10	08/16/2002 08:02--08/16/2002 12:44

Bar graphs can hide variations in traffic patterns. For example, the bar graph for “Matching Traffic Per Class Prior to QoS Actions” (Figure 4-14) does not show the spikes and lolls in traffic that appear on the linear version of the graph (Figure 4-6). On the other hand, bar graphs clearly show each traffic class, because bars cannot overlap like lines. These types of graphs can help you see broader traffic patterns, and can be useful for presentations.

**Figure 4-14 Bar Graph for Matching Traffic Per Class Prior to QoS Actions**

### Related Topics

- [Understanding QPM Monitoring, page 4-1](#)

## Lesson 4-3: Monitoring QoS in Real Time

This lesson describes how to set up and use a real-time monitoring task. Real-time monitoring is useful for troubleshooting an interface. If there seems to be a problem on an interface, you can monitor it to determine if there is a problem with the QoS policies. With real-time monitoring, you can only monitor one interface per task. However, you can start more than one task to view multiple interfaces.

### Before You Begin

You must use QPM to create QoS policies on an interface before you can use QPM to monitor the interface. Because you can only monitor real devices, this lesson uses devices on a Cisco test network as an example of how to set up and view a real-time monitoring task. When following this lesson, use devices and interfaces that reside on your own network. Only devices and interfaces you have defined in QPM are available for selection when you create a monitoring task.

### Procedure

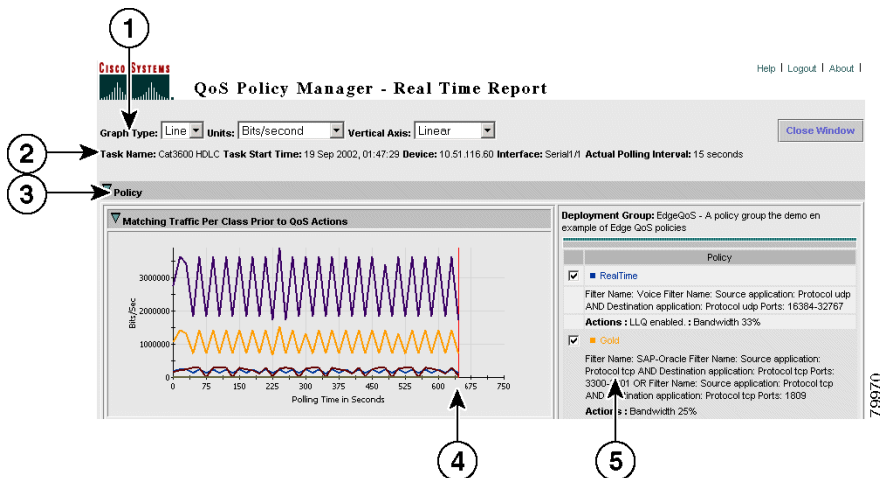
- 
- Step 1** Select **Reports > Analysis > Real-Time**. The Real-Time Monitoring Tasks page appears.
- Step 2** Click **Create**. The Real-Time Monitoring Wizard starts at the Device Selection page. Make these selections:
- **Name**—Enter a meaningful name for this task. For this example, the name is Cat3600 HDLC. The example will monitor the interface used in [Lesson 4-2: Monitoring QoS, page 4-18](#).
  - **Polling Interval**—Select how often you want QPM to collect information from the interface. The more often you poll the interface, the more effect monitoring can have on the interface's performance. For this example, the polling interval is 15 seconds.
  - **Device**—Select the device that has the interface you want to monitor. For this example, the device is 10.51.116.60.
  - **Description**—Optionally, enter a description for the task. You can rerun real-time monitoring tasks whenever you want, so a meaningful name and description can help you identify the task you want to rerun.

When finished, click **Next**. The Real-Time Monitoring Wizard - Interface Selection page appears.

- Step 3** On the Real-Time Monitoring Wizard - Interface Selection page, select the interface you want to monitor. For this example, the interface is Serial 1/1, an HDLC interface.
- Step 4** Click **Finish** to save your task definition. QPM opens a separate window and automatically starts the real-time monitoring task. You will not see any data until QPM has polled the interface three times. Then, data is posted to the real-time monitoring graphs as it is collected.

As data fills the graphs left to right, a vertical red line indicates which part of the data is the most recently gathered. When the graphical information reaches the right side of the graph, new data is overwritten on the graph left to right (Figure 4-15).

**Figure 4-15 Real-Time Demo—Real-Time Report Page, Initial View**



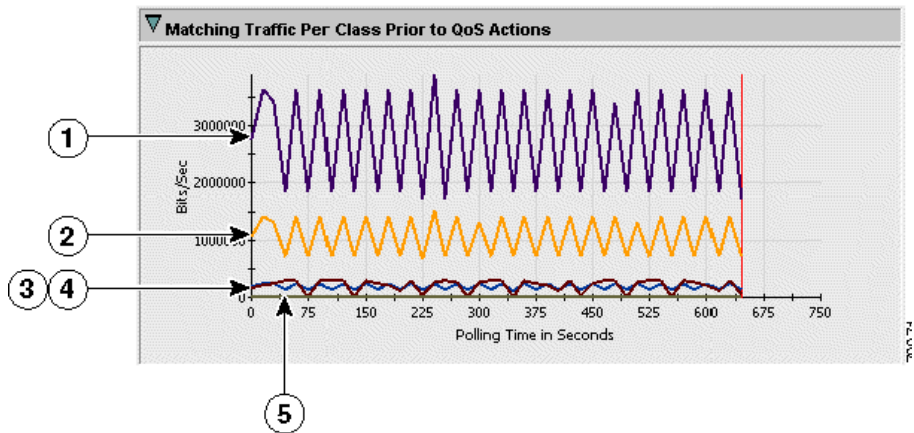
## 1 Customization controls—Fields that let you change how the data is displayed:

- **Graph Type**—Whether the graph is linear or bar. All data points are graphed, but fewer data points fit on the graph if you are using a bar graph. Thus, with bar graphs, data points will be overwritten more frequently than in linear graphs.
- **Units**—The unit of measure for the graph, either bits per second or packets per second.
- **Vertical Axis**—The scale used for the vertical axis: linear keeps the scale constant; logarithmic reduces the distance between numbers as the numbers get larger; and percentage shows the scale as the percentage of the available bandwidth.

2	<b>Task details</b> —The real-time monitoring task details, including name, start time, device, interface, and polling interval. Use this information to help you understand the displayed data.
3	<p><b>Group folders</b>—Folders that you can open or close to see the graphs related to that item. You can open or close each graph by clicking the arrow to the left of the graph's name. The colors used on the graphs are related to the colors used in the graphed items list.</p> <ul style="list-style-type: none"> <li>• <b>Policy</b>—Contains three graphs: matching traffic before applying QoS, matching traffic after applying QoS, and dropped traffic. These graphs are based on each policy applied to the interface.</li> <li>• <b>Filters</b>—Contains graphs for the filters for each policy. Each filter graph shows the matching traffic rate for each element of the filter.</li> <li>• <b>Actions</b>—Contains graphs for each policy, showing the results of the policy's actions on the traffic that met the policy's filter conditions.</li> </ul>
4	<b>Cursor</b> —This vertical line indicates the place where the most recent data point has been graphed. Data to the left of the line is most recent, data to the right of the line is old and is in the process of being overwritten.
5	<b>Graphed items</b> —The policies that can be displayed on the graphs. You can control which policies are graphed by checking or unchecking the associated box and clicking <b>Show Graphs</b> (not shown in this figure; the button is at the bottom of this group). If you have trouble seeing the data for an item (for example, because two lines occupy the same space), deselect the other items until you see the desired line. Switching between line and bar graphs can also help you identify overlapping data.

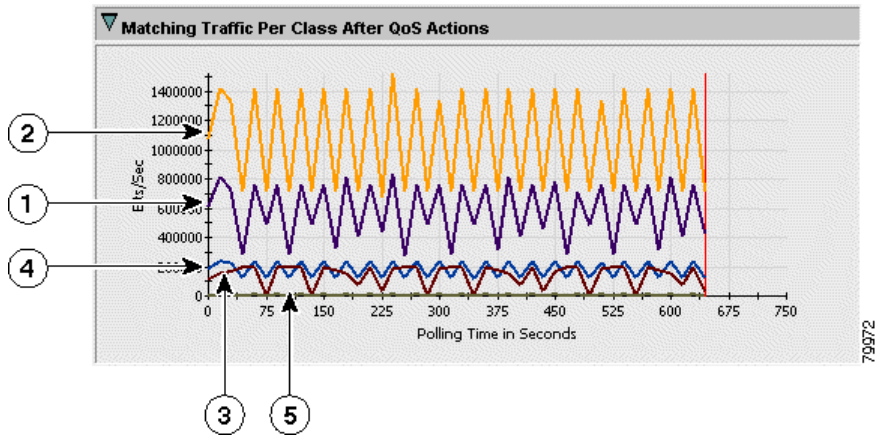
The following figures show examples of the real-time report for this interface. Because it is the same interface used in [Lesson 4-2: Monitoring QoS, page 4-18](#), you can compare these figures with the equivalent figures in that lesson.

**Figure 4-16** *Cat3600 HDLC Real-Time—Matching Traffic Per Class Prior to QoS Actions*



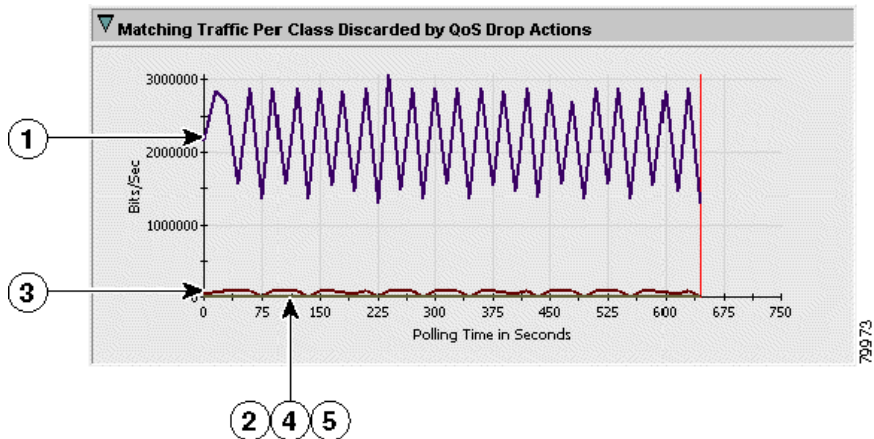
1	BestEffort
2	Gold
3	Silver
4	RealTime. The line for RealTime is mostly below the line for Silver. The lines occasionally cross.
5	VoiceControl. This line is just above the zero line.

**Figure 4-17 Cat3600 HDLC Real-Time—Matching Traffic Per Class After QoS Actions**



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl

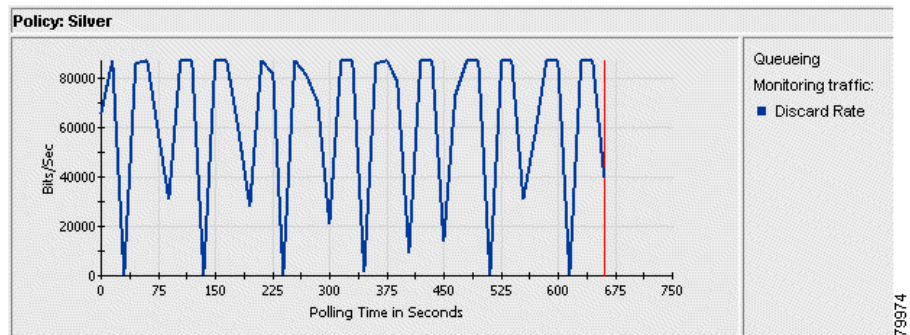
**Figure 4-18 Cat3600 HDLC Real-Time—Matching Traffic Per Class Discarded by QoS Drop Actions**



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl. Gold, VoiceControl, and RealTime overlap and are all 0 (no dropped traffic.)

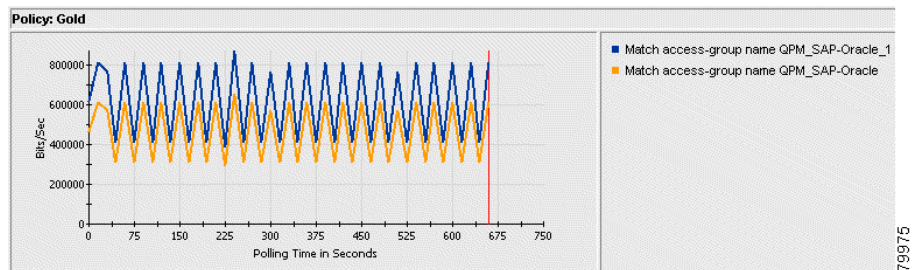
As you can see in [Figure 4-18](#), the discard rate for Silver traffic is close to zero. To get a clearer view of the discard rate, open the Action folder and look at the Silver policy ([Figure 4-19](#)).

**Figure 4-19 Cat3600 HDLC Real-Time—Action Graph for Silver Policy**



If you have a policy with multiple filter conditions, open the Filter folder and look at the graph for the policy. QPM shows you the matching traffic for each filter condition in this graph. In this example, the Gold policy has two conditions (Figure 4-20).

**Figure 4-20 Cat3600 HDLC Real-Time—Filter Graph for Gold Policy**



**Step 5** Click **Close Window** to close the Real-Time Report window and end the task.

### Tips

- You can rerun a real-time monitoring task by selecting **Reports > Analysis > Real-Time**, checking the box next to the desired task, and clicking **Run**.

### Related Topics

- [Understanding QPM Monitoring, page 4-1](#)