Getting Started Guide for CiscoWorks QoS Policy Manager 4.1
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.

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networking, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Getting Started Guide for CiscoWorks QoS Policy Manager 4.1
© 2008 Cisco Systems, Inc. All rights reserved.
Preface vii
Audience vii
Conventions vii
Product Documentation viii
Related Documentation ix
Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1
Introduction 1-1
Lesson 1-1: Getting Started with QPM 1-2
   Starting QPM 1-2
   Understanding the QPM User Interface 1-3
   Exiting QPM 1-5
Lesson 1-2: Importing the Tutorial Virtual Devices 1-6
Lesson 1-3: Creating the Tutorial Device Folder 1-7
Lesson 1-4: Creating the Tutorial Policy Group 1-8

CHAPTER 2
Data Network Tutorial 2-1
Understanding the Data Network Tutorial 2-1
   Understanding the Data Network Tutorial Example Network 2-2
   Understanding the Data Network Tutorial Devices 2-3
   Understanding the Data Network Tutorial Scenarios 2-4
   Using the QPM Policy Wizards 2-5
Lesson 2-1: Creating the Campus Access Cat6000 Port Policy 2-6
   Step 1: Defining the Campus Access Cat6000 Port Policy 2-6
   Step 2: Defining the Campus Access Cat6000 Port Policy QoS Properties 2-7
   Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy 2-9
   Step 4: Creating the ERP Traffic Coloring Traffic Rule 2-9
Lesson 2-2: Defining Policies and Traffic Rules To Color Campus Web Traffic 2-11
Lesson 2-2-1: Defining the Campus Access VLAN Policy 2-12
   Step 1: Defining the Campus Access VLAN Policy 2-13
   Step 2: Defining Elements to the Campus Access VLAN Policy 2-14
   Step 3: Creating the Web Traffic Coloring Traffic Rule 2-15
Lesson 2-2-2: Defining the Campus Access VLAN Ports Policy 2-18
   Step 1: Defining the Campus Access VLAN Ports Policy 2-18
Step 2: Defining the Campus Access VLAN Ports Policy QoS Properties 2-20
Step 3: Assigning Elements to the Campus Access VLAN Ports Policy 2-21

Lesson 2-3: Creating the Remote FastEthernet Policy 2-22
Step 1: Defining the Remote FastEthernet Policy 2-23
Step 2: Defining the Remote FastEthernet Policy QoS Properties 2-24
Step 3: Assigning Elements to the Remote FastEthernet Policy 2-25
Step 4: Creating the Web Traffic Coloring Traffic Rule 2-26
Step 5: Creating the ERP Traffic Coloring Policy 2-28

Lesson 2-4: Creating the WAN PPP Policy 2-30
Step 1: Defining the WAN PPP Policy 2-30
Step 2: Defining the WAN PPP Policy QoS Properties 2-32
Step 3: Assigning Elements to the WAN PPP Policy 2-33
Step 4: Creating the MQC CBWFQ Queuing Traffic Rules 2-34
Step 4a: Creating the ERP Traffic Queuing Traffic Rule 2-34
Step 4b: Creating the Web Traffic Queuing Traffic Rule 2-36
Step 4c: Creating the Class Default Traffic Rule 2-37

Lesson 2-5: Adding FTP Policing To the Campus Access VLAN Policy 2-39
Lesson 2-6: Deploying the Data Network Tutorial Policies 2-41
Lesson 2-7: Monitoring the Deployment Process 2-43

CHAPTER 3
IP Telephony Network Tutorial 3-1
Understanding the IP Telephony Network Example 3-2
Configuring QoS for the Campus Site 3-3
Configuring QoS for the WAN 3-3
Configuring QoS for the Remote Branch 3-4
Network Example Device Information 3-4
Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard 3-6
Using the IP Telephony Wizard 3-6
Step 1: Introduction 3-8
Step 2: Selecting Devices for QoS Configuration 3-9
Step 3: Selecting the IP Phone Connections 3-10
Step 4: Selecting the SoftPhone Connection 3-11
Step 5: Selecting the CallManager Port 3-12
Step 6: Selecting the IntraLAN Connections 3-14
Step 7: Selecting the Voice VLAN Connections 3-15
Step 8: Selecting the Switch to WAN Router Connection 3-16
Step 9: Selecting the Router WAN to Switch Connection 3-17
Step 10: Selecting the WAN Frame Relay Connections 3-19
Step 11: End 3-20
Lesson 3-2: Modifying the Voice Policies 3-20
Lesson 3-2-1: Enabling cRTP for the WAN-FR-Main-Interface Voice Policy 3-21
Lesson 3-2-2: Configuring the Gold Data Bandwidth for the WAN-FR-DLCI-Slow Voice Policy 3-24
Lesson 3-3: Deploying the IP Telephony QoS Policies 3-29
Lesson 3-4: Monitoring the Deployment Process 3-31

QoS Analysis Tutorial 4-1
Understanding QPM Monitoring 4-1
What is the Purpose of QoS Analysis? 4-1
What Can You Monitor Using QPM? 4-2
What Is the Difference Between Historical and Real-Time Monitoring? 4-2
How Much Disk Space Is Required for Historical Monitoring? 4-3
Lesson 4-1: Doing a Baseline Traffic Analysis 4-4
Understanding How to Monitor Traffic for Baseline Analysis 4-4
Step 1: Classifying Traffic for Analysis 4-5
Step 2: Setting Up an Historical Monitoring Task 4-9
Step 3: Reading the Historical Monitoring Graphs 4-10
Lesson 4-2: Monitoring QoS 4-12
Lesson 4-3: Monitoring QoS in Real Time 4-19
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 also know how to use the Windows 2000 operating system on your QPM server.

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords</td>
<td><strong>boldface</strong> font</td>
</tr>
<tr>
<td>Variables for which you supply values</td>
<td><em>italic</em> font</td>
</tr>
<tr>
<td>Displayed session and system information</td>
<td><strong>screen</strong> font</td>
</tr>
<tr>
<td>Information you enter</td>
<td><strong>boldface</strong> <strong>screen</strong> font</td>
</tr>
<tr>
<td>Variables you enter</td>
<td><em>italic</em>* screen** font</td>
</tr>
<tr>
<td>Menu items and button names</td>
<td><strong>boldface</strong> font</td>
</tr>
<tr>
<td>Selecting a menu item in paragraphs</td>
<td><strong>Option &gt; Network Preferences</strong></td>
</tr>
</tbody>
</table>

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.

Product Documentation

Note
We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

You can find product information, including documentation, at this URL on Cisco.com:

Table 1 describes the product documentation that is available.

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes for CiscoWorks QoS Policy Manager 4.1</td>
<td>• PDF on the product DVD.</td>
</tr>
<tr>
<td></td>
<td>prod_release_notes_list.html</td>
</tr>
<tr>
<td>Quick Start Guide for CiscoWorks QoS Policy Manager 4.1</td>
<td>• Printed document included with the product.</td>
</tr>
<tr>
<td></td>
<td>• PDF on the product DVD</td>
</tr>
<tr>
<td></td>
<td>prod_installation_guides_list.html</td>
</tr>
<tr>
<td>Installation Guide for QoS Policy Manager 4.1 on Solaris</td>
<td>• PDF on the product DVD.</td>
</tr>
<tr>
<td></td>
<td>prod_installation_guides_list.html</td>
</tr>
<tr>
<td>Installation Guide for QoS Policy Manager 4.1 on Windows</td>
<td>• PDF on the product DVD.</td>
</tr>
<tr>
<td></td>
<td>prod_installation_guides_list.html</td>
</tr>
<tr>
<td>Getting Started Guide for CiscoWorks QoS Policy Manager 4.1</td>
<td>• PDF on the product DVD and from the CiscoWorks QoS Policy Manager online help.</td>
</tr>
<tr>
<td></td>
<td>prod_installation_guides_list.html</td>
</tr>
</tbody>
</table>
Table 1  Product Documentation (continued)

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Guide for CiscoWorks QoS Policy Manager 4.1</td>
<td>• PDF on the product DVD and from the CiscoWorks QoS Policy Manager online help.</td>
</tr>
<tr>
<td></td>
<td>products_user_guide_list.html</td>
</tr>
<tr>
<td></td>
<td>products_device_support_tables_list.html</td>
</tr>
<tr>
<td>Context-sensitive Online Help</td>
<td>• Select an option from the navigation tree, then click Help.</td>
</tr>
<tr>
<td></td>
<td>• Click the Help button in the dialog box.</td>
</tr>
</tbody>
</table>

Related Documentation

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

QPM runs on the CiscoWorks Common Services Server. Documentation for CiscoWorks Common Services is available on Cisco.com at:


Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.
CHAPTER 1

Introduction

This tutorial introduces you to QoS Policy Manager (QPM) and provides examples of many of the tasks that you can perform with it. To make these examples easier to follow, you can follow 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, see to the QPM online help and User Guide for QoS Policy Manager.

The tutorial is structured as follows:

- **Chapter 1, “Introduction”** provides information about getting started with the product and the tutorial.
- **Chapter 3, “IP Telephony Network Tutorial”** allows you to practice configuring QoS for voice-over-IP (VoIP) networks.
- **Chapter 4, “QoS Analysis Tutorial”** helps you to understand how to use QPM monitoring to analyze the effect of your QoS policies on your network traffic.

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 1-6.

**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. Owing to this, they are unlikely to conflict with any real addresses already in your QPM inventory.
- To separate the tutorial policies from your existing policies, the tutorial instructs you to create a new policy group for the tutorial. For more information, see Lesson 1-4: Creating the Tutorial Policy Group, page 1-8.

**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.
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 1-6
- Lesson 1-3: Creating the Tutorial Device Folder, page 1-7
- Lesson 1-4: Creating the Tutorial Policy Group, page 1-8

Lesson 1-1: Getting Started with QPM

The following topics describe getting started with QPM:

- Starting QPM, page 1-2
- Understanding the QPM User Interface, page 1-2
- Exiting QPM, page 1-5

Starting QPM

QoS Policy Manager is accessed from the CiscoWorks desktop.

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

Step 2
Check the front page whether 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 3
Log into CiscoWorks with your user name and password. The CiscoWorks navigation tree appears in the left pane.

Step 4
Click QoS Policy Manager in the navigation tree. QPM opens in a separate browser window.

Related Topics

- Understanding the QPM User Interface, page 1-2
- Exiting QPM, page 1-5

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

<table>
<thead>
<tr>
<th>Number</th>
<th>Name of the Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Navigation Pane Tree</td>
<td>Displays hierarchical data in the form of an indented outline. In this outline, the nodes can be expanded (to display the next level in the hierarchy) or collapsed (hiding levels in the hierarchy).</td>
</tr>
</tbody>
</table>
| 2      | Navigation Pane Drawer      | Groups elements that are logically related. When a drawer is open, its content opens below it, as a tree. The following drawers are available in QPM:  
  - Getting Started—Displays basic information about the various features in QPM  
  - Devices—Contains options to manage devices and device groups in the QPM inventory. It also provides launch point to the Device Credentials Repository  
  - Provisioning—Contains options to define policy groups and policies and to configure QoS for IP telephony. It also allows you to work with global library policy components. This drawer also contains options to deploy QoS policies and to preview the CLI configuration on the devices.  
  - Monitoring—Contains options to monitor traffic on devices with QoS policies attached to them. You can perform Real-time, Historical, and Threshold analysis of the traffic  
  - Administration—Contains additional administration options. |
| 3      | Object Selector             | Allows you to select objects so that the corresponding information appears in the Content Area. Although this element is a part of the Content Area, it may not be present in all pages. |
| 4      | Content Area Title Bar      | Displays the title of the Content Area, based on the node you selected under a drawer |
| 5      | Content Area                | Displays information and controls or components, based on the node you selected under a drawer. This element frequently serves as a launch point for wizards, dialog boxes, message boxes, or other secondary windows. |
Now that you understand the QPM user interface, you are ready to learn how to exit QPM.

**Related Topics**
- Starting QPM, page 1-2
- Exiting QPM, page 1-5

## Exiting QPM

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

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

**Step 2** Click **Logout** in the CiscoWorks Desktop window.

The CiscoWorks session ends.

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

**Related Topics**
- Starting QPM, page 1-2
- Understanding the QPM User Interface, page 1-2
- Lesson 1-2: Importing the Tutorial Virtual Devices, page 1-6
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 2-1. For information about the devices used in the voice-over-IP network tutorial, see Understanding the IP Telephony Network Example, page 3-2.

Virtual devices are not physical devices, but 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.

**Step 1**
Copy the virtual devices file from the QPM server to a location on your client system.
The file is named TutorialDevices.xml. It is located at CSCOp\MDC\qpm\tutorial, in the CiscoWorks Common Services installation directory on the QPM server.

**Step 2**
In QPM, go to Devices > Device Management > Device Summary.
The Device Summary appears.

**Step 3**
Click Import Devices to QPM > From Virtual Devices File.
The Import Devices Wizard - General page appears.

**Step 4**
Do the following in the Import Devices Wizard - General page:

a. 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.

b. 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, check 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 that you can see the status of the import. The Discovery job that you just started is the last entry in the table.

Wait until the Discovery job is complete, as indicated by an entry in the Completed column.

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

a. Go to Devices > Device Management > Device Summary.

The Device Summary page appears.

You can find the imported devices under the Tutorial/Virtual Devices category in the object selector.

b. To view the network elements on a device, expand the node corresponding to the device name.

The interfaces of the device appear below the node, and you can click any interface to view its properties in the content area.

Now that you have imported the tutorial virtual devices, you are ready to create the tutorial device folder and policy group.

**Related Topics**
- Lesson 1-3: Creating the Tutorial Device Folder, page 1-7
- Lesson 1-4: Creating the Tutorial Policy Group, page 1-8

# 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.

**Step 1** Select Devices > Device Grouping > Device Folders.

The Device Folder 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.

**Step 4** Do the following in the object selector:

a. Select the tutorial virtual devices by checking 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
Lesson 1-4: Creating the Tutorial Policy Group

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

Step 1  Select Provisioning > Policy Management > Policy Groups.

The Policy Groups page appears.

Step 2  Do the following in the Policy Groups page:

   a.  Click Create.

      The Policy Group page appears.

   b.  Enter the name Tutorial in the Name field.

   c.  Enter the description of the Tutorial policy group in the Description field.

   d.  Click OK.

      The Policy Groups page appears.

Step 3  Verify that the Tutorial policy 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 1-6 and Lesson 1-4: Creating the Tutorial Policy Group, page 1-8.

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 2-1
- Lesson 2-1: Creating the Campus Access Cat6000 Port Policy, page 2-6
- Lesson 2-3: Creating the Remote FastEthernet Policy, page 2-20
- Lesson 2-4: Creating the WAN PPP Policy, page 2-28
- Lesson 2-5: Adding FTP Policing To the Campus Access VLAN Policy, page 2-38
- Lesson 2-6: Deploying the Data Network Tutorial Policies, page 2-40
- Lesson 2-7: Monitoring the Deployment Process, page 2-42

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 2-3
- Understanding the Data Network Tutorial Scenarios, page 2-4
- Using the QPM Policy Wizards, page 2-5
Understanding the Data Network Tutorial Example Network

The data network tutorial is based on an example enterprise data network that consists of the following sites:

- Campus Site, page 2-2
- Remote Site (Finance Users), page 2-2
- Remote Site (Sales Users), page 2-3

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**

### 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>
<thead>
<tr>
<th>Device Name</th>
<th>Device Model and IP Address</th>
<th>Software Version</th>
<th>Interfaces</th>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
</table>
| Core-7200-1 | 7204 10.1.1.1               | 12.2             | FastEthernet2/0  
FastEthernet 100,000 Kbit/sec (100 Mb/sec)  
FastEthernet3/0  
FastEthernet 100,000 Kbit/sec (100 Mb/sec)  
Serial4/0  
T1 line at 1544 Kbit/second (PPP)  
Serial4/1  
T1 line at 512 Kbit/second (PPP) | 10.1.1.1 | 255.255.255.0 |
| Core-3600-1 | 3620 10.3.1.1 | 12.2 | FastEthernet0/0  
FastEthernet 100,000 Kbit/sec (100 Mb/sec)  
Serial1/0  
T1 line at 1544 Kbit/second (PPP) | 10.3.1.1 | 255.255.255.0 |

10.2.2.1 | 255.255.255.0 |
10.2.3.1 | 255.255.255.0 |
Chapter 2      Data Network Tutorial

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, page 2-4
- **Scenario 2**—Coloring Campus Web Traffic, page 2-4
- **Scenario 3**—Coloring Remote Web and ERP Traffic, page 2-5
- **Scenario 4**—Queuing Web and ERP Traffic at WAN Edge, page 2-5
- **Scenario 5**—Policing FTP Traffic, page 2-5

### 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, page 2-6.

### 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 Policies and Traffic Rules To Color Campus Web Traffic, page 2-11.
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, page 2-20.

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, page 2-28.

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, page 2-38.

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, page 2-6

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

The Campus Access Cat6000 Port policy 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 are as follows.

- **Device Constraints:**
  - Catalyst 6000 Ethernet interfaces
  - CatOS 6.3
- **Network Element Assignments:** 3/1 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, page 2-6
- **Step 2:** Defining the Campus Access Cat6000 Port Policy QoS Properties, page 2-7
- **Step 3:** Assigning Elements to the Campus Access Cat6000 Port Policy, page 2-9
- **Step 4:** Creating the ERP Traffic Coloring Traffic Rule, page 2-9

Step 1: Defining the Campus Access Cat6000 Port Policy

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

- Name
- Description
- Constraints:
  - Catalyst 6000 Ethernet interfaces
  - CatOS 6.3

**Step 1**
Select **Provisioning > Policy Management > Manage Policies > Policy View.**
The Policy View page appears.

**Step 2** Select **Tutorial** from the Change Policy Group list box.

The page refreshes to display the policies in the Tutorial policy group. If you have not added any policies to the policy group, the list is empty.

**Step 3** Click **Custom Policy > New Policy**.

The Policy Definition wizard appears.

**Step 4** Do the following in the Policy Definition Wizard - General Definition page:

a. Enter **Campus Access Cat6000 Port** in the Policy Name field.

b. Enter **Colors inbound ERP traffic** in the Policy Description field.

c. Click **Next**.

The Policy Definition Wizard - Constraints Definition page appears.

**Step 5** Do the following in the Policy Definition Wizard - Constraints Definition page:

a. Click **Define Manually**.

   The Manual Constraint Definition area 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 list.

e. Select **Ethernet** from the Interface Type list.

f. Click **Add**.

   The Policy Definition Wizard - Constraints Definition page appears.

**Step 6** In the Policy Definition Wizard - Constraints Definition page, click **Capability Report**.

The QoS Capability Report dialog box appears, where you can view a summary of the QoS features that can be configured for the policy, according to the device constraints.

**Step 7** In the Policy Definition Wizard - Constraints Definition page, click **Next**.

The QoS Properties page appears.

You have completed creation of the Campus Access Cat6000 Port policy. Now you define its QoS properties. Continue with **Step 2: Defining the Campus Access Cat6000 Port Policy QoS Properties**, page 2-7.

---

**Related Topics**

- **Step 2: Defining the Campus Access Cat6000 Port Policy QoS Properties**, page 2-7

---

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

This step assumes that you have completed **Step 1: Defining the Campus Access Cat6000 Port Policy**, page 2-6.

In this step you assign the QoS Style=Port Based property to the policy. The policies are defined for individual switch ports and not for the VLAN, therefore the QoS style must be set to port-based.
Step 1 In the QoS Properties page, click **Edit**.
The QoS Properties Wizard - Congestion Management page appears.

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:
   a. Check the **Enable QoS Style** check box.
   b. Click the **Port based** radio button.
   c. Do not modify the other page fields.
   d. Click **Finish**.
The QoS Properties Wizard - Summary page appears, where you can view a summary of the QoS properties for the policy. **Figure 2-2** shows the QoS Properties Wizard - Summary page.

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

- Step 4 In the QoS Properties Wizard - Summary page, click **Finish**.
The QoS Properties page appears.
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, page 2-9.

**Related Topics**
- Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy, page 2-9
Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy

This step assumes that you have completed Step 2: Defining the Campus Access Cat6000 Port Policy QoS Properties, page 2-7.

In this step you assign the network element 3/1 on switch Access-Cat6000-2 to the policy.

**Step 1** Select Network Assignment in the Table of Contents.
The Network Assignment page appears.

**Step 2** In the Network Assignment page, click Add.
The Add Assignment dialog box opens.

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

a. Select the network element 3/1 on switch Access-Cat6000-2 by clicking the check box next to it.
b. Click Assign.
The dialog box closes. The selected network element appears in the Network Assignment page.

You have completed assigning elements to the Campus Access Cat6000 Port policy. Now you create the ERP Traffic Coloring policy. Continue with Step 4: Creating the ERP Traffic Coloring Traffic Rule, page 2-9.

Related Topics
- Step 4: Creating the ERP Traffic Coloring Traffic Rule, page 2-9

Step 4: Creating the ERP Traffic Coloring Traffic Rule

This step assumes that you have completed Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy, page 2-9.

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

**Step 1** Select Traffic Rules in the Table of Contents.
The Traffic Rules page appears.

**Step 2** Click Create > In Traffic Rules.
The In Traffic Rules wizard opens, displaying the In Traffic Rules Wizard - General page.

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

a. Enter **Color ERP traffic** in the Traffic Rule Name field.

b. Enter **Colors inbound ERP traffic** in the Enter Description for the Traffic Rule field.

   The QoS Policy check box is automatically selected.

c. Click **Next**.

   The In Traffic Rules Wizard - Traffic Classification page appears.

**Step 4**  
Do the following in the In Traffic Rules Wizard - Traffic Classification page:

a. Enter **ERP traffic** in the Traffic Classifier name field.

b. Click **Create** to define a traffic classifier condition.

   The Traffic Rule Settings page appears.

**Step 5**  
In the Traffic Rule Settings page, click **Edit** in the Protocol row of the Rule Setting table.

The Protocol Editor page opens.

**Step 6**  
Do the following in the Protocol Editor page:

a. Select the From Library radio button.

b. Select **TCP** from the Source list box.

c. Click **OK**.


**Step 7**  
In the Rule Settings page, click **Edit** in the Source IP row of the Traffic Rule Setting table.

The Source IP Editor page opens.

**Step 8**  
Do the following in the Source IP Editor page:

a. Click the IP Address / Host name list radio button, and ensure the IP radio button is clicked.

b. Enter 10.1.2.3 (the IP address of the ERP server) in the IP/Host field.

   Leave the Mask field empty. If you specify a mask, QPM interprets the IP address as a subnet, and the traffic classifier rule applies to all hosts on the specified subnet. If you only specify an IP address, only the host with that IP address matches the traffic classifier rule.

c. Click **Add**.

   The address is added to the Add a new value list.

d. Click **OK**.

   The Source IP Editor page closes and the Traffic Rule Setting page refreshes.

**Step 9**  
In the Traffic Rule Setting page, click **Done**.

The In Traffic Rules Wizard - Traffic Classification page appears.

**Step 10**  
In the In Traffic Rules Wizard - Traffic Classification page, click **Next**.

The In Traffic Rules Wizard - Marking page appears.

**Step 11**  
Do the following in the In Traffic Rules Wizard - Marking page:

a. Click the Value radio button.

b. Select 32 (cs4) from the Value list box.

   The Enable Marking check box is automatically checked.
c. Click Finish.

The In Traffic Rules Wizard - Summary page appears, where you can view a summary of the traffic rule. Figure 2-4 shows the summary page.

Figure 2-4 Lesson 2-1—Color ERP Traffic Rule Summary Page

<table>
<thead>
<tr>
<th>Step 12</th>
<th>In the In Traffic Rules Wizard - Summary page, click Finish. The In Traffic Rules page appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 13</td>
<td>Click Finish. The Policy View page appears. Now that you have completed creating the Campus Access Cat6000 Port policy to color ERP traffic that originates from the Campus application server, you can proceed with the next lesson, Lesson 2-2: Defining Policies and Traffic Rules To Color Campus Web Traffic, page 2-11.</td>
</tr>
</tbody>
</table>

Related Topics
- Lesson 2-1: Creating the Campus Access Cat6000 Port Policy, page 2-6

Lesson 2-2: Defining Policies and Traffic Rules 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 policies. The first policy is assigned to the VLAN network element, and contains the QoS policies. The second policy 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, page 2-12
- Lesson 2-2-2: Defining the Campus Access VLAN Ports Policy, page 2-16

**Lesson 2-2-1: Defining the Campus Access VLAN Policy**

The Campus Access VLAN policy, in combination with the Campus Access VLAN Ports policy, colors web traffic that originates from the Campus web server. This is to enable the devices between this server and the Sales and Finance so that 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 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. Each step assumes that you have just completed the previous step:

- **Step 1: Defining the Campus Access VLAN Policy, page 2-12**
- **Step 2: Assigning Elements to the Campus Access VLAN Policy, page 2-14**
- **Step 3: Creating the Web Traffic Coloring Traffic Rule, page 2-15**

**Step 1: Defining the Campus Access VLAN Policy**

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

- **Name**
- **Description**
- **Device constraints:**
  - Catalyst 6000 VLAN interfaces
  - CatOS 6.3
Step 1  Select **Provisioning > Policy Management > Manage Policies > Policy View**.

The Policy View page appears.

Step 2  Select **Tutorial** from the Change Policy Group list box.

The page refreshes to display the policies in the Tutorial policy group. If you have not added any policies to the policy group, the list is empty.

Step 3  Click **Custom Policy > New Policy**.

The Policy Definition wizard appears.

Step 4  Do the following in the Policy Definition Wizard - General Definition page:

a. Enter **Campus Access VLAN** in the Policy Name field.

b. Enter **Colors outbound web traffic** in the Policy Description field.

Do not modify the other page fields.

c. Click **Next**. The Policy Definition Wizard - Constraints Definition page appears.

Step 5  Do the following in the Policy Definition Wizard - Constraints Definition page:

a. Click **Define Manually**.

The Manual Constraint Definition area 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 **Add**.

The Policy Definition Wizard - Constraints Definition page appears. **Figure 2-5** shows the completed Policy Definition Wizard - Constraints Definition page.

---

**Figure 2-5**  *Lesson 2-2-1—Campus Access VLAN Policy Constraints Definition Page*

---

Step 6  In the Policy Definition Wizard - Constraints Definition page, click **Capability Report**.
The QoS Capability Report dialog box opens, where you can view a summary of the QoS features that can be configured for the policy, according to the device constraints.

**Step 7**
In the Policy Definition Wizard - Constraints Definition page, click **Next**.

The QoS Properties page appears.

This policy uses the default QoS properties, so you need not edit them.

You have completed creation of the Campus Access VLAN Policy. Now you can assign network elements to it. Continue with **Step 2: Assigning Elements to the Campus Access VLAN Policy**, page 2-14.

---

**Related Topics**
- **Step 2: Assigning Elements to the Campus Access VLAN Policy**, page 2-14

---

**Step 2: Assigning Elements to the Campus Access VLAN Policy**

This step assumes that you have completed **Step 1: Defining the Campus Access VLAN Policy**, page 2-12.

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

**Step 1**
Select **Network Assignment** in the Table of Contents.

The Network Assignment page appears.

**Step 2**
Click **Add**.

The Add Assignment dialog box opens.

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

a. Select the network element VLAN0020 on device Access-Cat6000-1 by checking the check box next to it.

b. Click **Assign**.

The dialog box closes. The selected network element appears in the Network Assignment page. **Figure 2-6** shows the completed Network Assignment page.

**Figure 2-6**  **Lesson 2-2-1—Campus Access VLAN Policy Network Assignment Page**

You have completed assigning elements to the Campus Access VLAN Policy Group.

You can now create the Web Traffic Coloring traffic rule. Continue with **Step 3: Creating the Web Traffic Coloring Traffic Rule**, page 2-15.
Related Topics

- Step 3: Creating the Web Traffic Coloring Traffic Rule, page 2-15

### Step 3: Creating the Web Traffic Coloring Traffic Rule

This step assumes that you have completed Step 2: Assigning Elements to the Campus Access VLAN Policy, page 2-14.

In this step you create the web traffic coloring traffic rule, which colors inbound web traffic to DSCP value 16.

**Step 1**

Select Traffic Rules in the Table of Contents.

The Traffic Rules page appears.

**Step 2**

Click Create > In Traffic Rules.

The In Traffic Rules wizard opens, displaying the In Traffic Rules Wizard - General page.

**Step 3**

Do the following In the In Traffic Rules Wizard - General page:

a. Enter *Color web traffic* in the Traffic Rule Name field.

b. Enter *Colors web traffic* in the Description field.

c. The QoS Policy check box is automatically selected.

d. Click Next.

The In Traffic Rules Wizard - Traffic Classification page appears.

The New Traffic Classifier check box is automatically selected

**Step 4**

Do the following in the In Traffic Rules Wizard - Traffic Classification page.

a. Enter *Web Traffic* in the Traffic Classifier Name field.

b. Click Create.

The Traffic Rule Setting page appears.

**Step 5**

In the Traffic Rule Settings page, click Edit in the Protocol table row.

The Protocol Editor page opens.

**Step 6**

Do the following in the Protocol Editor dialog box:

a. Click the From Library radio button.

b. Select www-TCP from the Source list box.

c. Click OK.

The Protocol Editor page closes. The Traffic Rule Setting page updates in the main QPM window.

**Step 7**

In the Traffic Rule Setting page, click Done.

The In Traffic Rules Wizard - Traffic Classification page appears.

**Step 8**

In the In Traffic Rules Wizard - Traffic Classification page, click Next.

The In Traffic Rules Wizard - Marking page appears.

**Step 9**

Do the following in the In Traffic Rules Wizard - Marking page:

a. Click the Value radio button.

b. Select 16 (cs2) from the Value list box.
The Enable Marking check box is automatically selected.

c. **Click Finish.**

The In Traffic Rules Wizard - Summary page appears, where you can view a summary of the policy. **Figure 2-7** shows the completed In Traffic Rules Wizard - Summary page.

**Figure 2-7  Lesson 2-2-1—Web Traffic Coloring Policy In Traffic Rules Wizard - Summary Page**

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Click <strong>Finish.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Traffic Rules page appears.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Click <strong>Finish.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Policy View page appears.</td>
</tr>
</tbody>
</table>

Now that you have completed creating the Campus Access VLAN policy 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, page 2-16.**

---

**Related Topics**
- **Lesson 2-2-2: Defining the Campus Access VLAN Ports Policy, page 2-16**

**Lesson 2-2-2: Defining the Campus Access VLAN Ports Policy**

The Campus Access VLAN Ports policy, in combination with the Campus Access VLAN policy, 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.
Chapter 2      Data Network Tutorial

Lesson 2-2: Defining Policies and Traffic Rules To Color Campus Web Traffic

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

The details of the Campus Access VLAN policy 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. Each step assumes that you have just completed the previous step:

- **Step 1:** Defining the Campus Access VLAN Ports Policy, page 2-17
- **Step 2:** Defining the Campus Access VLAN Ports Policy QoS Properties, page 2-18
- **Step 3:** Assigning Elements to the Campus Access VLAN Ports Policy, page 2-19

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

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

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

---

**Step 1**
Select **Provisioning > Policy Management > Manage Policies > Policy View**.

The Policy View page appears.

**Step 2**
Select **Tutorial** from the Change Policy Group list box.

The page refreshes to display the policies in the Tutorial policy group. If you have not added any policies to the policy group, the list is empty.

**Step 3**
Click **Custom Policy > New Policy**.

The Policy Definition wizard appears.

**Step 4**
Do the following in the Policy Definition Wizard - General Definition page:

a. Enter **Campus Access VLAN Ports** in the Policy Name field.

b. Enter **Applies VLAN Based QoS Style** in the Policy Description field.

c. Click Next.

The Policy Definition Wizard - Constraints Definition page appears.

**Step 5**
Do the following in the Policy Definition Wizard - Constraints Definition page:

a. Click **Define Manually**.

The Manual Constraint Definition area 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 list.
e. Select Ethernet from the Interface Type list.
f. Click Add.

The Policy Definition Wizard - Constraints Definition page appears. Figure 2-8 shows the completed Policy Definition Wizard - Constraints Definition page.

**Figure 2-8** Lesson 2-2-2—Campus Access VLAN Ports Policy Definition Wizard - Constraints Definition Page

---

### Step 6

In the Policy Definition Wizard - Constraints Definition page, click **Capability Report**.

The QoS Capability Report page appears, where you can view a summary of the QoS features that can be configured for the policy, according to the device constraints.

### Step 7

In the Policy Definition Wizard - Constraints Definition page, click **Next**.

The QoS Properties page appears.


---

### Related Topics
- **Step 2: Defining the Campus Access VLAN Ports Policy QoS Properties**, page 2-18

---

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

This step assumes that you have completed **Step 1: Defining the Campus Access VLAN Ports Policy**, page 2-17.

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

#### Step 1

In the QoS Properties page, click **Edit**.

The QoS Properties Wizard - Congestion Management page appears.

#### 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:

a. Check the **Enable QoS Style** check box.

b. Click the **VLAN based** radio button.
Do not modify the other page fields.

c. Click Next.

The QoS Properties Wizard - Summary page appears. Figure 2-9 shows the QoS Properties Wizard - Summary page.

Figure 2-9  Lesson 2-2-2—Campus Access VLAN Ports Policy QoS Properties Wizard - Summary Page

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

The QoS Properties page appears.

You have completed defining the QoS properties of the Campus Access VLAN Ports policy. Now you assign network elements to it. Continue with Step 3: Assigning Elements to the Campus Access VLAN Ports Policy, page 2-19.

Related Topics
- Step 3: Assigning Elements to the Campus Access VLAN Ports Policy, page 2-19

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

This step assumes that you have completed Step 2: Defining the Campus Access VLAN Ports Policy QoS Properties, page 2-18.

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

Step 1  Select Network Assignment in the Table of Contents.

The Network Assignment page appears.

Step 2  In the Network Assignment page, click Add.
The Add Assignment dialog box opens.

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

a. Select the network element 2/2 on device Access-Cat6000-1 by checking the check box next to it.  
b. Click **Assign**.

The dialog box closes.

The selected network element appears in the Network Assignment page. Figure 2-10 shows the completed Network Assignment page.

![Figure 2-10](Lesson 2-2-2—Campus Access VLAN Ports Policy Assigned Network Elements Page)

**Step 4** Click **Finish**.

The Policy View page appears.

Now that you have completed defining policy and QoS Properties to color campus web traffic, you can proceed with the next lesson, **Lesson 2-3: Creating the Remote FastEthernet Policy**, page 2-20.

---

**Related Topics**

- Lesson 2-3: Creating the Remote FastEthernet Policy, page 2-20

---

**Lesson 2-3: Creating the Remote FastEthernet Policy**

The Remote FastEthernet policy 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 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 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
Chapter 2      Data Network Tutorial
Lesson 2-3: Creating the Remote FastEthernet Policy

Step 1: Defining the Remote FastEthernet Policy

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

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

Step 1  Select Provisioning > Policy Management > Manage Policies > Policy View.
The Policy View page appears.

Step 2  Select Tutorial from the Change Policy Group list box.
The page refreshes to display the policies in the Tutorial policy group. If you have not added any policies to the policy group, the list is empty.

Step 3  Click Custom Policy > New Policy.
The Policy Definition wizard appears.

Step 4  Do the following in the Policy Definition Wizard - General Definition page:
  a. Enter Remote FastEthernet in the Policy Name field.
  b. Enter Colors web and ERP traffic from remote sites in the Policy Description field.
  c. Click Next.
     The Policy Definition Wizard - Constraints Definition page appears.

Step 5  Do the following in the Policy Definition Wizard - Constraints Definition page:
  a. Click Define Manually.
The Manual Constraint Definition area appears.

b. Select **2600** from the Model list.

c. Select **12.2** from the OS list.

d. Select **Interface** from the Network Element list.

e. Select **Ethernet** from the Interface Type list.

f. Click **Add**.

The Policy Definition Wizard - Constraints Definition page appears.

**Step 6**

Do the following in the Policy Definition Wizard - Constraints Definition page:

a. Click **Define Manually**.

The Manual Constraint Definition area appears.

b. Select **3600** from the Model list.

c. Select **12.2** from the OS list.

Interface is automatically entered in the Network Element field.

d. Select **Ethernet** from the Interface Type list.

e. Click **Add**.

The Policy Definition Wizard - Constraints Definition page appears. Figure 2-11 shows the completed Policy Definition Wizard - Constraints Definition page.

**Figure 2-11** Lesson 2-3—Remote FastEthernet Policy Definition Wizard - Constraints Definition Page

<table>
<thead>
<tr>
<th>Constraint No.</th>
<th>Model</th>
<th>OS Version</th>
<th>Compatible OS</th>
<th>Interface Type</th>
<th>Card Type</th>
<th>Network Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3600</td>
<td>12.2</td>
<td>12.2, 12.2T, 12.3, 12.3T, 12.4, 12.4T</td>
<td>Ethernet</td>
<td>NA</td>
<td>Interface</td>
</tr>
<tr>
<td>2</td>
<td>3600</td>
<td>12.2</td>
<td>12.2, 12.2T, 12.3, 12.3T, 12.4, 12.4T</td>
<td>Ethernet</td>
<td>NA</td>
<td>Interface</td>
</tr>
</tbody>
</table>

**Step 7**

In the Policy Definition Wizard - Constraints Definition page, click **Capability Report**.

The QoS Capability Report page appears, where you can view a summary of the QoS features that can be configured for the policy, according to the device constraints.

**Step 8**

In the Policy Definition Wizard - Constraints Definition page, click **Next**.

The QoS Properties page appears.


**Related Topics**

- **Step 2: Defining the Remote FastEthernet Policy QoS Properties, page 2-23**
Step 2: Defining the Remote FastEthernet Policy QoS Properties

This step assumes that you have completed Step 1: Defining the Remote FastEthernet Policy, page 2-21. In this step you define the Class-based QoS property to the policy.

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

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 2-12 shows the QoS Properties Wizard - Summary page.

   ![Image](image.png)

   **Figure 2-12 Lesson 2-3—Remote FastEthernet Policy QoS Properties Wizard - Summary Page**

   - Step 5 of 5 -

Step 3 In the QoS Properties Wizard - Summary page, click Finish.
The QoS Properties page appears.
You have defined the QoS properties of the Remote FastEthernet policy. Now you assign network elements to it. Continue with Step 3: Assigning Elements to the Campus Access Cat6000 Port Policy, page 2-9.

Related Topics
- Step 3: Assigning Elements to the Remote FastEthernet Policy, page 2-24
Step 3: Assigning Elements to the Remote FastEthernet Policy

This step assumes that you have completed Step 2: Defining the Remote FastEthernet Policy QoS Properties, page 2-23.

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

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

---

Step 1
Select **Network Assignment** in the Table of Contents.
The Network Assignment page appears.

Step 2
In the Network Assignment page, click **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 checking 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 Network Assignment page.


---

Related Topics

- Step 4: Creating the Web Traffic Coloring Traffic Rule, page 2-24

Step 4: Creating the Web Traffic Coloring Traffic Rule

This step assumes that you have completed Step 3: Assigning Elements to the Remote FastEthernet Policy, page 2-24.

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

---

Step 1
Select **Traffic Rules** in the Table of Contents.
The Traffic Rules page appears.

Step 2
Click **Create > In Traffic Rules**.
The In Traffic Rules wizard opens, displaying the In Traffic Rules Wizard - General page.

Step 3
Do the following In the In Traffic Rules Wizard - General page:

a. Enter **Web Traffic Coloring** in the Traffic Rule 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 Traffic Rules Wizard - Traffic Classification page appears.

**Step 4**
Do the following in the In Traffic Rules Wizard - Traffic Classification page:

a. Leave the Create a new Traffic Classifier radio button selected.

b. Enter **Web traffic** in the Traffic Classifier name field.

c. Click **Create** to define a traffic classifier rule.

   The Traffic Rule Settings page appears.

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

**Step 6**
Do the following in the Protocol Editor page:

a. Click the **From Library** radio button.

b. Select **www-TCP** from the Source list box.

c. Click **OK**.

   The Protocol Editor page closes. The Traffic Rule Setting page updates in the main QPM window.

**Step 7**
In the Traffic Rule Setting page, click **Done**. You should scroll to the bottom of the page to do this.

   The In Traffic Rules Wizard - Traffic Classification page appears.

**Step 8**
In the In Traffic Rules Wizard - Traffic Classification page, click **Next**.

   The In Traffic Rules Wizard - Marking page appears.

**Step 9**
Do the following in the In Traffic Rules Wizard - Marking page:

a. Select **16 (cs2)** from the Value list box.

   The Enable Marking check box is automatically selected.

b. Click **Finish**.
The In Traffic Rules Wizard - Summary page appears, where you can view a summary of the policy. Figure 2-13 shows the completed In Traffic Rules Wizard - Summary page.

Figure 2-13  Lesson 2-3—Remote FastEthernet Policy In Traffic Rules Wizard - Summary Page

Step 10  Click Finish.

The Traffic Rules page appears with the new traffic rule you created.

You have completed creation of the Web Traffic Coloring policy. Continue with Step 5: Creating the ERP Traffic Coloring Policy, page 2-26.

Related Topics
- Step 5: Creating the ERP Traffic Coloring Policy, page 2-26

Step 5: Creating the ERP Traffic Coloring Policy

This step assumes that you have completed Step 4: Creating the Web Traffic Coloring Traffic Rule, page 2-24.

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

Step 1  Select Traffic Rules in the Table of Contents.

The Traffic Rules page appears.

Step 2  Click Create > In Traffic Rules.

The In Traffic Rules wizard opens, displaying the In Traffic Rules Wizard - General page.
Step 3  Do the following In the In Traffic Rules Wizard - General page:
   a. Enter **Color ERP traffic** in the Traffic Rule Name field.
   b. Enter **Colors inbound ERP traffic** in the Enter Description for the Traffic Rule field.
   c. Leave the QoS Policy check box selected.
   d. Click **Next**.

   The In Traffic Rules Wizard - Traffic Classification page appears.

   Step 4  Do the following in the In Traffic Rules Wizard - Traffic Classification page:
   a. Enter **ERP traffic** in the Traffic Classifier name field.
   b. Click **Create** to define a traffic classifier condition.

   The Traffic Rule Setting page appears.

   Step 5  In the Traffic Rule Settings page, click **Edit** in the Protocol row of the Rule Setting table.

   The Protocol Editor page appears.

   Step 6  Do the following in the Protocol Editor page:
   a. Click the **From Library** radio button.
   b. Select **TCP** from the Source list box.
   c. Click **OK**.


   Step 7  In the Traffic Rule Setting page, click **Edit** in the Destination IP row of the Traffic Rule Setting table.

   The Destination IP Editor page appears.

   Step 8  Do the following in the Destination IP Editor page:
   a. Click the **IP Address/Host name list** radio button.
   b. Enter **10.1.2.3** (the IP address of the ERP server) in the IP/Host field.
   c. Click **Add**.

   The address is added to the Add a new value list. Leave the Mask field empty.
   d. Click **OK**.

   The Destination IP Editor page closes and the Traffic Rule Setting page refreshes.

   Step 9  Click **Done**.

   The In Traffic Rules Wizard - Traffic Classification page appears.

   Step 10 Click **Next**.

   The In Traffic Rules Wizard - Marking page appears.

   Step 11 Do the following in the In Traffic Rules Wizard - Marking page:
   a. Select **32 (cs4)** from the Value list box.

   The Enable Marking check box is automatically selected.
   b. Click **Finish**.
The In Traffic Rules Wizard - Summary page appears, where you can view a summary of the traffic rule. Figure 2-14 shows the completed In Traffic Rules Wizard - Summary page.

**Figure 2-14 Lesson 2-3—Remote FastEthernet Policy In Traffic Rules Wizard - Summary Page**

<table>
<thead>
<tr>
<th>Step 12</th>
<th>In the In Traffic Rules Wizard - Summary page, click <strong>Finish</strong>. The Traffic Rules page appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 13</td>
<td>Click <strong>Finish</strong>. The Policy View page appears with the new policy.</td>
</tr>
</tbody>
</table>

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**, page 2-28.

**Related Topics**
- Lesson 2-4: Creating the WAN PPP Policy, page 2-28

**Lesson 2-4: Creating the WAN PPP Policy**

The WAN PPP policy 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 is necessary because one policy with the necessary properties and traffic rules can be applied to all of the pertinent interfaces. This is unlike the situation with the coloring policy, in which two policies 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. Each step assumes that have just completed the previous step:

- **Step 1: Defining the WAN PPP Policy**, page 2-29
- **Step 2: Defining the WAN PPP Policy QoS Properties**, page 2-31
- **Step 3: Assigning Elements to the WAN PPP Policy**, page 2-32
- **Step 4: Creating the MQC CBWFQ Queuing Traffic Rules**, page 2-33

### Step 1: Defining the WAN PPP Policy

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

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

---

**Step 1** Select **Provisioning > Policy Management > Manage Policies > Policy View**.

The Policy View page appears.

**Step 2** Select **Tutorial** from the Change Policy Group list box.

The page refreshes to display the policies in the Tutorial policy group. If you have not added any policies to the policy group, the list is empty.

**Step 3** Click **Custom Policy > New Policy**.

The Policy Definition wizard appears.
Step 4  Do the following in the Policy Definition Wizard - General Definition page:

a. Enter **WAN PPP** in the Policy Name field.

b. Enter **Applies MQC CBWFQ to ERP and web traffic entering the WAN** in the Policy Description field.

c. Click **Next**.

The Policy Definition Wizard - Constraints Definition page appears.

Step 5  In the Policy Definition Wizard - Constraints Definition page, click **Define Manually**.

The Manual Constraint Definition area appears.

Step 6  Do the following in the Manual Constraint Definition area:

a. Select **2600** from the Model list.

b. Select **12.2** from the **OS list**.

c. Select **Interface** from the **Network Element list**.

d. Select **PPP** from the **Interface Type list**.

e. Click **Add**.

The Policy Definition Wizard - Constraints Definition page appears.

Step 7  In the Policy Definition Wizard - Constraints Definition page, click **Define Manually**.

The Manual Constraint Definition area appears.

Step 8  Do the following in the Manual Constraint Definition page:

a. Select **3600** from the Model list.

b. Select **12.2** from the **OS Version list**.

c. **Interface** is automatically entered in the from **Network Element field**.

d. Select **PPP** from the **Interface Type list**.

e. Click **Add**.

The Policy Definition Wizard - Constraints Definition page appears.

Step 9  In the Policy Definition Wizard - Constraints Definition page, click **Define Manually**.

The Manual Constraint Definition area appears.

Step 10 Do the following in the Manual Constraint Definition page:

a. Select **7200** from the Model list.

b. Select **12.2** from the **OS Version list**.

c. **Interface** is automatically entered in the from **Network Element field**.

d. Select **PPP** from the **Interface Type list**.

e. Click **Add**.
Chapter 2      Data Network Tutorial

Lesson 2-4: Creating the WAN PPP Policy

Step 11 In the Policy Definition Wizard - Constraints Definition page, click Capability Report.

The QoS Capability Report dialog box appears, where you can view a summary of the QoS features that can be configured for the policy, according to the device constraints.

Step 12 In the Policy Definition Wizard - Constraints Definition page, click Next.

The QoS Properties page appears.


Related Topics
- Step 2: Defining the WAN PPP Policy QoS Properties, page 2-31

Step 2: Defining the WAN PPP Policy QoS Properties

This step assumes that you have completed Step 1: Defining the WAN PPP Policy, page 2-29.

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

Step 1 In the QoS Properties page, click Edit.

The QoS Properties Wizard - Congestion Management page appears.

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.

Step 3 In the QoS Properties Wizard - Summary page, click Finish.

The QoS Properties page appears.
You have completed defining QoS properties for the WAN PPP policy. Now you assign network elements to it. Continue with Step 3: Assigning Elements to the WAN PPP Policy, page 2-32.

### Related Topics
- Step 3: Assigning Elements to the WAN PPP Policy, page 2-32

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

This step assumes that you have completed Step 2: Defining the WAN PPP Policy QoS Properties, page 2-31.

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

### Step 1
Select **Network Assignment** in the Table of Contents.
The Network Assignment page appears.

### Step 2
In the Assigned Network Elements page, click **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 checking 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 elements appear in the Network Assignment page.

You have completed assigning network elements to the WAN PPP policy. Now you create the MQC CBWFQ queuing traffic rules. Continue with Step 4: Creating the MQC CBWFQ Queuing Traffic Rules, page 2-33.

### Related Topics
- Step 4: Creating the MQC CBWFQ Queuing Traffic Rules, page 2-33
Step 4: Creating the MQC CBWFQ Queuing Traffic Rules

In this step you create the three traffic rules 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 traffic rules:

- Step 4a: Creating the ERP Traffic Queuing Traffic Rule, page 2-33
- Step 4b: Creating the Web Traffic Queuing Traffic Rule, page 2-35
- Step 4c: Creating the Class Default Traffic Rule, page 2-36

Step 4a: Creating the ERP Traffic Queuing Traffic Rule

This step assumes that you have completed Step 3: Assigning Elements to the WAN PPP Policy, page 2-32.

In this step you create the ERP Traffic Queuing traffic rule, 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.

---

Step 1
Select Traffic Rules in the Table of Contents.
The Traffic Rules page appears.

Step 2
Click Create > Out Traffic Rules.
The Out Traffic Rules wizard opens, displaying the In Traffic Rules Wizard - General page.

Step 3
Do the following in the Out Traffic Rules Wizard - General page:

a. Enter ERP Traffic Queuing in the Traffic Rule Name field.
b. Enter Queues ERP traffic entering the WAN in the Enter Description for the Traffic Rule field.
c. Leave the QoS Policy radio button selected.
d. Click Next.
The Out Traffic Rules Wizard - Traffic Classification page appears.

Step 4
Do the following in the Out Traffic Rules Wizard - Traffic Classification page:

a. Leave the Create a new traffic classifier radio button selected.
b. Enter ERP Traffic in the Traffic Classifier Name field.
c. Click Create.
The Traffic Rule Setting page appears.

Step 5
In the Traffic Rule Setting page, click Edit in the Service table row.
The Service Editor page appears.

Step 6
Do the following in the Service Editor page:

a. Select 32 (cs4) from the Value list box.
b. Click OK.

The Service Editor page closes, and the Traffic Rule Setting page refreshes.

Step 7

In the Traffic Rule Settings page, click Done.
The Out Traffic Rules Wizard - Traffic Classification page appears.

Step 8

In the Out Traffic Rules Wizard - Traffic Classification page, click Next.
The Out Traffic Rules Wizard - Marking page appears.

Step 9

Click Queuing in the Navigation list (Traffic Actions).
The Out Traffic Rules Wizard - Queuing page appears.

Step 10

Do the following in the Out Traffic Rules Wizard - Queuing page:

a. Enter 40 in the bandwidth field.

The Enable Bandwidth Allocation (CBQ) check box is automatically selected when you click outside the edit box.

b. Leave the Ratio radio button selected.

c. Click Finish.

The Out Traffic Rules Wizard - Summary page appears, where you can view a summary of the policy. Figure 2-16 shows the completed Out Traffic Rules Wizard - Summary page.

Figure 2-16   Lesson 2-4—WAN PPP Policy Out Traffic Rules Wizard - Summary Page

Step 11

In the Out Traffic Rules Wizard - Summary page, click Finish.
The Traffic Rules page appears.

Related Topics
- Step 4b: Creating the Web Traffic Queuing Traffic Rule, page 2-35

**Step 4b: Creating the Web Traffic Queuing Traffic Rule**

This step assumes that you have completed Step 4a: Creating the ERP Traffic Queuing Traffic Rule, page 2-33.

In this step you create the Web Traffic Queuing traffic rule, 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.

---

**Step 1**

In the Traffic Rules page, click Create > Out Traffic Rules.

The Out Traffic Rules wizard opens, displaying the Out Traffic Rules Wizard - General page.

**Step 2**

Do the following in the Out Traffic Rules Wizard - General page:
- **a.** Enter **Web Traffic Queuing** in the Traffic Rule Name field.
- **b.** Enter **Queues web 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 Traffic Rules Wizard - Traffic Classification page appears.

**Step 3**

Do the following in the Out Traffic Rules Wizard - Traffic Classification page:
- **a.** Leave the Create a new traffic classifier radio button selected.
- **b.** Enter **Web Traffic** in the Traffic Classifier Name field.
- **c.** Click **Create**.

The Traffic Rule Setting page appears.

**Step 4**

In the Traffic Rule Setting page, click **Edit** in the Service table row.

The Service Editor page appears.

**Step 5**

Do the following in the Service Editor page:
- **a.** Select **16 (cs2)** from the Value list box.
- **b.** Click **OK**.

The Service Editor page closes, and the Traffic Rule Setting page refreshes.

**Step 6**

In the Traffic Rule Setting page, click **Done**.

The Out Traffic Rules Wizard - Traffic Classification page appears.

**Step 7**

In the Out Traffic Rules Wizard - Traffic Classification page, click **Next**.

The Out Traffic Rules Wizard - Marking page appears.

**Step 8**

Click **Queuing** in the Navigation list (Traffic Actions).

The Out Traffic Rules Wizard - Queuing page appears.

**Step 9**

Do the following in the Out Traffic Rules Wizard - Queuing page:
- **a.** Enter **20** in the bandwidth field.

The Enable Bandwidth Allocation (CBQ) check box is automatically selected when you click outside the edit box.
b. Click Finish.

The Out Traffic Rules Wizard - Summary page appears, where you can view a summary of the policy. Figure 2-17 shows the completed Out Traffic Rules Wizard - Summary page.

Figure 2-17  Lesson 2-4—WAN PPP Policy Group Out Traffic Rules Wizard - Summary Page

Step 10

In the Out Traffic Rules Wizard - Summary page, click Finish.

The Traffic Rules page appears.

You have completed creating the Web Traffic Queuing policy. Now you create the Class Default policy. Continue with Step 4c: Creating the Class Default Traffic Rule, page 2-36.

Related Topics
- Step 4c: Creating the Class Default Traffic Rule, page 2-36

Step 4c: Creating the Class Default Traffic Rule

This step assumes that you have completed Step 4b: Creating the Web Traffic Queuing Traffic Rule, page 2-35.

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

Step 1

In the Traffic Rules page, click Create > Out Traffic Rules.

The Out Traffic Rules wizard opens, displaying the Out Traffic Rules Wizard - General page.

Step 2

Do the following in the Out Traffic Rules Wizard - General page:

a. Enter WAN PPP Default in the Traffic Rule Name field.

b. Enter Queues default traffic using WFQ in the Enter Description for the Traffic Rule field.
c. Leave the QoS Policy radio button selected.
d. Click Next.

The Out Traffic Rules Wizard - Traffic Classification page appears.

**Step 3**

Do the following in the Out Traffic Rules Wizard - Traffic Classification page:

a. Click the Class Default radio button.

b. Click Next.

The Out Traffic Rules Wizard - Marking page appears.

**Step 4**

Click **Queuing** in the Navigation list (Traffic Actions).

The Out Traffic Rules Wizard - Queuing page appears.

**Step 5**

Do the following in the Out Traffic Rules Wizard - Queuing page:

a. Check the **Enable WFQ** check box.

b. Click **Finish**.

The Out Traffic Rules Wizard - Summary page appears, where you can view a summary of the policy. **Figure 2-18** shows the completed Out Traffic Rules Wizard - Summary page.

**Figure 2-18  Lesson 2-4—WAN PPP Policy Out Traffic Rules Wizard - Summary Page**

---

**Step 6**

In the Out Traffic Rules Wizard - Summary page, click **Finish**.

The Traffic Rules page appears.

**Step 7**

Click **Finish**.

The Policy View page appears displaying the policy you created.
Now that you have completed creating the WAN PPP policy 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, page 2-38.

Related Topics
- Lesson 2-5: Adding FTP Policing To the Campus Access VLAN Policy, page 2-38

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

This lesson demonstrates how you can add additional functionality to an existing policy. 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.

This lesson assumes that you have completed Lesson 2-2: Defining Policies and Traffic Rules To Color Campus Web Traffic, page 2-11.

Step 1 Select Provisioning > Policy Management > Manage Policies > Policy View.

The Policy View page appears.

Step 2 Select Tutorial from the Change Policy Group list box.

The page refreshes to display the policies in the Tutorial policy group. If you have not added any policies to the policy group, the list is empty.

Step 3 Click the Campus Access VLAN policy in the object selector.

The properties of the policy appear in the content area.

Step 4 Click Traffic Rules.

The Traffic Rules page for the policy appears.

Step 5 In the Traffic Rules page, click Create > In Traffic Rule.

The In Traffic Rules Wizard - General page appears.

Step 6 Do the following in the In Traffic Rules Wizard - General page:
   a. Enter FTP Policing in the Traffic Rule Name field.
   b. Enter Polices FTP traffic in the Enter Description for the Traffic Rule field.
   c. Click Next.

The In Traffic Rules Wizard - Traffic Classification page appears.

Step 7 Do the following in the In Traffic Rules Wizard - Traffic Classification page:
   a. The New Traffic Classifier check box is automatically selected.
   b. Enter FTP Traffic in the Traffic Classifier name field.
   c. Click Create.

The Traffic Rule Setting page appears.

Step 8 In the Traffic Rule Setting page, click Edit in the Protocol table row.

The Protocol Editor page appears.
Step 9  Do the following in the Protocol Editor page:
   a. Leave the From Library radio button selected.
   b. Select ftp-TCP from the Source list box.
   c. Click OK.


Step 10  In the Traffic Rule Settings page, click Done.

The In Traffic Rules Wizard - Traffic Classification page appears.

Step 11  In the In Traffic Rules Wizard - Traffic Classification page, click Next.

The In Traffic Rules Wizard - Marking page appears.

Step 12  Select Policing in the Navigation list (Traffic Actions).

The In Traffic Rules Wizard - Policing page appears.

Step 13  Do the following in the In Traffic Rules Wizard - Policing page:
   a. Click the Aggregate radio button.
   b. Enter 128 in the Rate field.
      The Enable Policing check box is automatically selected when you click outside the edit box.
   c. Enter 128 in the Burst field.
   d. Select Mark and Transmit from the Conform Action list box.
   e. Select 0 (default) from the Mark with list box.
   f. Select Drop from the Exceed Action list box.
   g. Click Finish.
Lesson 2-6: Deploying the Data Network Tutorial Policies

The In Traffic Rules Wizard - Summary page appears, where you can view a summary of the policy. Figure 2-19 shows the completed In Traffic Rules Wizard - Summary page.

**Figure 2-19** Lesson 2-5—Campus Access VLAN Policy In Traffic Rules Wizard - Summary Page

### Step 14
In the In Traffic Rules Wizard - Summary page, click Finish. The Traffic Rules page appears.

### Step 15
Click Finish. The Policy View page appears.

Now that you have added FTP policing to the Campus Access VLAN policy, you can proceed with the next lesson, Lesson 2-6: Deploying the Data Network Tutorial Policies, page 2-40.

**Related Topics**
- Lesson 2-6: Deploying the Data Network Tutorial Policies, page 2-40

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

This lesson describes how to deploy the QoS policies that were saved in your policy 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” policy 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 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.

---

**Step 1** Select **Provision > Policy Deployment > Create Job**. The first step of the Deployment wizard is displayed—Job Details.

**Step 2** Enter **Data_Tutorial** in the Job Name field.

If required, you can enter a description for the job in the Job Description field.

**Step 3** Select the Schedule of policy deployment as **Now** or **Run at (Server Time)**, by clicking the corresponding radio button.

If you select the **Run at (Server Time)** option, you should select the date, and enter the time.

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

The Policy Group Selection page opens.

**Step 5** Select the **Current version of a Policy Group** radio button, and select **Tutorial** from the list box if it is not already selected.

**Step 6** Click **Next** to move to the next step of the wizard—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.

- 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.

- 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 7** When you have finished previewing the device’s configuration, click **Close** to close the Preview window.

**Step 8** 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 9** After you have verified the job information, click **Deploy** to deploy the policy group to the network.

The Active Jobs page appears, enabling you to monitor the deployment process, as described in the next lesson, **Lesson 2-7: Monitoring the Deployment Process**, page 2-42.

---

**Related Topics**

- Understanding the Data Network Tutorial Example Network, page 2-2
- Lesson 2-7: Monitoring the Deployment Process, page 2-42
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.

Step 1  Select Provision > Policy Deployment > Pending Jobs.
The Active Jobs page appears, displaying your current deployment job and its status.
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.
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 2-40
CHAPTER 3

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. It takes you 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 policies 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 according to voice policy templates that are based on the IP Telephony QoS guide. Each voice policy contains a "voice role" attribute, which specifies the role of the interface on the network, such as, IP phone and 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 1-6.

**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 3-4 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 3-2
- **Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard**, page 3-6
- **Lesson 3-2: Modifying the Voice Policies**, page 3-20
- **Lesson 3-3: Deploying the IP Telephony QoS Policies**, page 3-29
- **Lesson 3-4: Monitoring the Deployment Process**, page 3-31

**Related Topics**


### 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*

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

- **Configuring QoS for the Campus Site**, page 3-3
- **Configuring QoS for the WAN**, page 3-3
- **Configuring QoS for the Remote Branch**, page 3-4
- **Network Example Device Information**, page 3-4
Chapter 3      IP Telephony Network Tutorial

Understanding the IP Telephony Network Example

Configuring QoS for the Campus Site

The campus site includes a Cisco CallManager server, 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 3-2
- Step 3: Selecting the IP Phone Connections, page 3-10
- Step 4: Selecting the SoftPhone Connection, page 3-11
- Step 5: Selecting the CallManager Port, page 3-12
- Step 6: Selecting the IntraLAN Connections, page 3-13
- Step 7: Selecting the Voice VLAN Connections, page 3-15

Configuring QoS for the WAN

Since the 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 3-2
Configuring QoS for the Remote Branch

The remote site includes an IP phone that is connected using 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 3-2
- Step 3: Selecting the IP Phone Connections, page 3-10
- Step 9: Selecting the Router WAN to Switch Connection, page 3-17

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>
<thead>
<tr>
<th>Device Name</th>
<th>Device Model and IP Address</th>
<th>Software Version</th>
<th>Interfaces</th>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
</table>
| Core-7200-1 | 7200 10.1.1.1               | 12.2             | FastEthernet0/0  
                FastEthernet (100 Mb/sec)  
                Serial5/0  
                Frame Relay line at 1544 Kbit/second  
                Serial 5/0.1 DLCI 40 | 10.9.1.1  
                10.9.2.1 | 255.255.255.0  
                255.255.255.0 |
| Core-3600-2 | 3600                       | 12.2T            | FastEthernet0/1  
                FastEthernet (100 Mb/sec)  
                Fa0/1.150  
                voice VLAN  
                Fa0/1.5  
                data VLAN  
                Serial2/0  
                Frame Relay line at 512 Kbit/second  
                Serial 2/0.1 DLCI 40 | 10.8.150.1  
                10.8.5.1  
                10.8.2.2 | 255.255.255.0  
                255.255.255.0  
                255.255.255.0 |
### Table 3-1 Sample Network Device Information for IP Telephony Network Tutorial (continued)

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Device Model and IP Address</th>
<th>Software Version</th>
<th>Interfaces</th>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access-Cat6000-3</td>
<td>6509 10.6.1.2</td>
<td>6.3</td>
<td>VLAN5 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) GigabitEthernet1/0 Gigabit Ethernet (1000 Mb/sec)</td>
<td>10.6.1.2</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Access-Cat6000-4</td>
<td>6509 10.7.2.2</td>
<td>12.1E</td>
<td>GigabitEthernet1/1 Gigabit Ethernet (1000 Mb/sec) GigabitEthernet1/2 Gigabit Ethernet (1000 Mb/sec) FastEthernet2/1 FastEthernet (100 Mb/sec)</td>
<td>10.7.2.2</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Access-Cat3500-2</td>
<td>3524-PWR-XL 10.4.1.2</td>
<td>12.0</td>
<td>Ethernet2/3 Standard Ethernet (10/100 Mbit/sec) GigabitEthernet0/1 Gigabit Ethernet (1000 Mb/sec)</td>
<td>10.4.1.2</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Access-Cat2900-2</td>
<td>2900-XL 10.4.4.2</td>
<td>12.0</td>
<td>FastEthernet0/1 FastEthernet (100 Mb/sec) Ethernet3/1 Standard Ethernet (10/100 Mbit/sec)</td>
<td>10.4.4.2</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

**Related Topics**
- Understanding the IP Telephony Network Example, page 3-2
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 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.

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

- Step 1: Introduction, page 3-8
- Step 2: Selecting Devices for QoS Configuration, page 3-9
- Step 3: Selecting the IP Phone Connections, page 3-10
- Step 4: Selecting the SoftPhone Connection, page 3-11
- Step 5: Selecting the CallManager Port, page 3-12
- Step 6: Selecting the IntraLAN Connections, page 3-13
- Step 7: Selecting the Voice VLAN Connections, page 3-15
- Step 8: Selecting the Switch to WAN Router Connection, page 3-16
- Step 9: Selecting the Router WAN to Switch Connection, page 3-17
- Step 10: Selecting the WAN Frame Relay Connections, page 3-19
- Step 11: End, page 3-20

Before you Begin

To run the wizard, check whether:

- 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 1-6.
- The “Tutorial” deployment group has been created. See Lesson 1-4: Creating the Tutorial Policy Group, page 1-8.

Related Topics

- Using the IP Telephony Wizard, page 3-6

Using the IP Telephony Wizard

This section helps you to understand the following main features of the IP Telephony wizard and how to use them:

- Description, page 3-7
- Advanced, page 3-7
- Selection Table, page 3-7
- Assignment Summary, page 3-7
- Saving Your Assignments, page 3-7
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**
  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 policies. The wizard removes the assignment of selected elements from the voice policy.

- **Recommend**
  Activates the wizard to accept the recommended selection of network elements for the current voice role. This option is functional if QPM rules are available for a specific voice role.
  The network elements are selected but not assigned to voice policy. 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 do not 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 policies 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. You can also use the Navigation TOC that is displayed on the left side of each page to move directly to a particular step.

- If you click Next to move to the next configuration step, or to select another step forward in the Navigation TOC, it saves the voice policies and the assignments that were made for that voice role, to the deployment group.

- If you click Cancel, Back, or select another step backward in the Navigation TOC, it undoes any configuration changes you made in that step.

- If you select the Display Configuration Info. check box, clicking Next opens the assignments summary page for that configuration step.
The voice policies will be saved in the deployment group, but the assignment of interfaces to them will not be saved.

After reviewing your assignments summary and click Next in this page, it saves both the voice policy and the interface assignments. It also opens the next step of the wizard.

Related Topics
- Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard, page 3-6

Step 1: Introduction

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

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

Step 1 Select Provisioning > Manage Policies > Policy View

The Policy View page appears.

Step 2 Click Voice Policy.

The Introduction page of the wizard appears.

If the displayed policy group is not “Tutorial,” select it from the policy group list box.

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

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

Related Topics
- Understanding the IP Telephony Network Example, page 3-2
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 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 devices in your device group and whether they support QoS for voice, in the Voice Ready report.

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 1-6.

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

### Step 1
Select the following devices by checking 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  To view the Assignment Summary page you can do the following:

- If you want to view summary information about the assignments made at each configuration step of the wizard, check the Display Configuration Info. check box, and click Next. The Assignment Summary page appears.
- If you do not want to view the assignments summary at each configuration step of the wizard, uncheck 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 policies 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 3-2
- Configuring QoS for the Campus Site, page 3-3
- Using the IP Telephony Wizard, page 3-6
- Step 3: Selecting the IP Phone Connections, page 3-10

**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).

Step 1  Check 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  Check 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  Check 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.
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).
Step 1  Check 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 checked, the Configuration Info page appears.

Step 3  After reviewing the assignments summary, click Next or select CallManager in the Navigation TOC. The selected SoftPhone port is assigned to the appropriate voice policies 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 3-2
- Configuring QoS for the Campus Site, page 3-3
- Using the IP Telephony Wizard, page 3-6
- Step 5: Selecting the CallManager Port, page 3-12

**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).
Chapter 3

IP Telephony Network Tutorial

Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard

Step 1
Check 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 checked, the Configuration Info page appears.

Step 3
After reviewing the assignments summary, click Next or select IntraLAN in the Navigation TOC.
The selected CallManager port is assigned to the appropriate voice policy 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 3-2
- Configuring QoS for the Campus Site, page 3-3
- Using the IP Telephony Wizard, page 3-6
- Step 6: Selecting the IntraLAN Connections, page 3-13

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.

**Step 1** Check 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**

**Step 2** Click Next.

If the Display Configuration Info. check box is checked, the Configuration Info page appears.

**Step 3** After reviewing the assignments summary, click **Next** or select **Voice VLAN** in the Navigation TOC.
The selected interfaces are assigned to the appropriate voice policies 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 3-2
- Configuring QoS for the Campus Site, page 3-3
- Using the IP Telephony Wizard, page 3-6
- Step 7: Selecting the Voice VLAN Connections, page 3-15

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.

Step 1 Check 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 checked, the Configuration Info page appears.
Step 3  
After reviewing the assignments summary, click Next or select Switch to WAN Router in the Navigation TOC. 
The selected VLAN is assigned to the appropriate voice policies 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 3-2
- Configuring QoS for the Campus Site, page 3-3
- Using the IP Telephony Wizard, page 3-6
- Step 8: Selecting the Switch to WAN Router Connection, page 3-16

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.

Step 1  
Check the check box next to the FastEthernet2/1 interface in the table, to configure QoS for the distribution switch connection to the WAN router.
Step 2  Click Next.

If the Display Configuration Info. check box is checked, the Configuration Info page appears.

Step 3  After reviewing the assignments summary, click Next or select Router WAN to Switch in the Navigation TOC.

The selected interface is assigned to the appropriate voice policies 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 3-2
- Configuring QoS for the WAN, page 3-3
- Using the IP Telephony Wizard, page 3-6
- Step 9: Selecting the Router WAN to Switch Connection, page 3-17

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.

**Step 1**
Check the check box next to the Fa0/1.150 interface to configure QoS for the Core-3600-2 router interface to the Catalyst 2900 access switch.

This is the voice VLAN defined on the interface (the other VLAN is a data VLAN).

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

**Step 2**
Click Next.

- If the Display Configuration Info. check box is checked, 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 checked, the WAN Point-to-Point Connections page appears. Click Next, or select **WAN Frame Relay** in the Navigation TOC.

The selected interfaces are assigned to the appropriate voice policies 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 3-2
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 configures QoS separately for groups of interfaces, according to their link speed.

**Step 1** Check 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** Check 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.
Chapter 3      IP Telephony Network Tutorial

Lesson 3-2: Modifying the Voice Policies

The selected interfaces are assigned to the appropriate voice policies 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 3-2
- Configuring QoS for the WAN, page 3-3
- Using the IP Telephony Wizard, page 3-6
- Step 11: End, page 3-20
- Lesson 3-2: Modifying the Voice Policies, page 3-20

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 policy group.

From this page, you can go directly to the Policy wizard to deploy the policy group, or to the Policy page to view a detailed summary of all the voice policies that you created in the wizard.

From the Policy View page, you can modify the properties and policies configured in the voice policies.

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

1. Click the No radio button in the End page of the wizard.
2. Click Finish to close the wizard.

The Policy View page appears.

Related Topics
- Using the IP Telephony Wizard, page 3-6
- Lesson 3-2: Modifying the Voice Policies, page 3-20

Lesson 3-2: Modifying the Voice Policies

QPM allows you to customize policies to suit specific network configurations by modifying the voice policies. After you have completed the IP Telephony wizard, you can modify properties and policies of the voice policies created by the wizard.

QPM allows you to modify any of the properties and traffic rules of a voice policy, except for its device constraints. Changing the device constraints will cause the voice policy to lose its voice role. In this case, the IP Telephony wizard will be unable to assign network elements to the voice policy.

Note
You cannot modify a policy that is linked to a policy template. Whenever you want to modify a policy created by the IP Telephony wizard, you must first disconnect the policy from the template, or modify the template.
In this lesson, you will learn how to modify the following WAN Frame Relay voice policies that were created in Step 10: Selecting the WAN Frame Relay Connections of the wizard:

- **WAN-FR- Main-Interface**
  This voice policy is for a main Frame Relay interface that has DLCI interfaces for voice traffic. In this voice policy, 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. This 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.

- **WAN-FR-DLCI-Slow**
  This voice policy is for low speed Frame Relay interfaces. To ensure that important data traffic is not starved for bandwidth, you can create a traffic rule to define a minimum bandwidth for the data. In this lesson, you will learn how to configure the percentage of bandwidth that should be reserved for the important, or “gold,” data traffic.

**Before You Begin**

To do this lesson you should have completed Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard, page 3-6.

After you have completed the IP Telephony wizard and you selected not to deploy your QoS policies, as described in Step 11: End, page 3-20, the Policy Table page automatically appears.

The Policy Table page displays all the voice policies that were created by the wizard. For each voice policy group, its associated voice role is displayed.

You can also open the Policy Groups page by selecting Provision > Policy Table.

This lesson is divided into the following two lessons:

- Lesson 3-2-1: Enabling cRTP for the WAN-FR-Main-Interface Voice Policy, page 3-21
- Lesson 3-2-2: Configuring the Gold Data Bandwidth for the WAN-FR-DLCI-Slow Voice Policy, page 3-24

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

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.

**Step 1**

In the Policy View page, click the WAN-FR-Main-Interface policy in the object selector. The properties of the policy appears in the content area, as shown in Figure 3-12.
Lesson 3-2: Modifying the Voice Policies

Step 2 Click Disconnect to disconnect the voice policy from the template.
This allows you to edit the policy.

Step 3 Click QoS Properties.
The QoS Properties page appears, where you can see that 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.
On the Traffic Control Settings page, you can see the traffic control parameters that were configured by the IP Telephony wizard for the WAN-FR-Main-Interface voice policy.

Step 6  
Check the **Enable IP RTP Header Compression** check box to enable cRTP.

---

**Figure 3-14  Lesson 3-2-1—Traffic Control Settings for the WAN-FR-Main-Interface Policy**

---

Step 7  
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. The page shows that cRTP is now enabled for the policy.

---

**Figure 3-15  Lesson 3-2-1—Summary Page for the WAN-FR-Main-Interface Policy**

---

Step 8  
Click **Finish** to save the changes.
The QoS Properties page appears, displaying the modified configuration. cRTP is now configured for this voice policy.

**Step 9**

Click **Finish**.

The Policy View page appears.


---

**Related Topics**

- Lesson 3-2: Modifying the Voice Policies, page 3-20
- Lesson 3-1: Assigning Voice Policies Using the IP Telephony Wizard, page 3-6
- Step 10: Selecting the WAN Frame Relay Connections, page 3-19

---

**Lesson 3-2-2: Configuring the Gold Data Bandwidth for the WAN-FR-DLCI-Slow Voice Policy**

In this lesson, you will learn how to modify the WAN-FR-DLCI-Slow voice policy, by creating a QoS traffic rule that configures a minimum percentage of bandwidth on the interface that should be reserved for important, or “gold,” data traffic.

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

A QoS policy contains a traffic classifier and actions, so you will need to define the traffic classifier for the policy, and then the policy actions. After it is created, the new QoS policy will be added to the outbound policies that are currently defined for the template.

**Before You Begin**

The policy created in this lesson assumes that important data traffic has already been classified. For a policy like this one to work in your network, you must create classification policies on end-point interfaces to correctly classify traffic from attached devices.

**Step 1**

Go to **Provisioning > Pre-Configuration > Policy Templates**.

The Policy Templates page appears.

**Step 2**

Check the check box corresponding to the WAN-FR-DLCI-Slow policy template, and click **Edit**.

The General page of the Policy Definition Wizard appears.

**Step 3**

Click **Traffic Rules**.

The Traffic Rules page appears, displaying the current traffic rules defined for the policy template.
Step 4  Click Create > Out Traffic Rules.

The General page of the Out Traffic Rules wizard appears.

Step 5  In the Out Traffic Rules wizard - General page, enter this information (as shown in Figure 3-17).

- Enter Gold Data in the Traffic Rule Name field.
- Enter This policy configures the percentage of bandwidth to be reserved for gold data traffic in the Description field.

Figure 3-17 Lesson 3-2-2—Out Traffic Rules Wizard - General Page

Step 6  Click Next.
The Out Traffic Rules wizard - Traffic Classification page appears.

**Step 7**  
In the Out Traffic Rules wizard - Traffic Classification page, ensure that Create a new traffic classifier is selected, and enter Gold Data as the traffic classifier name, and create the rules for the traffic classifier:

a. Click Create.

b. In the Traffic Rule Setting page, click Edit next to the Service traffic classifier condition. The Service Editor page appears.

c. In the Service Editor page, select 18 (af21) from the Value list box. This is the DSCP value of the packet.

d. Click OK to select the value and return to the Traffic Rule Setting page.

e. In the Traffic Rule Setting page, click Done.

The Out Traffic Rule Wizard - Traffic Classification page reappears, displaying the traffic classifier rule you have defined.

f. Repeat this process to create rules for these DSCP values:
   - 20 (af22)
   - 22 (af23)

After you are finished, the Traffic Classifier Page should look as shown in Figure 3-18.

**Figure 3-18**  
Lesson 3-2-2—Out Traffic Rules Wizard - Traffic Classification Page

**Step 8**  
Click Next in the Out Traffic Rules Wizard - Traffic Classification page.

The Out Traffic Rules Wizard - Traffic Actions page for Shaping appears.

**Step 9**  
Define the QoS policy action:

a. Select Traffic Actions > Queuing in the wizard navigation TOC to open the page for defining the queuing actions.
Queuing actions manage congestion for outbound traffic.

b. Check the **Enable Bandwidth Allocation (CBQ)** check box.

c. Enter 25 in the Bandwidth field to define the percentage of the interface’s bandwidth you want to allocate to gold data traffic. Ensure that **Ratio** check box is selected, to indicate you are entering a number that is a percentage of bandwidth, rather than a rate.

*Figure 3-19  Lesson 3-2-2—Out Traffic Rules Wizard - Queuing Actions Page*

**Step 10** Click **Finish** to complete the wizard.

The Summary page appears, where you can read a summary of the traffic rule you just defined.

**Step 11** Click **Finish** to complete the traffic rule and exit the wizard and return to the Out Traffic Rules page.
When you define a traffic rule, it is automatically added to the end of the list of traffic rules that are already defined for the policy. Since traffic rules 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 3-20, the Class Default traffic rule precedes your new QoS traffic rule. Since this traffic rule is applied to all traffic that does not match any of the traffic classifiers, you must reorder the traffic rules so that it appears last in the list.

Otherwise, no traffic will match your new traffic rules, even if the traffic has the required DSCP values.

**Step 12** Change the order of the traffic rules in the policy template:

a. Click **Reorder** in the Out Traffic Rules page.

b. In the Reorder Policies dialog box, select **Gold Data** and click the Up button.

c. Click **OK**.

The dialog box closes, and the Out Traffic Rules page reappears displaying the new order.
Lesson 3-3: Deploying the IP Telephony QoS Policies

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

Although you can follow all the steps in this lesson, the actual deployment of the “Tutorial” policy 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 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 3-6.

---

**Step 1** Select **Provisioning > Policy Deployment**.

**Step 2** Click **Create Job** in ToC.

The first step of the Deployment wizard appears—Job Details page

**Step 3** Enter **IPT_Tutorial** in the Job Name field.

If required, you can enter a description for the job in the Job Description box.

**Step 4** Select the Schedule of policy deployment as **Now** or **Run at (Server Time)**, by clicking the corresponding radio button

If you select the Run at (Server Time) option, you should select the date, and enter the time.

**Step 5** Click **Next** to move to the next step of the wizard—Policy Group Selection page.

**Step 6** Select the Current version of a Policy Group radio button, and select **Tutorial** from the list box (if it isn’t already selected).

**Step 7** 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.

- 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.
- 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 8** After you have finished previewing the device’s configuration, click **Close** to close the Preview window.

**Step 9** Click **Next** to move to the final step of the wizard.

This page displays a summary of the data collected through the wizard for you to verify. If required, you can enter a description for the job in the Job Description box.

**Step 10** After you have verified the job information, click **Deploy** to deploy the policy group to the network.

The Active Jobs page appears, enabling you to monitor the deployment process, as described in the next lesson.
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.

Step 1  Select Provisioning > Policy Deployment > Pending Jobs.

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

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 3-2
- Lesson 3-4: Monitoring the Deployment Process, page 3-31
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 traffic classifiers 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 4-4
- Lesson 4-2: Monitoring QoS, page 4-12
- Lesson 4-3: Monitoring QoS in Real Time, page 4-19

Understanding QPM Monitoring

QPM monitors traffic based on the QoS policies that have been distributed to network interfaces using QPM, or have been distributed directly to the network interfaces using CLI commands. QPM cannot monitor traffic on interfaces that do not have QoS policies.

These topics help you understand QPM’s monitoring capabilities.

- What is the Purpose of QoS Analysis?, page 4-1
- What Can You Monitor Using QPM?, page 4-2
- What Is the Difference Between Historical and Real-Time Monitoring?, page 4-2
- How Much Disk Space Is Required for Historical Monitoring?, page 4-3

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 4-4 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 correct way, or if the policies need to be adjusted. Lesson 4-2: Monitoring QoS, page 4-12 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 whether a problem on an interface, is related to the QoS policies that are active on the interface. Lesson 4-3: Monitoring QoS in Real Time, page 4-19 describes how to do real-time monitoring.

What Can You Monitor Using QPM?

You can monitor class-based QoS and CAR QoS policies on devices running specific Cisco IOS software versions, as long as you have distributed QoS policies using QPM. User Guide for CiscoWorks QoS Policy Manager has a detailed explanation of what can be monitored.

For the purposes of these tutorial lessons, keep these basic rules in mind:

• The device and Cisco IOS Software version must support QPM monitoring, as detailed in the QPM device support tables at this URL:

• Class-based QoS policies are policies defined on interfaces where you have configured Class Based QoS as the scheduling property. Only QoS configurations that are defined as actions to these policies can be monitored. For example, if you want to monitor WRED, you must define it as the action for a policy. If you define it as a QoS property on the interface, it cannot be monitored.

• CAR policies are policing policies defined on interfaces where you have configured Default as the scheduling property. On supported devices, QPM translates these policing policies into CAR policies. Only policing policies are monitored on interfaces that use default scheduling.

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 only makes QPM aware of the policies. It also lets you use QPM to modify and redistribute these policies, hereafter.

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 4-4.

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 4-12.

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 large amount 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>
<thead>
<tr>
<th>Characteristic</th>
<th>Historical</th>
<th>Real-Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of interfaces monitored per task</td>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td>Disk space requirements</td>
<td>Substantial. See How Much Disk Space Is Required for Historical Monitoring?, page 4-3</td>
<td>No disk space used. Data is only presented on web page; it is not saved.</td>
</tr>
<tr>
<td>Polling interval for data collection</td>
<td>From 1 to 60 minutes.</td>
<td>From 10 to 30 seconds.</td>
</tr>
<tr>
<td>Length of task</td>
<td>Up to several months, depending on polling interval. QPM enforces a duration limit based on polling interval. See the User Guide for CiscoWorks QoS Policy Manager for the specific limits.</td>
<td>As long as you want, but you must be at the computer to see the data.</td>
</tr>
<tr>
<td>Reuse of monitoring task</td>
<td>Can only be run once, because you set a start and end time.</td>
<td>Can be rerun any time desired, because there is no set start or end time.</td>
</tr>
<tr>
<td>Reviewing results</td>
<td>Can review the results as many times as you want.</td>
<td>Results must be reviewed as they are collected.</td>
</tr>
</tbody>
</table>

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 traffic classifier 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.

Both of these would be considered as small tasks. An historical monitoring task for 12 interfaces that each have six policies (each with one condition in the traffic classifier 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 traffic classifiers—Separate statistics are collected for each traffic classifier 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. owing to the amount of data that can be generated, qpm limits the duration of tasks based on the polling interval. qpm will alert you if you select a duration that is too long for the polling interval. see user guide for ciscoworks qos policy manager 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 one 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 classify 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 4-4
- step 1: classifying traffic for analysis, page 4-5
- step 2: setting up an historical monitoring task, page 4-9
- step 3: reading the historical monitoring graphs, page 4-10

understanding how to monitor traffic for baseline analysis

qpm can only monitor traffic if the traffic meets the traffic classifier 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 classify traffic without affecting the traffic.

you can use class-based policing policies to accomplish this type of classifying. specifically, the policing policies should have these characteristics:

- qos property for the policy—select class-based qos for the scheduling method for the policy.
• Traffic Classifiers—Try to isolate types of traffic on your network that you will want to treat the same way.

For example, you might create a traffic classifier for applications that require real-time performance (such as voice and video), another traffic classifier for important data-intensive applications (such as database, CRM, or other ERP traffic), and another traffic classifier 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 classify 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: Classifying Traffic for Analysis, page 4-5
- Understanding QPM Monitoring, page 4-1

**Step 1: Classifying Traffic for Analysis**

Before you can do a baseline analysis of the traffic on an interface, you must create a policy with the interfaces and an appropriate set of policies. The policies classify 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 policy 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 traffic classifiers to make them meaningful for your network; the examples shown might not provide you with meaningful baseline information for your network.

Make sure the device and Cisco IOS Software version you use is supported for QPM monitoring. Find the device support information at this URL:


**Step 1**

Select **Provisioning > Policy Management > Manage Policies > Policy View**.

The Policy View page appears.

**Step 2**

Select your policy group from the Current Policy Group list box.

The page refreshes to display the policies in the policy group, if any.

**Step 3**

Create the policy:

a. Click **Custom Policy > New Policy**.

The Policy Definition wizard appears.

b. In the Policy Definition Wizard - General Definition page, enter a name and optionally a description for the policy. For this example, the policy name is **BaselineMonitoringDemo**.

c. Click **Next**.

The Policy Definition Wizard - Constraints Definition page appears.
d. In the Policy 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—HDLC

e. Click OK to save the device constraints.
   The Policy Definition Wizard - Constraints Definition page appears.
   If you want to add other device constraints, click Define Manually and add them.
f. After you are finished defining device constraints, click Capability Report in the Policy Definition
Wizard - Constraints Definition page.
   The Policy Definition Wizard - Capabilities Report page appears, where you can view a summary
of the QoS features that can be configured for the policy, according to the device constraints.
g. In the Policy Definition Wizard, click Finish.
   The QoS Properties page appears.

Step 4 Select Class-based QoS as the QoS property for the policy:

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.

c. Click Finish again to save your changes. The QoS Properties page appears.

Step 5 Assign network elements to the policy:

a. Select Network Assignment in the TOC.
   The Network Assignment page appears.

b. In the Network Assignment page, click 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 traffic rules to classify traffic into meaningful groups.

In this example, we will create five traffic rules. The traffic rule characteristics are described in
Table 4-2.
This procedure will show you how to create the EF Traffic Rule.

Step 7 Repeat the process to create the other traffic rules.
Follow these steps to create the policies:

a. Select **Traffic Rules** in the TOC.
   - The Traffic Rule page appears.

b. In the Traffic Rules page, click **Create > In Traffic Rules**.
   - The In Traffic Rule wizard opens, displaying the In Traffic Rule Wizard - General page.

c. In the In Traffic Rule Wizard - General page:
   - Enter **EF** in the Traffic Rule Name field.
   - Click the QoS Policy radio button.

d. Click **Next**.
   - The In Traffic Rule Wizard - Traffic Classification page appears.

e. In the In Traffic Rule Wizard - Traffic Classification page:
   - Click the **Create a new traffic classifier** check box
   - Enter **EF** in the Traffic Classifier name field.

---

### Table 4-2 Baseline Monitoring Demo Policies

<table>
<thead>
<tr>
<th>Policy Order</th>
<th>Policy Name</th>
<th>Traffic Classifier</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1            | EF          | • or DSCP: ef      | Policing: 
  • Rate Limit: rate 8.0, burst 8.0, exceed 8.0. 
  • Conform action: transmit 
  • Exceed action: transmit |
| 2            | AF3         | • or DSCP: af31    | Policing: 
  • Rate Limit: rate 8.0, burst 8.0, exceed 8.0. 
  • Conform action: transmit 
  • Exceed action: transmit |
| 3            | AF2         | • or DSCP: af21    | Policing: 
  • Rate Limit: rate 8.0, burst 8.0, exceed 8.0. 
  • Conform action: transmit 
  • Exceed action: transmit |
| 4            | AF1         | • or DSCP: af11    | Policing: 
  • Rate Limit: rate 8.0, burst 8.0, exceed 8.0. 
  • Conform action: transmit 
  • Exceed action: transmit |
| 5            | BestEffort  | Class Default      | Policing: 
  • Rate Limit: rate 8.0, burst 8.0, exceed 8.0. 
  • Conform action: transmit 
  • Exceed action: transmit |
f. In the In Traffic Rule Wizard - Traffic Classification page, click Create to define a traffic classifier condition.

The Traffic Rule Settings page appears.

g. Create the traffic classifier as follows:
   - In the Traffic Rule Settings page, click Edit in the Service row of the Rule Setting table.
     The Service Editor page appears.
   - In the Service Editor dialog box, select 46 (ef).
   - Click OK to save the setting and return to the Traffic Rule Settings page.
   - In the Rule Setting page, click Done.
     The In Traffic Rule Wizard - Traffic Classification page appears.

h. In the In Traffic Rule Wizard - Traffic Classification page, click Next.

The In Traffic Rule Wizard - Marking page appears.

i. Without making a selection in the Marking page, select Policing from the TOC.

The In Traffic Rule Wizard - Policing page appears.

j. 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.

k. Click Finish.

The In Traffic Rule Wizard - Summary page appears, where you can view a summary of the traffic rule.

l. In the In Traffic Rule Wizard - Summary page, click Finish to save the policy.

The In Traffic Rules page appears.

m. Repeat the process to define the other policies.

**Step 8**

Select Provisioning > Policy Deployment > Create Job and follow the wizard to deploy the policy.

See Lesson 2-6: Deploying the Data Network Tutorial Policies, page 2-40 and Lesson 2-7: Monitoring the Deployment Process, page 2-42 for more detailed information on deploying policies and monitoring the deployment.


**Related Topics**

- Understanding How to Monitor Traffic for Baseline Analysis, page 4-4
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 classify the traffic. Step 1: Classifying Traffic for Analysis, page 4-5, describes how to create QoS policies that do not affect traffic.

Step 1: Select Monitoring > QoS Monitoring > Historical.

The Historical Monitoring page appears. This page lists all the historical monitoring tasks that you have defined.

Step 2: Click Create Task > Class Based Monitoring.

The Create Task page appears.

Step 3: On the Create Task 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 4-3 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 2008, 19:34:00 (7:34 PM), and end time is 15 September 2008, 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.

Step 4: In the object selector, select the policies under the device interfaces you want to include in this monitoring task by checking the check box next to the policy.

You can select a maximum of 12 policies altogether.

Step 5: Click Create Task.

The task is saved and the Historical Monitoring Task page appears. Your task should be added to the list.

If the status of your task is “Processing,” QPM is still analyzing your task. Select a Refresh Rate 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 4-10.
Lesson 4-1: Doing a Baseline Traffic Analysis

Chapter 4  QoS Analysis Tutorial

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.

The graph uses the last collected data values in the graph, which will appear as straight lines until the device is successfully polled.

Step 1  Go to Monitoring > QoS Monitoring > Historical.

The Historical Monitoring 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 check 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 4-1  Baseline Demo—Policies Graphs Page, Initial View
Figure 4-2 shows the matching traffic per class prior to QoS actions graph from Figure 4-1.

**Figure 4-2  Baseline Demo—Matching Traffic Per Class Prior to QoS Actions Graph**

![Graph showing matching traffic per class prior to QoS actions](image)

1. Policy AF2. This policy matches DSCP af21, af22, or af23.
2. Policy BestEffort. This is the default class policy. Any traffic not matching the other policies matches this policy.
3. 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 4-2, you can see that traffic that matches the AF2 policy’s traffic classifier 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 4-3). Policy AF3, on the other hand, accounts for almost no traffic.

**Figure 4-3  Baseline Demo—Matching Traffic Per Class Prior to QoS Actions Graph, Percentage Format**

![Graph showing percentage format](image)

If a policy has more than one traffic classifier condition, like policy AF2 in this example, you can further analyze the traffic by looking at the traffic classifier graphs. The traffic classifier graphs show how much traffic matched each traffic classifier in a policy.
To see the traffic classifier graphs, click the **Filters Graphs** button at the bottom of the page. Figure 4-4 shows the traffic classifier 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 4-4** Baseline Demo—Traffic Classifier Graph for Policy AF2

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Match IP DSCP 18 (af21)</td>
</tr>
<tr>
<td>2</td>
<td>Match IP DSCP 20 (af22)</td>
</tr>
<tr>
<td>3</td>
<td>Match IP DSCP 22 (af23)</td>
</tr>
</tbody>
</table>

The graphs also include ones that show the matching traffic after applying QoS, and the traffic that was dropped because of 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 4-12 for a detailed example of monitoring QoS.

**Related Topics**
- Understanding How to Monitor Traffic for Baseline Analysis, page 4-4

**Lesson 4-2: Monitoring QoS**

Monitoring QoS is similar to baseline monitoring, as described in Lesson 4-1: Doing a Baseline Traffic Analysis, page 4-4. 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 that can be monitored 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. See *What Can You Monitor Using QPM?*, page 4-2 for information on the types of policies and devices that can be monitored.
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 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

<table>
<thead>
<tr>
<th>Policy Order</th>
<th>Policy Name</th>
<th>Traffic Classifier</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RealTime</td>
<td>• <strong>or Protocol</strong>: UDP and destination = Ports 16384 to 32767</td>
<td>• <strong>Priority</strong>: LLQ enabled (a type of queuing)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>Bandwidth</strong>: 33% (CBQ bandwidth allocation, a type of queuing)</td>
</tr>
<tr>
<td>2</td>
<td>VoiceControl</td>
<td>• <strong>or Protocol</strong>: TCP and destination = Ports 11000 to 11999</td>
<td>• <strong>Bandwidth</strong>: 2%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>or Protocol</strong>: TCP and destination = Port 1720</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Gold</td>
<td>• <strong>or Protocol</strong>: TCP and destination = Ports 3300 to 3301</td>
<td>• <strong>Bandwidth</strong>: 25%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>or Protocol</strong>: TCP and destination = Ports 1809</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Silver</td>
<td>• <strong>or Source NBAR application</strong>: HTTP</td>
<td>• <strong>Bandwidth</strong>: 15%</td>
</tr>
<tr>
<td>5</td>
<td>BestEffort</td>
<td>Class Default</td>
<td>• <strong>Fairness</strong> (WFQ queuing enabled without specifying a number of queues)</td>
</tr>
</tbody>
</table>

**Step 1**

Go to Monitoring > QoS Monitoring > Historical, and click Create Task > Class Based Monitoring, to set up a new historical monitoring task. Step 2: Setting Up an Historical Monitoring Task, page 4-9 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 2008 12:45:00 to 16 August 2008 12:45:00 (2 day duration).
Step 2

From the Historical Monitoring page, check the check 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 4-10 explains some of the basics of reading
these graphs. This discussion assumes you have already read that information.

Since 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 4-5) and the “Matching Traffic Per Class After QoS Actions” (Figure 4-6) 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 4-7), 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 expected result for this set of policies.

Figure 4-5  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.
Since 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 4-5, 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 4-8).

**Figure 4-8**  **Zooming In On Linear Graphs**

The resulting graphs show the network activity much more clearly for this time period.

**Figure 4-9**  **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.
Step 3  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 is 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 4-12).

Bar graphs can hide variations in traffic patterns. For example, the bar graph for “Matching Traffic Per Class Prior to QoS Actions” (Figure 4-13) does not show the spikes and lolls in traffic that appear on the linear version of the graph (Figure 4-5).

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.

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 for each 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. See What Can You Monitor Using QPM?, page 4-2 for information on the types of policies and devices that can be monitored.

---

**Step 1**  Select Monitoring > QoS Monitoring > Real Time.

The Real Time Monitoring page appears.

**Step 2**  Select the interface you want to monitor (by opening the tree for Device Group and Device). For this example, the interface is Serial 1/1, an HDLC interface.

**Step 3**  Click Show Real Time Chart.

QPM opens a separate window and displays the real time chart. The 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 4-14).
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.

Task details—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.

Group folders—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.

- **Policy**—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.
- **Filters**—Contains graphs for the traffic classifiers for each policy. Each traffic classifier graph shows the matching traffic rate for each element of the traffic classifier.
- **Actions**—Contains graphs for each policy, showing the results of the policy’s actions on the traffic that met the policy’s traffic classifier conditions.

Cursor—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.

Graphed items—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 **Show Graphs** (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 4-12, you can compare these figures with the equivalent figures in that lesson.

*Figure 4-15*  
*Cat3600 HDLC Real-Time—Matching Traffic Per Class Prior to QoS Actions*

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>BestEffort</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Gold</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Silver</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>RealTime. The line for RealTime is mostly below the line for Silver. The lines occasionally cross.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>VoiceControl. This line is just above the zero line.</td>
</tr>
</tbody>
</table>
As you can see in Figure 4-17, 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 4-18).
If you have a policy with multiple traffic classifier conditions, open the Filter folder and look at the graph for the policy. QPM shows you the matching traffic for each traffic classifier condition in this graph. In this example, the Gold policy has two conditions (Figure 4-19).

**Tip**

You can rerun a real-time chart by selecting Monitor > Real Time Status > Real Time Charts, selecting the interface, and then clicking Show Real Time Chart.

**Related Topics**

- Understanding QPM Monitoring, page 4-1
### A

audience for this document vii

### B

baseline traffic analysis 4
- classifying traffic 5
- reading graphs 10
- setting up analysis task 9
- understanding 4

### C

campus access Catalyst 6000 port policy 6
- assigning elements 9
- creating ERP coloring traffic rule 9
- defining policy 6
- defining QoS properties 7

campus access VLAN policy 12
- assigning elements 14
- coloring web traffic 15
- defining 13
- policing FTP traffic 39

campus access VLAN ports policy 18
- assigning elements 21
- defining policy 18
- defining QoS properties 20

campus network QoS configuration 3
- cautions
- significance of viii

Cisco CallManager QoS configuration 12
- classifying, baseline analysis 5
- cRTP, enabling 21

### D

data network tutorial 1
- campus access Catalyst 6000 port policy 6
  - assigning elements 9
  - creating ERP coloring traffic rule 9
  - defining policy 6
  - defining QoS properties 7
- campus access VLAN policy 12
  - assigning elements 14
  - coloring web traffic 15
  - defining 13
  - policing FTP traffic 39
- campus access VLAN ports policy 18
  - assigning elements 21
  - defining policy 18
  - defining QoS properties 20
- deploying 41
- devices 3
- example network 2
- monitoring deployment 43
- remote Fast Ethernet policy 22
  - assigning elements 25
  - coloring ERP traffic 28
  - coloring web traffic 26
  - defining policy 23
  - defining QoS properties 24
- scenarios 4
- understanding 1
Index

WAN PPP policy 30
   assigning elements 33
   creating default traffic rule 37
   creating ERP queuing traffic rule 34
   creating MQC CBWFQ queuing traffic rules 34
   creating web traffic queuing traffic rule 36
   defining policy group 30
   defining QoS properties 32

deploying
   data network QoS 41
   IP telephony QoS 29

device 6
   data network tutorial 3
   importing 6
   IP telephony tutorial 4
   selecting for IP telephony configuration 9

device folder, creating 7

disk space, QoS analysis 3

documentation viii
   audience for this vii
   related to this product ix
   typographical conventions in vii

environment, understanding tutorial 1

ERP traffic
   coloring 9, 28
   MQC CBWFQ queuing traffic rule 34

example data network 2

exiting QPM 5

F

Frame Relay 19
   enabling eRTP 21
   IP telephony configuration 19

FTP traffic policing 39

G

graph 10, 12
   reading historical 12
   reading historical baseline 10

H

historical QoS monitoring report 2
   baseline traffic analysis 4
   classifying traffic, baseline 5
   QoS analysis 12
   reading baseline graphs 10
   setting up baseline analysis task 9
   space requirements 3
   understanding baseline analysis 4

I

importing virtual devices 6
IntraLAN connections, configuring QoS 14

Introduction 1

IP phone, configuring QoS 10
IP SoftPhone, configuring QoS 11

IP telephony tutorial 1
   campus site QoS 3
   Cisco CallManager configuration 12
   configuration wizard 6
   configuration wizard, using 6
   configuring bandwidth policy for data traffic 24
   deploying 29
   devices 4
   enabling eRTP 21
   end 20

IntraLAN connections 14
   introduction 8
   modifying voice policies 20
   monitoring deployment 31
   remote branch QoS 4
router WAN to switch connections 17
selecting devices 9
selecting IP phone connections 10
selecting SoftPhone connections 11
switch to WAN configuration 16
understanding 2
Voice VLAN configuration 15
WAN Frame Relay connections 19
WAN QoS 3

L
logging into QPM 2
logging out of QPM 5

M
monitor 1
   IP telephony deployment 31
   QoS analysis capabilities 2
   QoS historical analysis 12

P
policing FTP traffic 39
policy 5
   campus access Catalyst 6000 port 6
      assigning elements 9
      creating ERP coloring traffic rule 9
      defining policy 6
      defining QoS properties 7
   campus access VLAN 12
      assigning elements 14
      coloring web traffic 15
      defining policy 13
      policing FTP traffic 39
   campus access VLAN ports 18
      assigning elements 21

Q
QoS analysis tutorial 1
   baseline traffic analysis 4
   classifying traffic, baseline 5
   purpose of 1
   QoS analysis 12
   reading baseline graphs 10
   real-time analysis 19
   setting up baseline analysis task 9
   space requirements 3
   types of reports 2
   understanding 1
   understanding baseline analysis 4
   what can be monitored 2
QPM
   exiting 5
Index

getting started 2
interface, understanding 3
IP telephony wizard 6
IP telephony wizard, using 6
starting 2
understanding policy wizards 5

QoS analysis 1
understanding environment 1
typographical conventions in this document vii

U
user permission requirements 1

V
VLAN, configuring voice 15
voice policy 6
assigning using IP telephony wizard 6
configuring data policy with 24
deploying 29
enabling cRTP 21
modifying 20
monitoring deployment 31

W
WAN 3
configuring connections to switches 17
configuring QoS for connections from switches 16
Frame Relay IP telephony configuration 19
QoS configuration 3
WAN PPP policy 30
assigning elements 33
creating default traffic rule 37
creating ERP queuing traffic rule 34
creating MQC CBWFQ queuing traffic rules 34
creating web traffic queuing traffic rule 36
defining policy 30
defining QoS properties 32
web traffic 36
coloring 15, 26
MQC CBWFQ queuing traffic rule 36

S
SoftPhone, configuring QoS 11
starting QPM 2
switch 16, 17
configuring connections to WAN 16
configuring router WAN connections to 17

T
traffic rule
coloring ERP traffic 9, 28
coloring web traffic 15, 26
ERP queueing 34
MQC CBWFQ default 37
web traffic queuing 36
tutorial 1
IP telephony 1