CHAPTER 10

Monitoring: Using QoS Analysis

QPM allows you to obtain a baseline traffic profile of your network and analyze the effect of QoS on the network.

The following topics describe how to use QPM performance analysis:

Understanding QoS Analysis

QPM allows you to perform the following analysis of your network's traffic:

- You can perform a baseline analysis to determine how traffic is flowing on the network, and also to discover the protocols present in the traffic. For more information, see Performing Baseline QoS Analysis, page 10-4.
- You can analyze the effect of QoS on the network. You can use this information to assess the effectiveness of the QoS and plan policy changes. For more information, see Understanding the Types of QoS Analysis, page 10-2.

For information about monitoring QoS that you configured without using QPM, see Performing Historical QoS Analysis, page 10-5.

If you add interfaces to a device that has network elements that are being monitored (by running a historical monitoring task, or by running a real-time monitoring report, or by running a threshold monitoring task), you must rediscover the device.

If you do not rediscover the device, the monitoring application will not be able to poll monitoring data for the device interfaces, resulting in an application error. For information about rediscovering devices, see Rediscovering Device Information, page 4-12.

The following topics provide more overview information about using QPM QoS analysis:

Understanding the Types of QoS Analysis

There are three types of QoS analysis in QPM:

- Historical analysis monitors traffic for the QPM policies you select on one or more interfaces, polling on a regular basis and storing the gathered data.

  Historical monitoring jobs gather data between a start time and end time that you define. All of the gathered data can be displayed in historical monitoring reports.

  You would typically use historical monitoring as an operations tool. It is useful for monitoring the performance of your network's QoS configuration on an ongoing basis, over a period of time.

- Real-time analysis monitors traffic for all QPM policies on one interface continuously, in real time. No historical data is stored.

  You would typically use real-time monitoring for immediately viewing the effects of QoS change, troubleshooting QoS problems, or investigating new QoS configurations in a lab environment.

- Threshold Analysis monitors traffic based on the Threshold Sets assigned to a device interface.

  You would typically use threshold monitoring to assign high and low level thresholds (for each class based metric) for the traffic through the interface, and monitor them for threshold violations.

Related Topics

- Performing Historical QoS Analysis, page 10-5
- Performing Real Time Chart Analysis, page 10-16
- Preparing for Threshold Analysis, page 10-17
- Performing Event Browser Threshold Analysis, page 10-25

Understanding What QPM Monitors

QPM monitors protocols, class-based QoS, CAR QoS, and Port QoS policies (both parent policy and child policy) on devices running specific Cisco IOS software versions. When you create a QoS analysis task, QPM only lets you select device interfaces that have supported Cisco IOS software versions and supported QoS policy types.

Note these points while creating QoS analysis tasks; this information can also help you decide what types of policies to define on interfaces you want to monitor.

- See the QPM device support information for a detailed list of devices and Cisco IOS Software versions that are supported for QoS analysis. Select the device support page for your version of QPM at this URL:

  http://www.cisco.com/en/US/products/sw/cscowork/ps2064/products_device_support_tables_list.html

- QPM uses the information collected in the Class Based QoS MIB and in the CAR MIB. Features that are not supported by the Class Based QoS MIB or the CAR MIB cannot be monitored.

  For example, the CAR MIB does not include DSCP information, so policies with the DSCP option cannot be monitored.

- QPM uses the Cisco Port QoS MIB to provide monitoring capabilities for each port. This feature enables you to monitor catalyst switches that have the Cisco Port QoS MIB.

  Port QoS MIB allows you to monitor and display traffic for matching DSCP values, matching CoS values, and dropped traffic. It also lets you police the traffic for each port.

- An interface will have Class Based QoS MIB information if you define the QoS scheduling property for the interface as Class based QoS. In addition, only the policies on the interface are 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.
- An interface will have CAR MIB information if you define the QoS scheduling property as Default, and define policing policies on the interface. Only policing policies are monitored.
- If you define WRED as a policy action, only IP precedence-based WRED can be monitored; if you use DSCP-based WRED, you will not be able to monitor WRED on the interface.
- QPM does not monitor network elements that are assigned to a policy configured with Modular Shaping.
- If you define a policy on the interface using the device's CLI commands, and add the device to the QPM device inventory, QPM can monitor the device using Independent QoS Monitoring feature. This means, you need not deploy a policy created in QPM on to the device to be monitored, if the device already has monitorable policies attached (outside QPM).
- If the device to be monitored has no monitorable policies attached, you can create policies in QPM, and attach the same to the device.
- If you make changes in the device configuration, you can rediscover the device in QPM, and continue monitoring the device.

Both historical and real-time QoS monitoring reports display the same types of QoS monitoring data. Each QoS monitoring report contains graphs of the following types of QoS monitoring data:

- The amount of traffic that matched the policy's traffic classifiers (before QoS), the amount of matching traffic that was dropped by QoS, and the amount of matching traffic that was transmitted (after QoS).

  This information provides a general view of the efficiency of queued traffic through an interface. For example, you can see how much traffic has been dropped, and whether, on average, the classes of traffic are using the bandwidth allocated to them efficiently.

  See the following topics for more detailed information:

  – Policies Graphs: Matching and Dropped Traffic for Policies Page, page D-11
  – Real Time Charts Window for Class Based Monitoring, page D-3
- A breakdown of the traffic that matched each of the policy's traffic classifiers.

  This information allows you to see how traffic within each class is distributed among its match statements. This enables you to analyze your traffic by application. For example, you can see if traffic from one application is using too much of the bandwidth allocated to its traffic class.

  See the following topics for more detailed information:

  – Filters Graphs: Matching Traffic for Filter Conditions Page, page D-13
  – Real Time Charts Window for Class Based Monitoring, page D-3
- The amount of traffic to which QoS actions were applied because of the policy's QoS configuration, broken out by the following types of QoS features:

  – Queuing
  – WRED
  – Policing
  – Traffic shaping

  If the only action is marking or CAR, there are no action graphs.

See the following topics for more detailed information:

- Actions Graphs: Policy Actions on Matching Traffic Page, page D-15
- Real Time Charts Window for Class Based Monitoring, page D-3

Performing Baseline QoS Analysis

To determine how to deploy QoS on a network, it is helpful to perform a baseline analysis of the network's traffic flow. A baseline QoS analysis shows you how the important traffic classes on your network are flowing. You can use this information to design QoS that better meets the needs of your network.

Baseline QoS analysis is part of the larger QoS workflow that you should use to ensure the effectiveness of the QoS on your network on an ongoing basis. For more information, see Planning for QoS Deployment, page 2-1.

In summary, you use QPM QoS analysis to perform a baseline traffic analysis by deploying QoS policies that identify the important traffic classes on your network without performing any QoS actions that affect traffic flow. The purpose of this is to identify the traffic and initiate data collection. Then you can view QoS analysis reports that show traffic throughput for identified applications or classes.

You can perform a baseline QoS analysis using either historical or real-time QoS analysis. For information about determining which type of QoS analysis to use, see Understanding the Types of QoS Analysis, page 10-2.

Selecting Traffic Classes

Baseline QoS analysis works when you identify 12 or fewer traffic classes to monitor. Each traffic class can contain one or more traffic types (for example, voice classes, SAP, Oracle, or web traffic), so you should group the important applications running on your network into meaningful classes.

Note QPM 4.1 does not allow you to monitor more than 12 interfaces during baseline QoS analysis.

The QoS monitoring reports show network activity only at the class level. You can view the breakdown of the traffic types within a class, only if there are any policy traffic classifier rules defined for that class.

Applying QoS Policies To Enable Baseline Traffic Analysis

After you have identified your traffic classes, you can create QPM policies that mark the classes without taking any QoS actions that affect traffic flow. The following QoS settings are ideal for this:

- QoS feature: Policing.
- Set conformed, exceeded, and violated actions to transmit.
- Do not configure an excess rate.

For information about creating policies, see Provisioning: Working with Policies, Properties, and Traffic Rules.

Related Topics

- Planning for QoS Deployment, page 2-1
- Provisioning: Working with Policies, Properties, and Traffic Rules

Performing Historical QoS Analysis

To monitor policies, you create a QoS monitoring task. Each historical monitoring task has a corresponding report that you can view.

You will not see data on the historical graphs immediately after the task starts. Depending on when you start the task, the length of the polling interval, and how many other tasks are being run concurrently, it can take several hours to see graphed data. This is because of the way in which QPM collects the data and writes it to the QPM database.

To see any data in the graphs, your task must include at least three polling periods. For example, if you use a polling period of 30 minutes, and run the task for only one hour, you will not see any graphed data for the task. If you need to see data immediately, as it is collected, use real-time monitoring.

You define the traffic to be monitored by specifying the interfaces and policies (both parent policy and child policy) to be monitored. Each historical QoS analysis task can monitor a maximum of 20 interfaces, a maximum of 20 policies on each interface, and a maximum of 20 match statements per policy traffic classifier.

You specify when each task starts and ends, and the polling interval. The duration limits for historical monitoring tasks depend on the polling interval, as shown in Table 10-1.

Table 10-1 Historical Monitoring Task Duration Limits

Polling Interval (Min)	Maximum Task Duration (Days)
1	1
5	5
10	10
15	30
20	40
25	50
30	90
60	180

Note When viewing a historical analysis report, you can select the time period of data that is displayed. This lets you zoom in on selected parts of the graphs.

The amount of time required to load a report into the Analysis Report page depends on the amount of data collected, and can take from half a minute to several minutes.

Historical QoS analysis data is stored with all the QPM data, on the QPM server. If you run out of available disk space for collecting historical QoS analysis data, all current tasks are automatically stopped.

- If you make changes using QPM to a QoS feature that QPM is monitoring, running historical monitoring tasks that are monitoring the QoS feature stop when you deploy the changes. All data collected up to the time of the change is preserved. To continue monitoring the QoS feature that you changed, you must create new monitoring tasks.

- If you remove a device that contains network elements that are being monitored by a historical monitoring task, QPM continues to monitor these network elements. To stop QPM from monitoring these network elements, you must stop or delete the historical monitoring task.

  If the historical monitoring task was monitoring other network elements that you want to continue to monitor, you must create a new historical monitoring task to monitor those network elements, because you cannot edit a historical monitoring task.

The following topics describe historical QoS analysis:

- Defining a Class-based Historical Monitoring Task, page 10-6
- Defining a VLAN Monitoring Task, page 10-8
- Defining a Port-QoS Historical Monitoring Task, page 10-9
- Defining an NBAR PD Monitoring Task, page 10-10
- Editing Historical Monitoring Tasks, page 10-11
- Deleting Historical Monitoring Tasks, page 10-12
- Stopping Historical Monitoring Tasks, page 10-13
- Viewing Historical QoS Monitoring Reports, page 10-13
- Exporting Historical Monitoring Data, page 10-14
- Customizing Historical Monitoring Reports, page 10-15

Related Topics

- Understanding QoS Analysis, page 10-1

Defining a Class-based Historical Monitoring Task

Define a class-based historical monitoring task to begin monitoring traffic for policies (both parent policy and child policy) on one or more interfaces. The collected data is stored and used in historical monitoring reports.

Before You Begin

QoS analysis operates within the context of the active device group. For more information, see Setting the Active Device Group, page 4-22. This has the following effects:

- When creating a QoS monitoring task, you can select only devices that belong to the active device group.
- The Monitoring Tasks page displays the tasks that monitor the network elements, which belong to the active device group.

To define a historical monitoring task:

Step 1 Choose **Monitoring > Historical Monitoring**.

The Monitoring Tasks page appears.

Step 2 Choose **Create Task > Class Based Monitoring**.

The Create Task window opens.

Step 3 Do the following in the Create Task window:

a. Enter a task name in the Name field.

b. Select a polling interval from the Polling Interval (min) list box.

The polling interval is the period of time (in minutes) between each collection of the monitored data.

c. Enter a start date and time and an end date and time in the Start Time and End Time fields.

You can enter each date directly into the field (in the format mm/dd/yyyy), or you can click the calendar button and use the popup calendar that appears. You should enter the time in a 24 hour format.

If the duration of the task is longer than the limit for the specified polling interval (see Table 10-1), an error message appears, displaying the duration limit in days.

d. Select the Job Frequency of the monitoring task. You can select daily, weekly, bi-weekly, or monthly schedules.

e. Check the **Enabled** check box to enable the task. If you do not, the task will not run.

Optionally, you can enter a comment or description for the task in the Enter a comment or description field.

f. Check the check box next to the policies (both parent policy and child policy) that appear when you expand the tree of device group, device, and interfaces that you want to monitor.

QPM lists only those devices that contain interfaces on which you have defined QoS policies that QPM can monitor.

However, do not select more than 20 interfaces.

By default, in a single historical monitoring task, you should not select more than 20 policies (sum of parent and child policies) per interface, or should not select policies with more than 20 match statements per policy traffic classifier.

If you want to monitor more policies in a single historical monitoring task, you can change the variable ‘MonPolicyLimit’ that appears in the file called qpm.cfg under CSCOpx/MDC/qpm.

We recommend that you create a backup copy of the existing qpm.cfg file before making the changes.

To change ‘MonPolicyLimit’:

a. Open qpm.cfg in a Notepad.

b. Edit the line that contains MonPolicyLimit=20. You can replace the default value of 20 to any other value.

c. Save this file after ensuring the saved filename is qpm.cfg.

You should restart QPM after you change the value of MonPolicyLimit.

QPM recommends the maximum value of 20 for MonPolicyLimit so that the graphs generated from the Historical Monitoring Task are easy to infer.

g. Click **Create**.

The Monitoring Tasks page appears with the new task displayed in the task list.

Related Topics

- Performing Historical QoS Analysis, page 10-5
- Viewing Historical QoS Monitoring Reports, page 10-13
- Historical Monitoring Page, page D-8
- Troubleshooting QoS Analysis Problems, page 14-10

Defining a VLAN Monitoring Task

QPM supports monitoring of VLAN interfaces that are based on CBQoS MIB. QPM supports both real time and historical monitoring jobs for VLAN interfaces.

Before You Begin

QoS analysis operates within the context of the active device group. For more information, see Setting the Active Device Group, page 4-22. Note the following:

- While creating a QoS monitoring task, you can select only devices that belong to the active device group.
- The Monitoring Tasks page displays the tasks that monitor the network elements. These tasks belong to the active device group.

To define a VLAN historical monitoring task:

Step 1 Choose **Monitoring > Historical Monitoring**.

The Monitoring Tasks page appears.

Step 2 Choose **Create Task > Class Based Monitoring**.

The Create Task window opens.

Step 3 Do the following in the Create Task window:

a. Enter a task name in the Name field.

b. Select a polling interval from the Polling Interval (min) list box.

The polling interval is the period of time (in minutes) between each collection of the monitored data.

c. Enter the Start and End dates and times in the Start Time and End Time fields.

You can enter the dates (in the format mm/dd/yyyy), or click the Calendar button and select the dates from the popup calendar. Enter the time in a 24 hour format.

If the duration of the task is longer than the limit for the specified polling interval (see Table 10-1), an error message appears, displaying the duration limit in days.

d. Select the Job Frequency of the monitoring task. You can select daily, weekly, bi-weekly, or monthly schedules.

e. Check the **Enabled** check box to enable the task. If you do not do this, the task will not run.

Optionally, you can enter a comment or description for the task in the Enter a Comment or Description field.

f. Expand the device group tree and select the VLAN interfaces that appear under each device that you want to monitor.

A list of Parent and Child policies that are attached to each VLAN interface appear.

g. Select the check box next to the policies that are attached to the VLAN interfaces (both Parent policy and Child policy).

h. Click **Create**.

The Monitoring Tasks page appears with the new task displayed in the task list.

If you are upgrading from QPM 4.1 to QPM 4.1.1, you cannot view the VLAN interfaces of the existing devices. You can view the VLAN interfaces only after rediscovering the existing devices or after adding new devices.

Note You can also monitor VLAN interfaces based on CBQoS MIB in real time.

Related Topics

Performing Real Time Chart Analysis, page 10-16

Viewing Historical QoS Monitoring Reports, page 10-13

Defining a Port-QoS Historical Monitoring Task

Define a port-QoS historical monitoring task to begin monitoring traffic for policies on one or more interfaces. The collected data is stored and used in port-QoS historical monitoring reports.

Before You Begin

QoS monitoring operates within the context of the active device group. For more information, see Setting the Active Device Group, page 4-22. This has the following effects:

- When creating a QoS monitoring task, you can select only devices that belong to the active device group.
- The Monitoring Tasks page displays the tasks that monitor the network elements, which belong to the active device group.

To define a port-QoS historical monitoring task:

Step 1 Choose **Monitoring > Historical Monitoring**.

The Monitoring Tasks page appears.

Step 2 Choose **Create Task > Port QoS Monitoring**.

The Create Task window opens.

Step 3 Do the following in the Create Task window:

a. Enter a task name in the Name field.

b. Select a polling interval from the Polling Interval (minutes) list box.

The polling interval is the period of time (in minutes) between each collection of the monitored data.

c. Enter a start date and time and an end date and time in the Start Time and End Time fields.

You can enter each date directly into the field (in the format mm/dd/yyyy), or you can click the calendar button and use the popup calendar that appears. You should enter the time in a 24 hour format.

If the duration of the task is longer than the limit for the specified polling interval (see Table 10-1), an error message appears, displaying the duration limit in days.

d. Select the Job Frequency of the monitoring task. You can select daily, weekly, bi-weekly, or monthly schedules.

e. Check the **Enabled** check box to enable the task. If you do not, the task will not run.

Optionally, you can enter a comment or description for the task in the Enter a comment or description field.

f. Select the check box next to the policies that appear when you expand the tree of device group, device, and interfaces that you want to monitor.

QPM lists only those devices that support port-QoS monitoring.

Note You should have configured the SNMP RW Community string for the device for it to appear in this tree.

Do not select more than 20 interfaces.

g. Click **Create**.

The Monitoring Tasks page appears with the new task displayed in the task list.

Defining an NBAR PD Monitoring Task

NBAR PD (Protocol Discovery) provides an easy way of discovering the application protocols that are operating on an interface so that appropriate quality of service (QoS) features can be applied. With Protocol Discovery, you can discover any protocol traffic that is supported by NBAR and obtain statistics that are associated with that protocol.

Protocol Discovery maintains the following statistics for enabled interfaces for each protocol:

- Total number of input packets and bytes
- Total number of output packets and bytes
- Input bit rates
- Output bit rates

The statistics can then be used when you later define traffic policies.

In QPM, you can define an NBAR PD historical monitoring task to start monitoring the protocols in inbound and outbound traffic through the interfaces. The collected data is stored and used in NBAR PD historical monitoring reports.

Before You Begin

QoS monitoring operates within the context of the active device group. For more information, see Setting the Active Device Group, page 4-22. Note the following:

- When creating a QoS monitoring task, you can select only devices that belong to the active device group.
- The Monitoring Tasks page displays the tasks that monitor the network elements, which belong to the active device group.

To define an NBAR PD historical monitoring task:

Step 1 Choose **Monitoring > Baseline Monitoring > Historical Monitoring**.

The Monitoring Tasks page appears.

Step 2 Click **Create**.

The Create Task window opens.

Step 3 Do the following in the Create Task window:

a. Enter a task name in the Name field.

b. Select a polling interval from the Polling Interval (minutes) list box.

The polling interval is the period of time (in minutes) between each collection of the monitored data.

c. Enter a start date and time and an end date and time in the Start Time and End Time fields.

You can enter each date directly into the field (in the format mm/dd/yyyy), or you can click the calendar button and use the popup calendar that appears. You should enter the time in a 24 hour format.

If the duration of the task is longer than the limit for the specified polling interval (see Table 10-1), an error message appears, displaying the duration limit in days.

d. Select the Job Frequency of the monitoring task. You can select daily, weekly, bi-weekly, or monthly schedules.

e. Check the Enabled check box to enable the task. If you do not, the task will not run.

Optionally, you can enter a comment or description for the task in the Enter a comment or description field.

f. Check the check box next to the policies that appear when you expand the tree of device group, device, and interfaces that you want to monitor.

QPM lists only those devices that support NBAR PD monitoring.

Note You should have configured the SNMP RW Community string for the device for it to appear in this tree.

Do not select more than 20 interfaces.

g. Click **Create**.

The Monitoring Tasks page appears with the new task displayed in the task list.

Editing Historical Monitoring Tasks

You can edit tasks that have not completed running and have the following status displayed in the Status column of the Monitoring Tasks page:

- In Edit
- Collector Error

After a task has started running normally or has finished running, you cannot edit it.

To edit a historical monitoring Task:

Step 1 Choose **Monitoring > Historical Monitoring**.

The Monitoring Tasks page appears.

Step 2 Select a task from the list, then click **Edit**.

The Monitoring Task Wizard starts.

Step 3 Edit any of the task parameters using the Monitoring Task wizard, as described in Defining a Class-based Historical Monitoring Task, page 10-6.

Related Topics

- Performing Historical QoS Analysis, page 10-5
- Viewing Historical QoS Monitoring Reports, page 10-13

Deleting Historical Monitoring Tasks

You can delete historical monitoring tasks that you no longer want to use. When you delete a task, all historical data collected by that task is deleted.

To delete a historical monitoring task:

Step 1 Choose **Monitoring > Historical Monitoring**.

The Monitoring Tasks page appears.

Step 2 Select a task from the list, then click **Delete**.

Step 3 Confirm the deletion when prompted.

Related Topics

- Performing Historical QoS Analysis, page 10-5

Stopping Historical Monitoring Tasks

You can stop a running task. You cannot restart or edit a stopped task, so the primary use of this feature is to stop tasks that have collected sufficient data, but are still running.

To stop a historical monitoring task:

Step 1 Choose **Monitoring > Historical Monitoring**.

The Monitoring Tasks page appears.

Step 2 Select a task from the list, then click **Stop**.

Step 3 Confirm that you want to stop the task when you are prompted.

The task's state changes to Stopped. Within an hour, the status will convert to Finished.

Related Topics

- Performing Historical QoS Analysis, page 10-5

Viewing Historical QoS Monitoring Reports

You will not see data on the historical graphs immediately after the task starts. Depending on when you start the task, the length of the polling interval, and how many other tasks are being run concurrently, it can take several hours to see graphed data. This is because of how QPM collects the data and writes it to the QPM database.

To see any data in the graphs, your task must include at least three polling periods.

For example, if you use a polling period of 30 minutes, and run the task for only one hour, you will not see any graphed data for the task. If you need to see data immediately, as it is collected, use real-time monitoring.

To view a historical monitoring report:

Step 1 Choose **Monitoring > Historical Monitoring**.

The Monitoring Tasks page appears.

Step 2 Select a task from the list, then click **View Report**.

The Analysis Report page appears. For information about this report, see Policies Graphs: Matching and Dropped Traffic for Policies Page, page D-11.

Related Topics

- Performing Historical QoS Analysis, page 10-5
- Customizing Historical Monitoring Reports, page 10-15
- Troubleshooting QoS Analysis Problems, page 14-10

Exporting Historical Monitoring Data

You can export the data gathered by an historical monitoring task to a zip file on your client system. The zip file contains a set of XML files grouped by interface. You can use these files to import the data to another application for analysis.

If you export the data from a task that has not run or did not run successfully, the resulting file will contain only variable names, without the variable definitions that result from running the task.

If a device was unreachable during a polling period, the number shown for the data points is -1.0.

Export File Format

The export file is in XML format. It contains the data collected by a historical monitoring task, which is separated into the following sections:

- Policy Data—This section contains traffic flow data about all of the traffic monitored by the task. This section contains the following columns:
  - TimeStamp

    The time at which each sample was taken. The first column of the entire file contains timestamps, which are used to correlate the data in the sections of the file.
  - Per Class Traffic Discarded by All QoS Drop Actions Bits/sec

    The rate, in bits per second, that data was dropped due to QoS actions, since the previous sample.
  - Per Class Traffic Discarded by All QoS Drop Actions Packets/sec

    The rate, in packets per second, that data was dropped due to QoS actions, since the previous sample.
  - Matching Traffic Per Class After QoS Actions Bits/sec

    The rate, in bits per second, that data was transmitted after QoS was applied, since the previous sample.
  - Matching Traffic Per Class After QoS Actions Packets/sec

    The rate, in packets per second, that data was transmitted after QoS was applied, since the previous sample.
  - Per Class Prior to QoS Actions Bits/sec

    The rate, in bits per second, that data matched the policy's traffic classifiers before taking any QoS actions, since the previous sample.
  - Per Class Prior to QoS Actions Packets/sec

    The rate, in packets per second, that data matched the policy's traffic classifiers before taking any QoS actions, since the previous sample.
- Filter Data—This section contains a set of data for each traffic classifier monitored by the task. Each set of data contains the following columns:
  - TimeStamp

    The time at which each sample was taken. The first column of the entire file contains timestamps, which are used to correlate the data in the sections of the file.
  - Matching Traffic Bits/sec

    The rate, in bits per second, that data matched the traffic classifier, since the previous sample.
  - Matching Traffic Packets/sec

The rate, in packets per second, that data matched the traffic classifier, since the previous sample.

- Actions—This section contains a set of data for each QoS action monitored by the task. The columns differ depending on the type of QoS action, but the first column is the time at which each sample was taken.

To export a historical monitoring data:

Step 1 Choose **Monitoring > Historical Monitoring**.

The Historical Trends page appears.

Step 2 Select a report from the list, then click **Export Data**.

A dialog box appears stating that the operation might take a few minutes.

Step 3 Click **OK**.

The browser file download process begins.

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

To view the exported files, unzip them so that the unzip process recreates the directory structure for the files. If the files are not unzipped into the correct directory structure, you will have problems viewing them.

In the directory structure, each interface has its own folder. Within the interface's folder, there are separate files for each policy defined on the interface.

Customizing Historical Monitoring Reports

Each historical QoS analysis report has the same customization controls that you can use to customize how the analysis data is presented in the report.

The types of customization you can perform include:

- Displaying the graphs in line or bar format.
- Selecting the graph units of measure.
- Selecting the scale of the graph vertical axis.
- Selecting to organize the graphs by policy or by interface.
- Selecting the time period of data to display.
- Selecting which policies or interfaces to display.

View a historical QoS analysis report as described in Viewing Historical QoS Monitoring Reports, page 10-13. Use the customization controls available in each historical reports page. See the following for more information:

- Policies Graphs: Matching and Dropped Traffic for Policies Page, page D-11
- Filters Graphs: Matching Traffic for Filter Conditions Page, page D-13
- Actions Graphs: Policy Actions on Matching Traffic Page, page D-15

Related Topics

- Performing Historical QoS Analysis, page 10-5
- Viewing Historical QoS Monitoring Reports, page 10-13

Performing QoS Report Card Analysis

The QoS Report Card provides you the real time details of each device in the device group that has been configured in QPM. You can view the most latest report regarding the policies (both parent policy and child policy) that are assigned (or being assigned) to a device (or its interfaces).

Before You Begin

QoS Report Card operates within the context of the active device group. For more information, see Setting the Active Device Group, page 4-22. When monitoring QoS, only devices that belong to the active device group are available for selection.

To view the QoS Report Card in real time:

Step 1 Choose **Monitoring > QoS Report Card**.

Step 2 Select the device for which you want to view the real time QoS report.

The QoS report card appears in the content area.

Related Topics

- QoS Report Card Page, page D-1

Performing Real Time Chart Analysis

To analyze the effect of QoS in real time, you can make use of real time charts. You define the traffic to be monitored by specifying the device interface. All policies configured on the interface are monitored.

Data collection occurs only while the task is running, and no historical data is saved.

Before You Begin

QoS analysis operates within the context of the active device group. For more information, see Setting the Active Device Group, page 4-22. This has the following effects:

- When monitoring QoS, only devices that belong to the active device group are available to select.
- The QoS analysis task lists (historical and real time) only display tasks that monitor network elements that belong to the active device group.
- QPM allows you to monitor both class-based and port-QoS policies.

To view real time charts:

Step 1 Choose **Monitoring > Real Time Monitoring** and select a device interface from the Select Device Interface pane

Step 2 Click **Show Real Time Chart**.

The Real Time Charts page is displayed.

Real time monitoring will only monitor up to 20 policies (sum of parent and child policies) for each interface. If an interface has more than 20 QoS policies defined on it, only 20 are shown.

- If you make changes using QPM to a QoS feature that QPM is monitoring, running a real time QoS analysis task will stop collecting data when you deploy the changes. Close and rerun the real time monitoring task.
- If you remove a device that contains a network element that is being monitored by a running real time QoS analysis task, you can stop QPM from monitoring this network element by just closing the Real Time Charts page for that network element.

Related Topics

- Real Time Monitoring Page, page D-2

Preparing for Threshold Analysis

The monitoring of devices using threshold analysis requires you to have a basic understanding of Cisco Class-Based QoS MIB, and the associated objects.

This section guides you through the basics of Cisco Class-Based QoS MIB, and its relationship with QPM.

For more details about Cisco Class-Based QoS MIB, go to the url http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&mibName=CISCO-CLASS-BASED-QOS-MIB

The following sections describe some basics about the MIB:

- Cisco Class-Based QoS MIB, page 10-17
- QoS Objects, page 10-18
- Runtime Instance vs Configuration Instance, page 10-18
- Navigation, page 10-19
- cbQosPolicyTable, page 10-19
- cbQosObjectsTable, page 10-19
- Understanding the Relationship between Objects, page 10-19
- CbQosCMStatsEntry, page 10-20

Cisco Class-Based QoS MIB

Cisco Class-Based QoS MIB provides read access to Quality of Service (QoS) configuration and statistics information for Cisco platforms that support the Modular Quality of Service Command-line Interface (Modular QoS CLI).

Configuration information available through this MIB includes all ClassMap, PolicyMap, Match Statements, and Feature Actions configuration parameters.

The definitions of each objects mentioned above are explained in the QoS objects section.

Statistics available through this MIB include summary counts/rates by traffic class before and after any configured QoS policies are enforced. In addition, detailed feature-specific statistics are available for select PolicyMap features.

A logical interface in the context of this MIB is either a main-interface, a sub-interface, a Frame Relay DLCI, or an ATM virtual circuit.

QoS Objects

To understand Class-Based QoS features and how to navigate the MIB tables above, the key element is to comprehend the relationships among the different QoS objects. QoS objects consist of ClassMaps, Match Statements and PolicyMaps, and each Feature Actions.

- Match Statement

  The specific match criteria to identify packets for classification purposes.

- ClassMap

  A user-defined traffic class that contains one or many match statements used to classify packets into different categories.

- Feature Action

  An action is a QoS feature. Features include police, traffic-shaping, queueing, random detect and packet marking (set). After the traffic is being classified, based on the traffic classification, we can apply these action to each traffic class.

- PolicyMap

  A user-defined policy that associates each QoS action to the user-defined traffic class (ClassMap).

- Service Policy

  Service policy is a policymap that is being attached to a logical interface. Because a policymap can also be a part of the hierarchical structure (inside a classmap), only a policymap that is directly attached to a logical interface is considered a service policy.

  Each service policy is uniquely identified by an index called cbQosPolicyIndex. This number is usually identical to its cbQosObjectsIndex as a policymap.

Runtime Instance vs Configuration Instance

Each QoS object has two sets of behaviors :

- Configuration instance

  Each QoS objects has it's configuration portion of information attached to it. This information does not change whether this object is attached on multiple interfaces and used multiple times. We uniquely identify each QoS object with identical configuration with the same index - cbQosConfigIndex. This index is used in all configuration related tables.

- Runtime instance

  Each QoS objects has it's statistical portion of information attached to it. This information changes when this object is attached on multiple interfaces and used in various different places. We uniquely identify each QoS runtime object instance with an index that is unique across multiple instances of the identical object - cbQosObjectsIndex. This index is used in all statistical related tables.

In summary, a QoS object has 2 indexes associated with it:

- cbQosConfigIndex

  Identifies its configuration. This does not change regardless of number of times and where it is being used

- cbQosObjectsIndex

  Identifies its runtime statistics. Depending on which interface and where in a given PolicyMap hierarchy this object is used, it may have multiple unique identifiers to distinguish each unique usage (instance) of the same object.

Navigation

The recommended method of navigating through all of the MIB tables is to start by learning the cbQosPolicyTable and cbQosObjectsTable MIB tables.

We recommend that you understand the cbQosObjectsIndex and cbQosParentObjectsIndex of each QoS feature.

The cbQosPolicyIndex and cbQosObjectsIndex are system-assigned numbers that identify each unique instance of a QoS feature. These indexes are never reused between router reboots, even when changes are made to the QoS configuration.

The cbQosPolicyIndex is designed to identify the service policies attached to logical interfaces, while the cbQosObjectsIndex is designed to identify each QoS feature on a specified device.

The cbQosParentObjectsIndex is designed to show the hierarchical relationship of each QoS feature.

cbQosPolicyTable

Accessing cbQosPolicyTable requires cbQosPolicyIndex. This index is a system-assigned number to uniquely identify each service policy hanging off of each logical interface.

Given cbQosPolicyIndex, the tables provide the type of interface/media type on which this policy is applied, the direction in which this policy is enforced, and the cbQosIfIndex (SNMP interface index) of the underlying interface.

- If a policy being applied on a Frame Relay DLCI, the cbQosFrDLCI gives you the Frame Relay DLCI number to which this policy is attached.
- If a policy being attached to an ATM VC, cbQosAtmVPI and cbQosAtmVCI display the VPI and VCI of the ATM interface respectively.

cbQosObjectsTable

Accessing cbQosObjectsTable requires two indexes, cbQosPolicyIndex and cbQosObjectsIndex.

In a particular service policy on a given interface, there are PolicyMaps, ClassMaps, Match Statements, and Feature Actions. Each instance of these objects is uniquely identified by cbQosObjectsIndex.

You need to decide which QoS object is needed and use the cbQosPolicyIndex and cbQosObjectsIndex to locate that QoS object .

Understanding the Relationship between Objects

To understand the relationship of cbQosObjectsIndex, cbQosParentObjectsIndex and the hierarchical relationship of the QoS objects, go to the url http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&mibName=CISCO-CLASS-BASED-QOS-MIB.

CbQosCMStatsEntry

QPM uses some objects in CbQosCMStatsEntry table to specify ClassMap related Statistical information. Each entry in this table describes the statistical information about ClassMap. ClassMap specific information you can find in this table are:

- Pre/Post policy pkt/byte counts,
- Bit rates
- Drop pkt/bytes
- Buffer drops.

This table contains statistical information only, no configuration information associated with it. Therefore, it is indexed by the instance specific IDs, such as cbQosPolicyIndex and cbQosObjectsIndex.

For more details, go to:
http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&mibName=CISCO-CLASS-BASED-QOS-MIB.

Threshold Sets and MIBs in QPM

To perform threshold analysis of the traffic flowing through an interface, you need to configure Threshold Sets in QPM and assign them to the interface.

Threshold Sets contain class based QoS metrics from CbQosCMStatsEntry table, with a high and a low watermark value defined for each metric.

Note QPM contains a Default Threshold Set, which you cannot modify. You can add and configure new Threshold Sets.

Table 10-2 describes the cbQoS MIBs from the CbQosCMStatsEntry table, used in QPM. You can set the metrics for each MIB, for the corresponding Threshold Set.

Table 10-2 MIBs in Threshold Sets page

MIBs in Threshold Sets page	Description
cbQosCMPrePolicyPkt64	The 64 bits count of inbound packets before running any QoS policies. This metric is a counter.
cbQosCMDropPkt64	The 64 bits counter of dropped packets for each class as the result of all Traffic Rule/Class Map features that can produce drops. For example, policing, random detection, and so on. This metric is a counter.
cbQosCMDropByte64	The 64 bits counter of dropped bytes for each class as the result of all Traffic Rule/Class Map features that can produce drops. For example, policing, random detection, and so on). This metric is a counter.
cbQosCMDropBitRate	The bit rate (in bits per second) of the drops for each class as the result of all Traffic Rule/Class Map features that can produce drops. For example, policing, random detection, and so on. This metric is a gauge.

Table 10-2 MIBs in Threshold Sets page

MIBs in Threshold Sets page	Description
cbQosCMPostPolicyByte64	The 64 bits count of outbound octets after running QoS policies. This metric is a counter.
cbQosCMPrePolicyBitRate	The bit rate (in bits per second) of the traffic before running any QoS policies. This metric is a gauge.
cbQosCMPrePolicyByte64	The 64 bits count of inbound octets before running any QoS policies. This metric is a counter.
cbQosCMPostPolicyBitRate	The bit rate (in bits per second) of the traffic after running QoS policies. This metric is a gauge.
cbQosCMNoBufDropPkt64	The 64 bits drop packet count that occurred because the SRAM buffers were not available during output processing on an interface. This metric is a counter.

To create Threshold Sets:

Step 1 Go to **Monitoring > Threshold Configuration > Threshold Sets**.

The Threshold Sets page appears.

Step 2 Enter a name for the new Threshold Set, and click **Clone**.

To populate threshold sets with high and low water mark values for each metric:

Step 1 Choose **Monitoring > Threshold Configuration > Threshold Sets.**

Step 2 Select a Threshold Set from the Threshold Set pane.

Step 3 Enter values corresponding to each CBQoS metric, for High Water Mark and Low Water Mark.

Step 4 Click **Save**

Related Topics

- Threshold Sets Page, page D-19

Assigning Threshold Sets to Interfaces

You can assign the threshold sets to the traffic flow of the selected device interfaces, through the Threshold Assignment page. QPM stores these threshold assignments as jobs, which you can see under Pending Jobs page or Completed Jobs page.

To assign Threshold Sets to interfaces:

Step 1 Choose **Monitoring > Threshold Configuration > Threshold Assignment**.

The Threshold Assignment page appears.

Step 2 Select the Threshold Set and the traffic flow (inward or outward) of the device interfaces, in the corresponding panes.

Step 3 Select the Class Map Metric type (Object Name or OID).

Step 4 Click **Assign**.

Step 5 Enter a job name for the threshold assignment.

The selected Threshold Set is assigned to the device interfaces.

To remove the selected Threshold Set from a device interface:

Step 1 Choose **Monitoring > Threshold Configuration > Threshold Assignment**.

The Threshold Assignment page appears.

Step 2 Select the Threshold Set and the traffic flow (inward or outward) of the device interface, in the corresponding panes.

Step 3 Select the Class Map Metric type (Object Name or OID).

Step 4 Click **Unassign** to remove the threshold configuration.

Related Topics

- Threshold Assignment Page, page D-20
- Pending Jobs Page, page D-21
- Completed Jobs Page, page D-22
- Threshold Job Details Page, page D-23
- Threshold Errors and Warnings Page, page D-24
- Threshold Deployment History Page, page D-25

Viewing the Assignment Status

You can view the status of the threshold assignment job using the Active Jobs page. The Active Jobs page provides a dynamic view of all the active assignments and their status.

For each threshold assignment job, the start time of its configuration, its status, and a summary of the number of devices assigned according to their status, are displayed.

The status of a job assignment or a device assignment might be Pending, In Progress, Completed, or Failed. A job might also have the status of Aborted or Paused.

During the threshold assignment process, an In Progress status will be displayed for a job. When the job is completed successfully, its status will change to Completed.

For an assignment job to be Completed, all the devices must be successfully configured. If the assignment of at least one device fails, and all the other devices passed without errors, the overall status of the assignment is Failed.

Completed jobs are automatically removed from the display after ten minutes.

From the Active Jobs page, you can:

- View the assignment details of a job.
- Pause and resume the assignment process.
- Stop the assignment.
- Redeploy a failed assignment.
- Remove an assignment job from the display.

To view the assignment status:

Step 1 Choose **Monitoring > Thresholds Configuration > Pending Jobs**.

The Active Jobs page appears, displaying the currently active threshold assignment jobs and their status, in a table.

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

For more information about the Active Jobs page, see Pending Jobs Page, page D-21.

Step 2 View the status of the active job assignments:

- To view the details of a threshold assignment job, select its Job Name link in the table. The Job Details report appears.
- To remove a deployment job from the table, select it and click **Remove From Display**.

Related Topics

- Pausing and Resuming a Threshold Assignment Job, page 10-23
- Stopping a Threshold Assignment Job, page 10-24
- Redeploying a Threshold Assignment Job, page 10-24

Pausing and Resuming a Threshold Assignment Job

You can pause a job during the threshold assignment. However, QPM will not stop the configuration of a device after it has begun. Any devices that are being configured when the Pause command is issued will be finished.

Devices for which assignment had not yet begun will remain with the status Pending. You can also cause any paused assignment to resume configuration of devices. This does not create a new job. Instead, it continues the selected job.

To pause and resume a threshold assignment job:

Step 1 Choose **Monitoring > Thresholds Configuration > Pending Jobs**.

The Active Jobs page appears.

Step 2 In the Active Jobs list, check the check box next to your assignment job and click **Pause**.

A message appears asking you if you are sure you want to pause the assignment of your job.

Step 3 Click **Yes** to pause the assignment of your job.

To resume the assignment of your job, check the check box next to the job and click **Resume**.

The assignment of the selected job resumes.

Related Topics

- Viewing the Assignment Status, page 10-22

Stopping a Threshold Assignment Job

You can stop a threshold assignment job that is currently in progress or has been paused. This feature is useful if you want to change a job's configuration details before assigning it, or if a job hangs.

Terminating a job stops the configuration of the devices. All the devices that were In Progress or Pending will receive a Failed status. You cannot resume a stopped assignment job.

To stop a threshold assignment job:

Step 1 Choose **Monitoring > Thresholds Configuration > Pending Jobs**.

The Active Jobs page appears.

Step 2 In the Active Jobs list, check the check box next to the assignment job (In Progress or Pending) that you want to stop, and click **Abort**.

A message appears warning you that the job will be terminated with no option to resume it.

Step 3 Click **Yes** to confirm the stop procedure.

The selected assignment job will be terminated.

Related Topics

- Viewing the Assignment Status, page 10-22

Redeploying a Threshold Assignment Job

You can manually request that threshold assignment be retried for either a specific device that failed or all failed devices in any displayed failed job. This does not create a new job. Instead, it creates another assignment for the job.

The redeployment process resets the status of the selected devices and re-requests the assignment of the selected job.

To redeploy a threshold assignment job:

Step 1 Choose **Monitoring > Thresholds Configuration > Pending Jobs**.

The Active Jobs page appears.

Step 2 In the Active Jobs table, check the check box next to the job you want to redeploy and click **Redeploy**.

Related Topics

- Pending Jobs Page, page D-21

Performing Event Browser Threshold Analysis

QPM provides you with real time event browsers that help you to analyze the network traffic for threshold violations. You can generate reports of these snapshot events or live events, and export them as a csv or pdf file.

Before You Begin

QoS analysis operates within the context of the active device group. For more information, see Setting the Active Device Group, page 4-22. This has the following effects:

- When monitoring QoS, only devices that belong to the active device group are available to select.
- The QoS analysis task lists (historical and real time) only display tasks that monitor network elements that belong to the active device group.

To perform a snapshot event analysis:

Step 1 Choose **Monitoring > Event Browser > Snapshot**.

The Snapshot Event Browser Properties page opens.

Step 2 Select a device from the Devices pane, specify the start time and end time for the event.

Step 3 Click **Submit**.

The Snapshot Event Browser page opens.

To perform a live event analysis:

Step 1 Choose **Monitoring > Event Browser > Live**.

The Live Event Browser Properties page appears.

Step 2 Select a device from the Devices pane, specify the maximum events (which need to be shown) and the Refresh Rate.

Step 3 Click **Submit.**

The Live Event Browser page opens.

- If you make changes using QPM to a QoS feature that QPM is monitoring, running a real time QoS analysis task will stop collecting data when you deploy the changes.

  Close and rerun the real time monitoring task.

- If you remove a device that contains a network element that is being monitored by a running real time QoS analysis task, QPM continues to monitor this network element.

  To stop QPM from monitoring this network element, you must stop running the real time QoS analysis task.

Related Topics

- Historical Event Browser Page, page D-26
- Live Event Browser Page, page D-29