



## CHAPTER 4

# QoS Analysis Tutorial

---

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

This can help you adjust your policy definitions to obtain the desired impact on traffic.

- [Understanding QPM Monitoring, page 4-1](#)
- [Lesson 4-1: Doing a Baseline Traffic Analysis, page 4-6](#)
- [Lesson 4-2: Monitoring QoS, page 4-19](#)
- [Lesson 4-3: Monitoring QoS in Real Time, page 4-30](#)

## 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 4-2
- [What Can You Monitor Using QPM?](#), page 4-3
- [What Is the Difference Between Historical and Real-Time Monitoring?](#), page 4-4
- [How Much Disk Space Is Required for Historical Monitoring?](#), page 4-5

## 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 4-6](#) describes how to do baseline traffic analysis.

- **QoS Analysis**—The analysis of how your QoS policies are affecting network traffic. By monitoring QoS policies, you can determine if they are affecting traffic in the desired way, or if the policies need to be adjusted. [Lesson 4-2: Monitoring QoS, page 4-19](#) describes how to do QoS analysis.
- **QoS Troubleshooting**—The real-time analysis of traffic on an interface, based on QoS policy, to help you determine if a problem you are having on an interface is related to the QoS policies that are active on the interface. [Lesson 4-3: Monitoring QoS in Real Time, page 4-30](#) 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:

[http://www.cisco.com/en/US/products/sw/cscowork/ps2064/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/sw/cscowork/ps2064/products_device_support_tables_list.html)

- 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 simply makes QPM aware of the policies. It also lets you thenceforth use QPM to modify and redistribute these policies.

If you do not already have QoS policies defined, you can use QPM to create a set of QoS policies that do not affect traffic to categorize traffic and help you establish a baseline for the traffic on your network, as described in [Lesson 4-1: Doing a Baseline Traffic Analysis, page 4-6](#).

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 4-19](#).

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

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

Real-time monitoring is best used for immediate troubleshooting. [Table 4-1](#) shows some differences between the types of monitoring.

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

Characteristic	Historical	Real-Time
Maximum number of interfaces monitored per task	20	1
Disk space requirements	Substantial. See <a href="#">How Much Disk Space Is Required for Historical Monitoring?</a> , page 4-5	No disk space used. Data is only presented on web page; it is not saved.
Polling interval for data collection	From 1 to 60 minutes.	From 10 to 30 seconds.
Length of task	Up to several months, depending on polling interval. QPM enforces a duration limit based on polling interval.  See the <i>User Guide for CiscoWorks QoS Policy Manager</i> for the specific limits.	As long as you want, but you must be at the computer to see the data.
Reuse of monitoring task	Can only be run once, because you set a start and end time.	Can be rerun any time desired, because there is no set start or end time.
Reviewing results	Can review the results as many times as you want.	Results must be reviewed as they are collected.

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

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

The same task would generate 3000KB if the polling interval was reduced to 2 minutes.

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

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

- Number of interfaces monitored—The more interfaces, the more data is collected.
- Number of policies—The policies on each interface are considered unique policies. For example, if you deploy the same five policies to ten interfaces, the total number of policies is 50, not five.
- Number of filters—Separate statistics are collected for each filter condition in a policy.
- Number and type of actions—Separate statistics are collected for each action in a policy. The amount of data also differs based on the type of action; for example, complex actions like policing (three counters) or WRED (21 counters) generate more data than simple queuing (one counter).
- Polling interval and duration—QPM collects a complete set of data during each polling interval, so the more frequent the polling interval, and the longer the task is run, the more data is collected.

Owing to the amount of data that can be generated, QPM limits the duration of tasks based on the polling interval; QPM will tell you if you select a duration too long for the polling interval. See *User Guide for CiscoWorks QoS Policy Manager* for the specific limitations.

The polling interval and duration can also affect how many concurrent tasks you can run. In general, you should run concurrent tasks on a representative sample of your WAN interfaces.

If you choose a polling period of 1 minute, you should not collect data on more than 50 interfaces. If you select longer polling periods, you can analyze more interfaces.

When you install QPM, you specify how much free disk space should be maintained for database backups.

If you leave insufficient space, monitoring tasks might use up your disk space. If this happens, all historical monitoring tasks stop and you must delete them. Thus, you should manage the disk space used by historical monitoring tasks by:

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

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

Before you develop QoS policies, you might want to analyze your existing network traffic to help you determine the types of policies from which your network might benefit.

To monitor your existing network traffic using QPM, you must first deploy QoS policies to the interfaces you want to monitor. These policies should filter traffic into meaningful groups, but they should not affect the traffic.

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

- [Understanding How to Monitor Traffic for Baseline Analysis, page 4-7](#)
- [Step 1: Filtering Traffic for Analysis, page 4-8](#)
- [Step 2: Setting Up an Historical Monitoring Task, page 4-13](#)
- [Step 3: Reading the Historical Monitoring Graphs, page 4-16](#)

## Understanding How to Monitor Traffic for Baseline Analysis

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

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

- **QoS Property for the policy**—Select Class-Based QoS for the scheduling method for the policy.
- **Filters**—Try to isolate types of traffic on your network that you will want to treat the same way.

For example, you might create a filter for applications that require real-time performance (such as voice and video), another filter for important data-intensive applications (such as database, CRM, or other ERP traffic), and another filter for traffic that is not critical to your business (such as Gnutella traffic).

Each network has its own definition of critical versus non-critical traffic, so use your knowledge of the network to filter traffic into meaningful groups.

- **Actions**—Set the Rate, Burst Size, and Exceed Burst policing rates to 8.0 Kbps. Set both the Conform and Exceed actions to Transmit. This ensures that all traffic is transmitted without the policies affecting the traffic.

### Related Topics

- [Step 1: Filtering Traffic for Analysis, page 4-8](#)
- [Understanding QPM Monitoring, page 4-1](#)

## Step 1: Filtering Traffic for Analysis

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

### Before You Begin

This step assumes you have already added devices and interfaces to QPM, and that you have created a 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 filters 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:

[http://www.cisco.com/en/US/products/sw/cscowork/ps2064/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/sw/cscowork/ps2064/products_device_support_tables_list.html)

---

**Step 1** Select **Provision > Policy Table**.

The Policy Table 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 **Create**.

The Policy Definition wizard starts.

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

- Step 4** 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.

- e. After you are finished defining device constraints, click **Next** 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.

- f. In the Policy Definition Wizard - Capabilities Report page, click **Finish**. The QoS Properties page appears.

- Step 5** 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 6** Assign network elements to the policy:
- a. Select **Assigned Network Elements** in the TOC.  
The Assigned Network Elements page appears.
  - b. In the Assigned Network Elements page, select **Add**.  
The Assignment dialog box opens.
  - c. In the Assignment dialog box, select the network elements that you want to monitor.  
  
In this example, we are selecting the single interface Serial0 on 10.51.116.154.
  - d. Click **Assign**. The dialog box closes and the selected network elements appear on the Assigned Network Elements page.
- Step 7** Create the traffic rules to filter 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. Repeat the process to create the other traffic rules.

**Table 4-2** *Baseline Monitoring Demo Policies*

Policy Order	Policy Name	Filter	Action
1	EF	<ul style="list-style-type: none"> <li>• or DSCP: ef</li> </ul>	<b>Policing:</b> <ul style="list-style-type: none"> <li>• Rate Limit: rate 8.0, burst 8.0, exceed 8.0.</li> <li>• Conform action: transmit</li> <li>• Exceed action: transmit</li> </ul>
2	AF3	<ul style="list-style-type: none"> <li>• or DSCP: af31</li> <li>• or DSCP: af32</li> <li>• or DSCP: af33</li> </ul>	<b>Policing:</b> <ul style="list-style-type: none"> <li>• Rate Limit: rate 8.0, burst 8.0, exceed 8.0.</li> <li>• Conform action: transmit</li> <li>• Exceed action: transmit</li> </ul>

Table 4-2 Baseline Monitoring Demo Policies (continued)

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

Follow these steps to create the policies:

- a. Select **In Traffic Rules** in the TOC.  
The In Traffic Rule page appears.
- b. In the In Traffic Rules page, click **Create**.  
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 Policy Name field.
  - Select the QoS Policy radio button.
 Click **Next**. The In Traffic Rule Wizard - Filter page appears.
- d. In the In Traffic Rule Wizard - Filter page:
  - Select **Create a new filter**.
  - Enter **EF** in the Filter name field.

- e. In the In Traffic Rule Wizard - Filter page, click **Create** to define a filter condition.

The Rule Settings page appears. Create the filter as follows:

- In the Rule Settings page, click **Edit** in the Service row of the Rule Setting table. The Service Editor dialog box opens.
- In the Service Editor dialog box, select **46 (ef)**. Click **OK** to save the setting and return to the Rule Settings page.
- In the Rule Setting page, click **Done**. The In Traffic Rule Wizard - Filter page appears.

- f. In the In Traffic Rule Wizard - Filter page, click **Next**.

The In Traffic Rule Wizard - Marking page appears.

- g. Without making a selection in the Marking page, select **Policing** from the TOC.

The In Traffic Rule Wizard - Policing page appears. Make these selections to define the policing policy:

- Select **Enable Policing**.
- Enter **8** in the Rate, Burst Size, and Exceed Burst fields.
- Select **Transmit** in both the Conform Action and Exceed Action fields.

- h. Click **Finish**.

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

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

The In Traffic Rules page appears.

- j. Repeat the process to define the other policies.

**Step 8** Select **Provision > Policy Deployment > Create Job** and follow the wizard to deploy the policy.

See [Lesson 2-6: Deploying the Data Network Tutorial Policies, page 2-64](#) and [Lesson 2-7: Monitoring the Deployment Process, page 2-66](#) for more detailed information on deploying policies and monitoring the deployment.

Proceed with [Step 2: Setting Up an Historical Monitoring Task, page 4-13](#).

### Related Topics

- [Understanding How to Monitor Traffic for Baseline Analysis, page 4-7](#)

## Step 2: Setting Up an Historical Monitoring Task

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

### Before You Begin

You must use QPM to deploy policies to an interface before you can use QPM to monitor the interface. The policies you deploy do not have to affect the traffic, they just have to filter the traffic.

[Step 1: Filtering Traffic for Analysis, page 4-8](#), describes how to create QoS policies that do not affect traffic.

---

#### Step 1 Select **Monitor > Historical Trends**.

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

#### Step 2 Click **Create**.

The Monitoring Task Wizard starts at Step 1, Task Definition.

#### Step 3 On the Monitoring Task Wizard - Task Definition page, fill in these fields to define the historical monitoring task:

- **Name**—A name you find meaningful.  
For this example, the name is **Baseline remote demo**.
- **Polling Interval**—How often you want to collect data from the devices. The more frequent you poll the devices, the more effect the monitoring task might have on device performance.

Also, the more frequent you poll the devices, the larger amount of data will be collected (thus filling up your disk space). See [How Much Disk Space Is Required for Historical Monitoring?, page 4-5](#) 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 2007, 19:34:00 (7:34 PM), and end time is 15 September 2007, 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** When you are finished defining the task, click **Next**.

The Monitoring Task Wizard - Select Devices page appears.

**Step 5** On the Monitoring Task Wizard - Select Devices page, select each device you want to include in this monitoring task by checking the box next to the device.

Keep in mind that each monitoring task can have a maximum of 12 interfaces, so do not select more devices than you can use in this task.

**Step 6** When you are finished selecting devices, click **Next**.

The Monitoring Task Wizard - Select Interfaces page appears.

**Step 7** On the Monitoring Task Wizard - Select Interfaces page, select the interfaces you want to include in the monitoring task. You can select a maximum of 12 interfaces.

**Step 8** When you are finished selecting interfaces, click **Next**.

The Monitoring Task Wizard - Select Policies page appears.

**Step 9** On the Monitoring Task Wizard - Select Policies page, select the policies you want to include in the monitoring task.

To select all policies, you can check the box in the table heading.

**Step 10** When you are finished selecting policies, click **Next**.

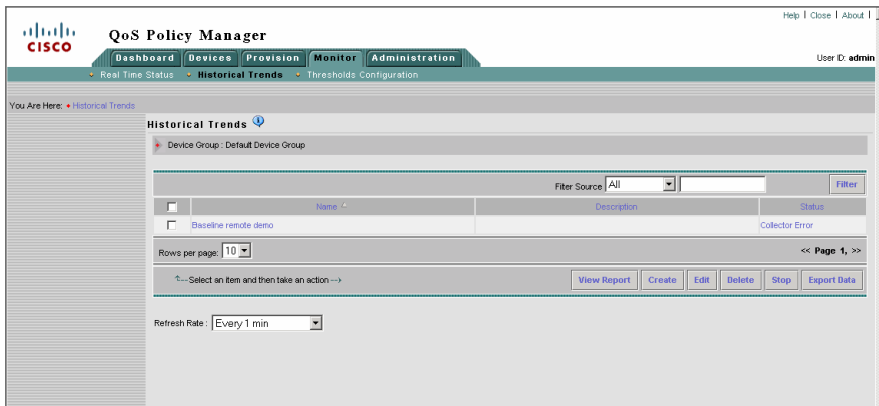
The Monitoring Task Wizard - Summary page appears.

**Step 11** On the Monitoring Task Wizard - Summary page, review your task settings. If you want to make changes, click the links in the TOC to go to the page in the wizard that you want to change.

**Step 12** When you are satisfied with the task definition, click **Finish**.

The task is saved and the Historical Monitoring Task page appears (Figure 4-1). Your task should be added to the list.

**Figure 4-1** Lesson 4-1, Step 2, Historical Monitoring Tasks Page After Defining Task



If the status of your task is “Processing,” QPM is still analyzing your task. Select **Monitor > Historical Trends** 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 4-16](#).

### Related Topics

- [Understanding How to Monitor Traffic for Baseline Analysis, page 4-7](#)

## 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.

If a device is not successfully polled (for example, when a device is unreachable), a red triangle appears along the X axis at the point where the device data could not be collected.

The graph uses the last collected data values in the graph, which will appear as straight lines until the device is successfully polled. For bar graphs, a red triangle indicates there was at least one unsuccessful polling period in the bar.

---

### Step 1 Select **Monitor > Historical Trends**.

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

### Step 2 Select the task you want to view by checking the box next to the task. For this example, the task is **Baseline remote demo**.

### Step 3 Click **View Report**.

The Policies Graphs page appears ([Figure 4-2](#)).

Figure 4-2 Baseline Demo—Policies Graphs Page, Initial View



Figure 4-3 shows the matching traffic per class prior to QoS actions graph from Figure 4-2.

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

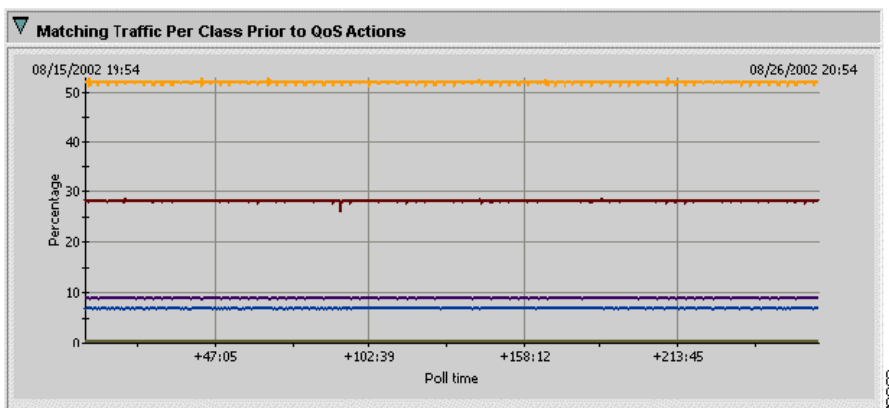


1	Policy AF2. This policy matches DSCP af 21, af22, or af23.
2	Policy BestEffort. This is the default class policy. Any traffic not matching the other policies matches this policy.
3	Policy EF. This policy matches DSCP ef.
4	Policy AF1. This policy matches DSCP af11, af12, or af13.
5	Policy AF3. This policy matches DSCP af31, af32, or af33.

From the information in [Figure 4-3](#), you can see that traffic that matches the AF2 policy's filter consumes approximately 1050 Kbps of the interface's bandwidth.

If you select **Percentage** from the Vertical Axis list box, you can see that this is approximately 52% of the interface's bandwidth ([Figure 4-4](#)). Policy AF3, on the other hand, accounts for almost no traffic.

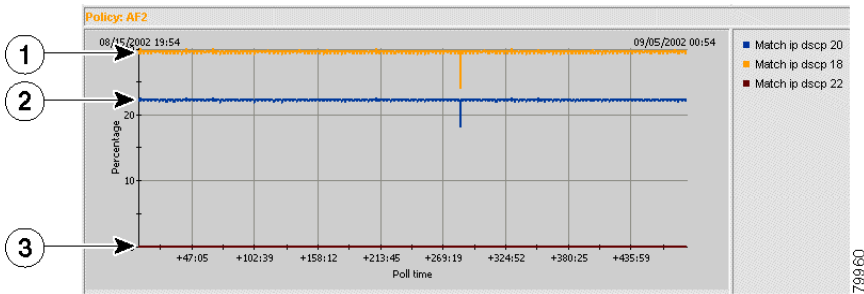
**Figure 4-4** *Baseline Demo—Matching Traffic Per Class Prior to QoS Actions Graph, Percentage Format*



If a policy has more than one filter condition, like policy AF2 in this example, you can further analyze the traffic by looking at the filter graphs. The filter graphs show how much traffic matched each filter in a policy.

To see the filter graphs, click the **Filters Graphs** button at the bottom of the page. [Figure 4-5](#) shows the filter graph for policy AF2. In this case, no traffic matched DSCP 22 (af23). DSCP 20 (af22) used approximately 22% of the bandwidth; DSCP 18 (af21) used approximately 30%.

**Figure 4-5** Baseline Demo—Filter Graph for Policy AF2



1	Match IP DSCP 18 (af21)
2	Match IP DSCP 20 (af22)
3	Match IP DSCP 22 (af23)

The graphs also include ones that show the matching traffic after applying QoS, and the traffic that was dropped due to QoS action. However, because this is a baseline traffic analysis, the QoS policies do not affect traffic, so these graphs do not contain interesting information.

After you apply QoS policies that do affect traffic, you can monitor how the policies affect the traffic using the same techniques discussed in this section. Proceed with [Lesson 4-2: Monitoring QoS, page 4-19](#) for a detailed example of monitoring QoS.

### Related Topics

- [Understanding How to Monitor Traffic for Baseline Analysis, page 4-7](#)

## Lesson 4-2: Monitoring QoS

Monitoring QoS is similar to baseline monitoring, as described in [Lesson 4-1: Doing a Baseline Traffic Analysis, page 4-6](#). 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 4-3 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

Policy Order	Policy Name	Filter	Action
1	RealTime	<ul style="list-style-type: none"> <li>or <b>Protocol:</b> UDP and destination = Ports 16384 to 32767</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Priority:</b> LLQ enabled (a type of queuing)</li> <li>• <b>Bandwidth:</b> 33% (CBQ bandwidth allocation, a type of queuing)</li> </ul>
2	VoiceControl	<ul style="list-style-type: none"> <li>• or <b>Protocol:</b> TCP and destination = Ports 11000 to 11999</li> <li>• or <b>Protocol:</b> TCP and destination = Port 1720</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bandwidth:</b> 2%</li> </ul>
3	Gold	<ul style="list-style-type: none"> <li>• or <b>Protocol:</b> TCP and destination = Ports 3300 to 3301</li> <li>• or <b>Protocol:</b> TCP and destination = Ports 1809</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bandwidth:</b> 25%</li> </ul>
4	Silver	<ul style="list-style-type: none"> <li>• or <b>Source NBAR application:</b> HTTP</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bandwidth:</b> 15%</li> </ul>
5	BestEffort	Class Default	<ul style="list-style-type: none"> <li>• <b>Fairness</b> (WFQ queuing enabled without specifying a number of queues)</li> </ul>

**Step 1** Select **Monitor > Historical Trends**, and click **Create**, to set up a new historical monitoring task. [Step 2: Setting Up an Historical Monitoring Task, page 4-13](#) 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 2007 12:45:00 to 16 August 2007 12:45:00 (2 day duration).

- **Device and Interface**—10.51.116.60 Serial 1/1.
- **Policies**—All policies described in [Table 4-3](#).

After the task has run long enough to poll the device at least 3 times (and at minimum one hour has passed), you can view the task and start analyzing the graphs.

**Step 2** From the Historical Trends page (**Monitor > Historical Trends**), check the box next to the task and click **View Report**.

The Policies Graphs page appears and shows the graphs of the data collected by the task.

**Step 3: Reading the Historical Monitoring Graphs, page 4-16** explains some of the basics of reading these graphs. This discussion assumes you have already read that information.

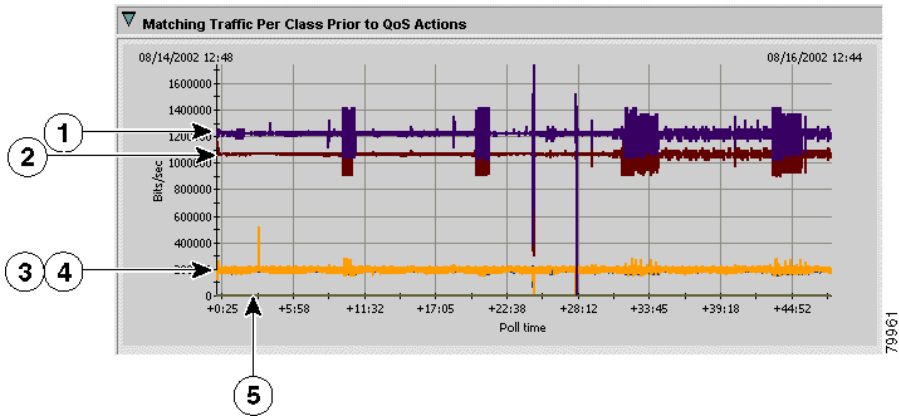
Because this monitoring task is monitoring QoS policies that are intended to affect the network traffic on the interface, you should see a difference between the “Matching Traffic Per Class Prior to QoS Actions” ([Figure 4-6](#)) and the “Matching Traffic Per Class After QoS Actions” ([Figure 4-7](#)) graphs.

In this example, notice that traffic matching the BestEffort policy (number 1 in the figures) is approximately 1200 Kbps before QoS actions (roughly 60% of the interface’s bandwidth), but only 600 Kbps after QoS actions.

If you open the “Matching Traffic Per Class Discarded by QoS Drop Actions” graph ([Figure 4-8](#)), you can see that roughly 600 Kbps of BestEffort traffic is being dropped.

Also note that there is some Silver traffic dropping, but that no RealTime, VoiceControl, or Gold traffic is dropped. This is exactly the desired result for this set of policies.

**Figure 4-6** *MonDemoTask—Matching Traffic Per Class Prior to QoS Actions*



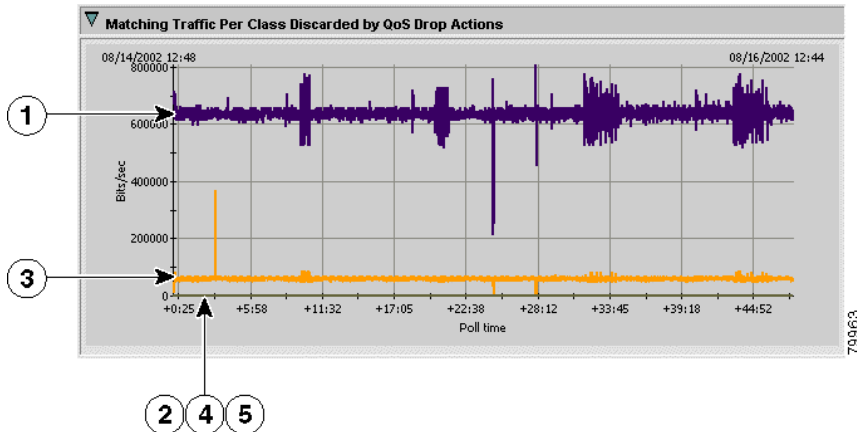
1	BestEffort
2	Gold
3	Silver
4	RealTime. The line for RealTime is behind the line for Silver.
5	VoiceControl. This line is just above the zero line.

Figure 4-7 MonDemoTask—Matching Traffic Per Class After QoS Actions



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl

**Figure 4-8** *MonDemoTask—Matching Traffic Per Class Discarded by QoS Drop Actions*



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl. Gold, VoiceControl, and RealTime overlap and are all 0 (no dropped traffic.)

Because linear graphs display all collected data points, the lines can be difficult to read if you are trying to analyze a portion of the data. To get a clearer view, you can zoom in on a specific time period.

For example, in [Figure 4-6](#), you can see some significant spikes approximately 25 hours into the task.

To zoom in on the first spike, modify the From Time and To Time fields to approximate this period, and click **Apply**. In this case, change the From Time to 08/15/2002 13:20:00 and the To Time to 08/15/2002 13:50:00 ([Figure 4-9](#)).

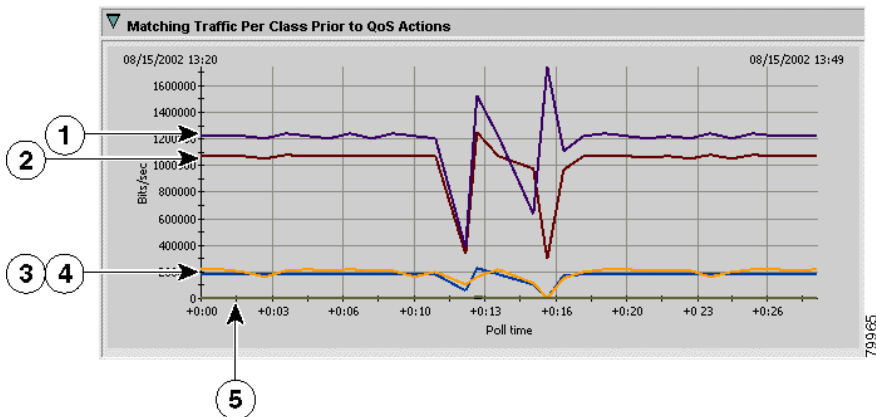
Figure 4-9 Zooming In On Linear Graphs

From time: 08/15/2002 13:20

To time: 08/15/2002 13:50

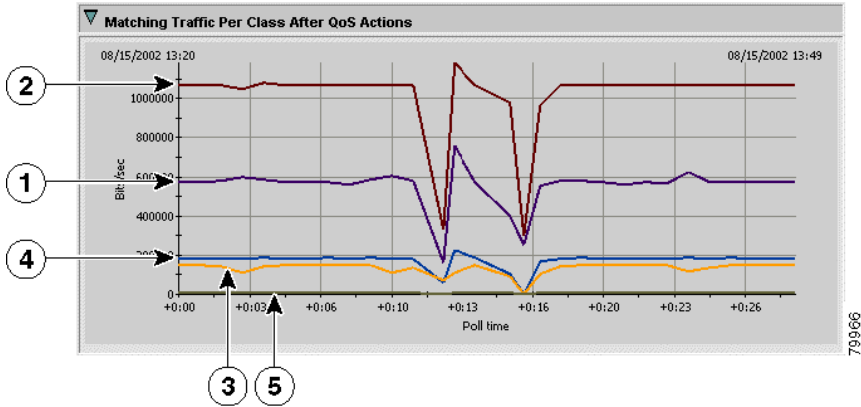
79964

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

Figure 4-10 *MonDemoTask—Matching Traffic Per Class Prior to QoS Actions (After Zoom)*

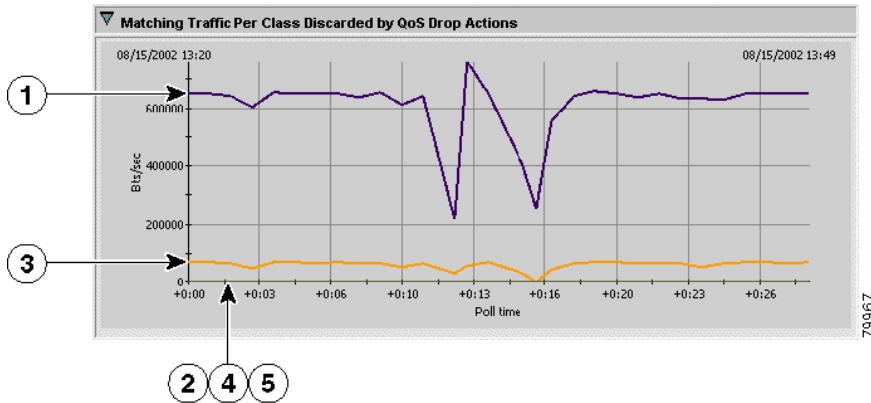
1	BestEffort
2	Gold
3	Silver
4	RealTime. The line for RealTime is mostly below the line for Silver. The lines occasionally cross.
5	VoiceControl. This line is just above the zero line.

**Figure 4-11** *MonDemoTask—Matching Traffic Per Class After QoS Actions (After Zoom)*



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl

**Figure 4-12** *MonDemoTask—Matching Traffic Per Class Discarded by QoS Drop Actions (After Zoom)*



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl. Gold, VoiceControl, and RealTime overlap and are all 0 (no dropped traffic.)

**Step 3** To get a simplified view of the network traffic, you can select Bar for **Graph Type** to see bar graphs.

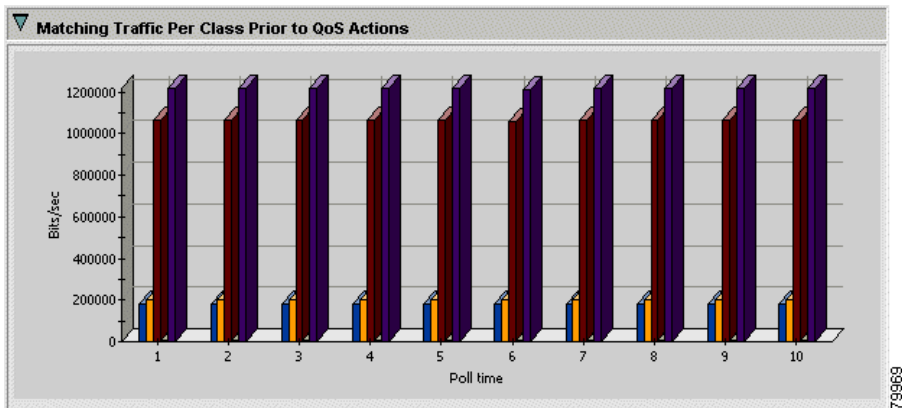
Unlike linear graphs, bar graphs do not show every data point collected. Instead, bar graphs show 10 data points, each one an average of the data collected over one tenth of the task's duration. The collection periods are shown in the lower right of the Policies Graphs page ([Figure 4-13](#)).

**Figure 4-13** *Periods for Bar Graph Data Points*

Graphs X-axis Values	
Poll Time	Time From - Time To
1	08/14/2002 12:48--08/14/2002 17:36
2	08/14/2002 17:37--08/14/2002 22:23
3	08/14/2002 22:24--08/15/2002 03:10
4	08/15/2002 03:11--08/15/2002 07:58
5	08/15/2002 07:59--08/15/2002 12:47
6	08/15/2002 12:48--08/15/2002 17:36
7	08/15/2002 17:37--08/15/2002 22:25
8	08/15/2002 22:26--08/16/2002 03:13
9	08/16/2002 03:14--08/16/2002 08:00
10	08/16/2002 08:02--08/16/2002 12:44

Bar graphs can hide variations in traffic patterns. For example, the bar graph for “Matching Traffic Per Class Prior to QoS Actions” (Figure 4-14) does not show the spikes and lolls in traffic that appear on the linear version of the graph (Figure 4-6).

On the other hand, bar graphs clearly show each traffic class, because bars cannot overlap like lines. These types of graphs can help you see broader traffic patterns, and can be useful for presentations.

**Figure 4-14** *Bar Graph for Matching Traffic Per Class Prior to QoS Actions*

**Related Topics**

- [Understanding QPM Monitoring, page 4-1](#)

## Lesson 4-3: Monitoring QoS in Real Time

This lesson describes how to set up and use a real-time monitoring task. Real-time monitoring is useful for troubleshooting an interface. If there seems to be a problem on an interface, you can monitor it to determine if there is a problem with the QoS policies.

With real-time monitoring, you can only monitor one interface per task. However, you can start more than one task to view multiple interfaces.

**Before You Begin**

You must use QPM to create QoS policies on an interface before you can use QPM to monitor the interface. Because you can only monitor real devices, this lesson uses devices on a Cisco test network as an example of how to set up and view a real-time monitoring task.

When following this lesson, use devices and interfaces that reside on your own network. Only devices and interfaces you have defined in QPM are available for selection when you create a monitoring task.

See [What Can You Monitor Using QPM?, page 4-3](#) for information on the types of policies and devices that can be monitored.

---

**Step 1** Select **Monitor > Real Time Status > Real Time Charts**.

The Real Time Charts page appears.

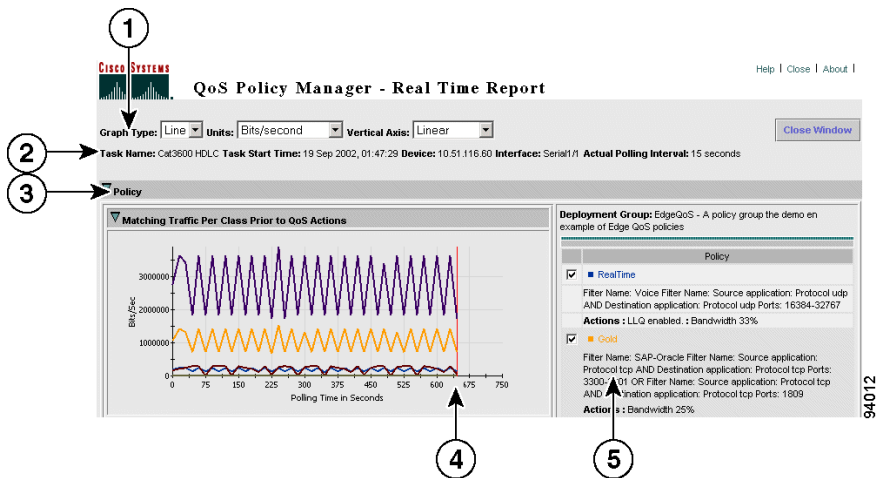
**Step 2** Select the interface you want to monitor (by opening the tree for Device Group and Device). For this example, the interface is Serial 1/1, an HDLC interface.

**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 4-15](#)).

Figure 4-15 Real-Time Demo—Real-Time Report Page, Initial View



## 1 Customization controls—Fields that let you change how the data is displayed:

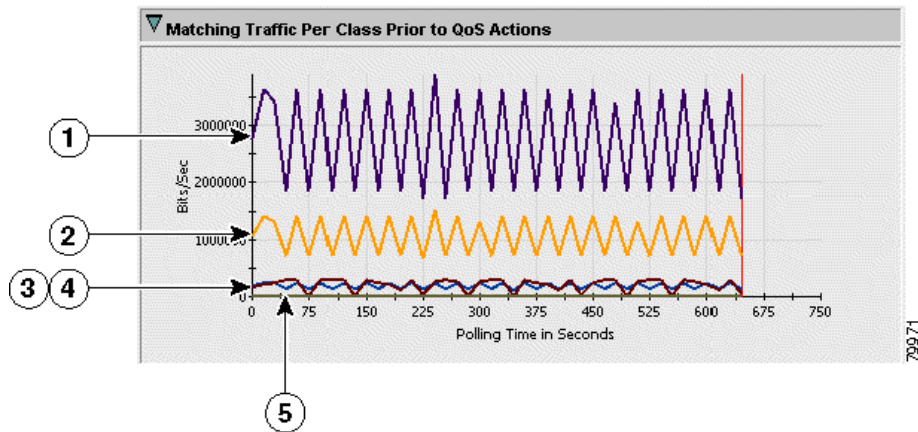
- **Graph Type**—Whether the graph is linear or bar. All data points are graphed, but fewer data points fit on the graph if you are using a bar graph. Thus, with bar graphs, data points will be overwritten more frequently than in linear graphs.
- **Units**—The unit of measure for the graph, either bits per second or packets per second.
- **Vertical Axis**—The scale used for the vertical axis: linear keeps the scale constant; logarithmic reduces the distance between numbers as the numbers get larger; and percentage shows the scale as the percentage of the available bandwidth.

## 2 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.

- 
- 3 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 filters for each policy. Each filter graph shows the matching traffic rate for each element of the filter.
  - **Actions**—Contains graphs for each policy, showing the results of the policy's actions on the traffic that met the policy's filter conditions.
- 
- 4 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.
- 
- 5 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.
- 

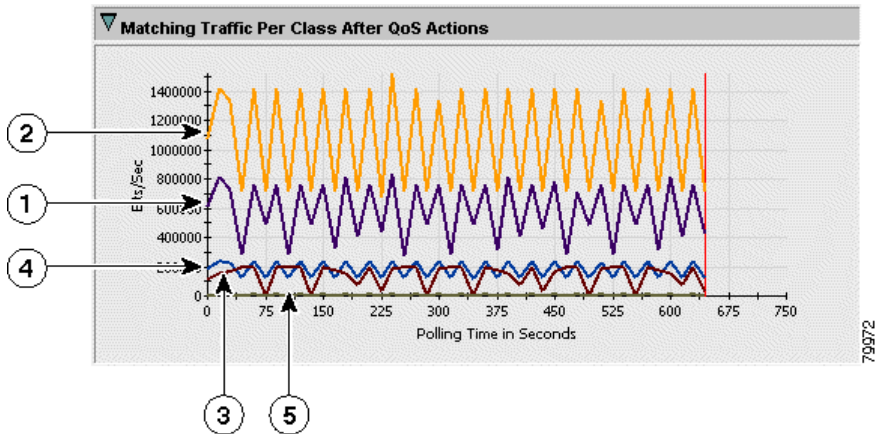
The following figures show examples of the real-time report for this interface. Because it is the same interface used in [Lesson 4-2: Monitoring QoS, page 4-19](#), you can compare these figures with the equivalent figures in that lesson.

**Figure 4-16** *Cat3600 HDLC Real-Time—Matching Traffic Per Class Prior to QoS Actions*



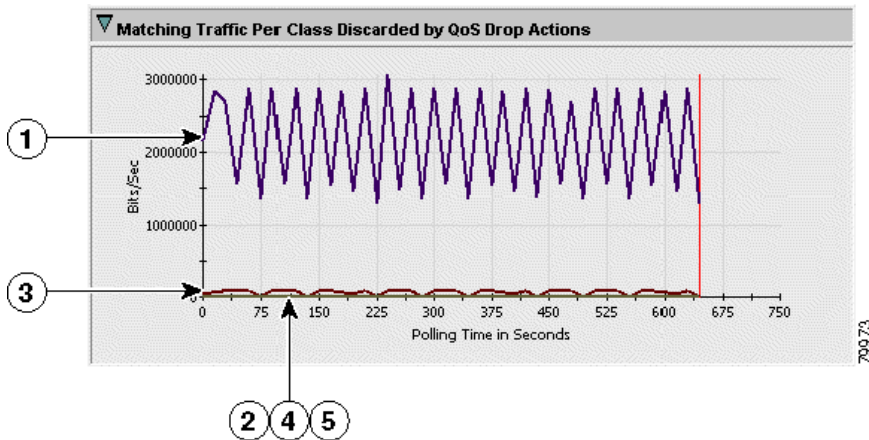
1	BestEffort
2	Gold
3	Silver
4	RealTime. The line for RealTime is mostly below the line for Silver. The lines occasionally cross.
5	VoiceControl. This line is just above the zero line.

**Figure 4-17** *Cat3600 HDLC Real-Time—Matching Traffic Per Class After QoS Actions*



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl

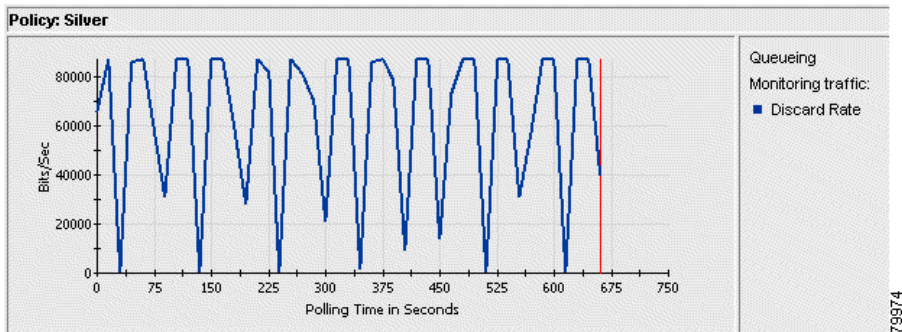
**Figure 4-18** *Cat3600 HDLC Real-Time—Matching Traffic Per Class Discarded by QoS Drop Actions*



1	BestEffort
2	Gold
3	Silver
4	RealTime
5	VoiceControl. Gold, VoiceControl, and RealTime overlap and are all 0 (no dropped traffic.)

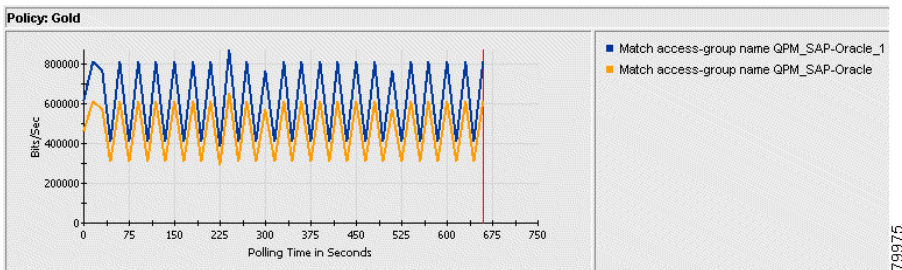
As you can see in [Figure 4-18](#), the discard rate for Silver traffic is close to zero. To get a clearer view of the discard rate, open the Action folder and look at the Silver policy ([Figure 4-19](#)).

**Figure 4-19** *Cat3600 HDLC Real-Time—Action Graph for Silver Policy*



If you have a policy with multiple filter conditions, open the Filter folder and look at the graph for the policy. QPM shows you the matching traffic for each filter condition in this graph. In this example, the Gold policy has two conditions (Figure 4-20).

**Figure 4-20** *Cat3600 HDLC Real-Time—Filter Graph for Gold Policy*



**Step 4** Click **Close Window** to close the Real-Time Report window and end the task.

### Tips

- 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](#)