APPENDIX D

Monitoring Drawer Reference

The following topics describe the pages that are accessed from the Monitoring tab:

QoS Report Card Page

Use this page to view the details about a device, the interfaces contained in the device, and the policies (both parent policy and child policy) assigned to the interfaces.

To open this page, choose **Monitoring > QoS Report Card**.

The QoS Report Card page allows you to select devices only from the active device group. To view the Qos Report Card of a device, select the device from the tree view by selecting the radio button next to the device name. The QoS Report Card appears on the right area of the pane.

The following topics provide more information about the QoS Report Card page:

Device Identity Area

Table D-1 describes the fields in the Device Identity area.

Table D-1 QoS Report Card - Device Identity Area

Field	Description
Device Name	Displays the device name.
Device Type	Displays the device type.
OS Version	Displays the operating system (OS) version of the device.

Interfaces Area

Table D-2 describes the fields in the Interface area.

Table D-2 QoS Report Card - Interfaces Area

Field	Description
Number of Interfaces	Displays the number of interfaces on the selected device.
Number of Interfaces with Qos Policies	Displays the number of interfaces for which policies are assigned.
Number of Threshold-enabled interfaces	Displays the number of interfaces on which Threshold Sets are assigned.

Monitorable Interfaces Area

The Monitorable Interfaces area (Table D-3) displays the number of monitorable QoS policies assigned to the interfaces of the selected device.

The message,

```
This device has no monitorable policies attached
```

appears if no monitorable policies are assigned to the device.

Table D-3 QoS Report Card - Monitorable Interfaces Area

Field	Description
QoS Policies	Displays the number of monitorable QoS policies on the selected device.
Interface	Displays the interface name. If you click the interface name, you can view the Real Time Chart of the traffic through the interface.
Policy	Displays the Traffic Rule(s) assigned to the interface.
Direction	Displays the direction of the Traffic Rule.

Related Topics

- Real Time Monitoring Page, page D-2

Real Time Monitoring Page

Use this page to view the real-time chart for a selected device interface.

To open this page, choose **Monitoring > Real Time Monitoring**.

The Real Time Monitoring page allows you to select devices only from the active device group. To view the real-time chart for a device interface, select the interface from the Select Device Interface pane and click **Show Real Time Chart**. The Real Time Charts Window for Class Based Monitoring page is displayed.

The following topics provide more information about Real Time Monitoring:

- Real Time Charts Window for Class Based Monitoring, page D-3
- Real Time Charts Window for Port Qos Monitoring, page D-6

Real Time Charts Window for Class Based Monitoring

Use this window to view the real-time monitoring report of a device interface. The real-time monitoring report includes graphs that display information about the policy actions.

To open this window, select a device interface from the Select Device Interface pane, and click the **Show Real Time Chart** button in the Real Time Monitoring Page.

The real-time policy analysis charts do not show the effect of traffic dropping for reasons other than QoS policy actions, such as dropping because of full queues.

Therefore, it is possible that the traffic volume shown for an interface will be greater than the capacity of the interface. In this case, if you set the vertical axis to percentage, the traffic volume for the interface will exceed 100% of the interface's capacity.

If a device is deleted from the device inventory while the real-time monitoring chart is displayed for that device, the following error message will be displayed and the real-time monitoring task will be stopped:

```
Monitored device is deleted. Please close the Real Time Charts window.
```

A device will not be successfully polled if a device is unreachable or if the SNMP community string is changed on the device, while it is being polled.

If a device is not successfully polled, the policy action graphs are not plotted for that interval.

Table D-4 describes the fields in the Real Time Charts window for Class Based Monitoring.

Table D-4 Real Time Charts Window for Class Based Monitoring

Field	Description
Graph Type	Select the graph type: • Line—Presents data in line chart format. • Bar—Presents data in bar chart format.
Units	Select the unit for data flow rate: • Packets/second—Displays data flow rate in packets per second. • Bits/second—Displays data flow rate in bits per second. • Kilobits/second—Displays data flow rate in kilobits per second. • Megabits/second—Displays data flow rate in megabits per second.
Vertical Axis	Select the vertical scale for graphs: • Linear—Displays the vertical scale of charts in linear format (the distance between units remains constant). • Logarithmic—Displays the vertical scale of charts in logarithmic format (the distance between units gets smaller as the total gets higher). • Percentage—Displays the vertical scale of charts as a percentage of the total bandwidth available on the interface.
Task Name	Displays the name of the task.
Task Start Time	Displays the start time of the task.
Device	Displays the name of the device that is monitored in the report.

Table D-4 Real Time Charts Window for Class Based Monitoring (continued)

Field	Description
Interface	Displays the name of the interface that is monitored in the report.
Actual Polling Interval	Displays the polling interval at which the task polls for data. This interval might be different than the polling interval configured for the task. If QPM is not able to poll at the interval configured for the task (for example, because of network congestion), it will determine the shortest interval at which it can poll. This value is displayed in this field.
Policy selection controls	Check the check box next to the policies (both parent policies and child policies) you want to view, and then click **Show Graphs**. You can select a maximum of 12 policies at a time.
Show Graphs button	Click this button to display the real-time chart for the selected policies.
Close Window button	Click this button to close the report window.
Matching Traffic Per Class Prior to QoS Actions graph	Displays the traffic flows that matched each policy group's traffic classifiers, before any policy actions were performed. This data is obtained from the cbQosCMPrePolicyPkt and cbQosCMPrePolicyByte MIB variables.
Matching Traffic Per Class After QoS Actions graph	Displays the traffic flows that matched each policy group's traffic classifiers and was transmitted (not dropped) by the configured QoS policies. This data is obtained as follows: • The bits data is obtained from the cbQosCMPostPolicyByte MIB variable. • The packets data is obtained by subtracting the cbQosCMDropPkt MIB variable from the cbQosCMPrePolicyPkt MIB variable.
Per Class Traffic Discarded By All QoS Drop Actions graph	Displays the traffic flows that matched each policy group's traffic classifiers and was dropped (not transmitted) by QoS policy drop actions. This data is obtained from the cbQosCMDropPkt and cbQosCMDropByte MIB variables.

Table D-4 Real Time Charts Window for Class Based Monitoring (continued)

Field	Description
Filters graphs	Displays how much traffic in each class matched the traffic classifiers of each class. Each graph includes a legend that shows the time period represented by each point on the poll time (horizontal) axis. The correlation between the traffic classifiers shown in this graph and the traffic classifier rules configured in the policy is not exact. Whenever possible, QPM translates the traffic classifier rules configured in QPM to modular CLI match statements. However, there are cases in which only ACL translation can reflect the traffic classifier definition, resulting in multiple traffic classifier rules being combined into one match statement. Rules combined by OR become separate match statements and rules combined by AND are combined into one match statement. This data is obtained from the cbQosMatchPrePolicyPkt and cbQosMatchPrePolicyByte MIB variables.
Actions graphs	See Policy Actions Graphs, page D-5.

Policy Actions Graphs

Policy actions graphs display information about the effect of policy actions. Only actions that are configured in a policy will appear in this page.

For example, if a policy has queuing and policing actions assigned, only actions graphs for queuing and policing will appear.

The following actions can appear in the graphs:

- Policing—Displays the following traffic amounts:
  - Conformed—Traffic that conformed to the rate limit.

    This data is obtained from the cbQosPoliceConformedPkt and cbQosPoliceConformedByte MIB variables.
  - Exceeded—Traffic that exceeded the rate limit.

    This data is obtained from the cbQosPoliceExceededPkt and cbQosPoliceExceededByte MIB variables.
  - Violated—Traffic that violated the rate limit.

    This data is obtained from the cbQosPoliceViolatedPkt and cbQosPoliceViolatedByte MIB variables.
- Queuing—Displays the amount of traffic dropped because of queuing.

  This data is obtained from the cbQosQueueingDiscardByte and cbQosQueueingDiscardPkt MIB variables.
- WRED—Displays counts of the following per precedence level:
  - Random drop—Traffic exceeded minimum but was less than maximum count.

    This data is obtained from the cbQosREDRandomDropPkt and cbQosREDRandomDropByte MIB variables.

  - Tail drop—Traffic exceeded maximum count.

    This data is obtained from the cbQosREDTailDropPkt and cbQosREDTailDropByte MIB variables.

  - Transmit counter—Traffic was transmitted.

    This data is obtained from the cbQosREDTransmitPkt and cbQosREDTransmitByte MIB variables.

- Traffic Shaping—Displays counts of the following:
  - Delayed traffic.

    This data is obtained from the cbQosTSStatsDelayedByte and cbQosTSStatsDelayedPkt MIB variables.

  - Traffic drop because of traffic shaping.

    This data is obtained from the cbQosTSStatsDropByte and cbQosTSStatsDropPkt MIB variables.

- CAR action (non modular QoS)—Displays counts of the following:
  - Bytes/packets that conformed to rate limit.
  - Packets/bytes that exceeded rate limit.

Real Time Charts Window for Port Qos Monitoring

Use this window to view a real-time monitoring report on a device interface that supports Port QoS monitoring.

To open this window, select a device interface from the Select Device Interface pane, and click the **Show Real Time Chart** button in the Real Time Monitoring Page.

The real-time policy analysis charts do not show the effect of traffic dropping for reasons other than QoS policy actions, such as dropping because of full queues.

If a device is deleted from the device inventory while the real-time monitoring chart is displayed for that device, the following error message will be displayed and the real-time monitoring task will be stopped:

```
Monitored device is deleted. Please close the Real Time Charts window.
```

If a device is not successfully polled (for example, when a device is unreachable, or the SNMP community string has been changed on the device directly while being polled), the graph is not plotted for that interval.

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

Table D-5 describes the fields in the Real Time Charts window for Port QoS Monitoring.

Table D-5 Port QoS Monitoring: Real Time Chart Page

Field	Description
Graph Type	Select the graph type to display: • Line Chart—Presents data in a line chart format. • Bar Chart—Presents data in a bar chart format.
Units	Select the unit for data flow rate: • Packets/second—Displays data flow rate in packets per second. • Bits/second—Displays data flow rate in bits per second. • Kilobits/second—Displays data flow rate in kilobits per second. • Megabits/second—Displays data flow rate in megabits per second.
Task Name	Displays the name of the task.
Task Start Time	Displays the start time of the task.
Device	Displays the name of the device that is monitored in the report.
Interface	Displays the name of the interface that is monitored in the report.
Actual Polling Interval	Displays the polling interval at which the task polls for data. This interval might be different than the polling interval configured for the task. If QPM is not able to poll at the interval configured for the task (for example, because of network congestion), it will determine the shortest interval at which it can poll. This value is displayed in this field.
Close Window button	Click to close the report window
DSCP Traffic Details	Select the DSCP values, and the direction of traffic (Input or Output) you want to monitor for matching DCSP values. You can move the DSCP values from the Available list to the Selected list. You can include maximum eight DSCP values in the Selected list.
Matching DSCP Traffic	Displays the traffic flows that matched the DSCP values that you selected. This data is obtained from the cportQosPrePolicyPkts and cportQosPostPolicyPkts variables.
CoS Traffic Details	Select the CoS values you want to monitor. You can move the CoS values from the Available list to the Selected list. You can include maximum eight CoS values in the Selected list.

Table D-5 Port QoS Monitoring: Real Time Chart Page (continued)

Field	Description
Matching CoS Traffic	Displays the traffic flows that matched the CoS values that are selected. This data is obtained from the cportQosPrePolicyPkts and cportQosPostPolicyPkts variables.
Policed Traffic	Shows graphs for policing action on the interface, for both conforming and exceeding traffic in both directions.
Dropped Traffic	Shows graphs for dropped traffic on the interface in both directions.

Historical Monitoring Page

Use this page to:

- View, create, edit, delete, and stop historical monitoring tasks for either class based or Port QoS monitoring
- View historical monitoring reports
- Export collected data from tasks

The following sections describe the pages that are launched from Historical Monitoring page:

- Create Task Dialog Box, page D-10
- Historical Reports Pages for Class Based Analysis, page D-11
- Historical Report Page for Port QoS Analysis, page D-17

Historical trends collect data for historical monitoring reports.

To open this page, choose **Monitoring > Historical Monitoring**.

When the historical QoS analysis data collected by QPM reaches the configured disk space limit, the following happens:

- All running monitoring tasks are stopped automatically, and are set to the status “Stopped due to out of disk space.”
- The next time you open the Historical Trends page, a message notifies you that the disk space limit was reached and provides recover instructions. This message only appears on the Historical Trends page. You will not receive notification that the disk space limit was reached until you open this page.

All data collected before the tasks were stopped is available for display in reports. To free the necessary disk space and continue monitoring, you must delete the stopped tasks and run the database rebuild utility. Then you can recreate the deleted tasks to resume running them.

Table D-6 describes the fields in the Historical Monitoring page.

Table D-6 Historical Monitoring Page

Field	Description
Check box column	Select check box to select its row.
Name	Displays the task name. For tasks with the Job Frequency as Daily, the name appears as *TaskName_ddmon_ddmon*. For example: NewTask_08Aug_09Aug
Description	Displays the task description.
Start Time	Displays the start time of the corresponding task.
End Time	Displays the end time of the corresponding task.
Task Type	Displays the type of monitoring task: • Policy—For class based monitoring. This is when you have selected the interface and the policy while creating the task • Port QoS—For Port QoS monitoring. This is when you have selected the interface that supports Port QoS monitoring while creating the task
Status	Displays the task status. The following are the possible statuses: • Processing—Initial status for tasks, indicating the task is being created. • Running—Task is running correctly and collecting data. • Stopped—Task was stopped by user request. • Stopped due to disk space limit—The amount of collected data reached the configured disk space limit. • Collector Error—Task could not be created because of a data collection error. One possible reason of this error is that the SNMP community string has been changed directly on the device while the device is undergoing a monitoring task. • In Edit—Task is disabled, and has not started yet. • Finished—Task successfully finished. It will not collect any more data. • Not Applicable—Parent task has been created but the child tasks are not yet created. The following pop-up message will be displayed when you click on this hyperlink: `It is a parent task. Check the status of the child task.`
View Report button	Click this button to view a report of the selected task. The Matching and Dropped Traffic for Policies page appears.
Class Based Monitoring button	Click this button to create a new task for class based monitoring. The Create Task dialog box appears.
Port QoS Monitoring button	Click this button to create a new task for Port QoS Monitoring. The Create Task dialog box appears.

Table D-6 Historical Monitoring Page (continued)

Field	Description
Edit button	Click this button to edit a task that is in an error status. The Create Task page appears. You can edit tasks in the following statuses: • Collector Error • In Edit
Delete button	Click this button to delete the selected task. A confirmation dialog box opens.
Stop button	Click this button to stop a running task.
Export Data button	Click this button to export a task's collected monitoring data to a zip file that contains a set of XML data files. The browser file download process starts. Ensure that you have the unzip application to recreate the folder structure of the zipped files when unzipping them. Each interface has a separate folder. Within each folder is a separate file for each policy defined on the interface.
Refresh Rate	Select a page refresh rate from the list. The refresh rate determines how often the page refreshes with updated information.

Create Task Dialog Box

Use this dialog box to create Historical Monitoring tasks either for Class Based Monitoring or for Port QoS Monitoring.

Table D-7 describes the fields in the Create Task dialog box.

Table D-7 Create Task dialog box

Field	Description
Name	Enter the name of the Historical Monitoring Task
Start Time	Enter the start date and time for the task. You should enter the date in MM/DD/YYYY format, or you can use the calender icon to select the date. You should enter the time in 24 hour format.
End Time	Enter the end date and time for the task. You should enter the date in MM/DD/YYYY format, or you can use the calender icon to select the date. You should enter the time in 24 hour format.
Polling Interval	Select the polling interval (in minutes) for the monitoring task
Job Frequency	Select the frequency of the job as daily, weekly, bi-weekly, or monthly
Description	Enter a description for the task
Enabled	Check this to enable historical monitoring at the specified period

Table D-7 Create Task dialog box (continued)

Field	Description
Create Task button	Click this button to save and apply the task details
Object Selector	Lists the devices and interfaces that are compatible with either Class Based monitoring or Port QoS monitoring (based on the type of task you selected). Use the filter options in the object selector to search for one or more devices. On this page, you can search for devices based on the following two criteria: device names and device folder names. See Appendix 3, "Using Object Selector Filter Options". If you have chosen Class Based monitoring task, select the policy (displayed under the interface) that you want to monitor. If you have chosen Port QoS monitoring task, select the interface that you want to monitor.

Historical Reports Pages for Class Based Analysis

The following topics describe the pages that are launched from class based historical monitoring report:

- 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

To open these pages, click **View Report** corresponding to a task that shows the Task Type as "Policy".

The historical policy analysis graphs do not show the effect of traffic dropping for reasons other than QoS policy actions, such as dropping because of full queues.

Therefore, it is possible that the traffic volume shown for an interface will be greater than the capacity of the interface. In this case, if you set the vertical axis to percentage, the traffic volume for the interface will exceed 100% of the interface's capacity.

Policies Graphs: Matching and Dropped Traffic for Policies Page

Use this page to view data that shows how much traffic matched the policies and whether it was transmitted or dropped. You can customize the page with the customization controls.

To open this page, do either of the following:

- Click **View Report** corresponding to the task which shows the status as "Policy", in the Historical Monitoring Page.
- Click **Policies Graphs** in any historical monitoring report page.

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 up to several hours to see graphed data.

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.

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.

Table D-8 describes the Policies Graphs - Matching and Dropped Traffic for Policies page.

Table D-8 Policies Graphs - Matching and Dropped Traffic for Policies Page

Field	Description
Graph Type	Select the graph type to display: • Line—Presents data in a line chart format. • Bar—Presents data in a bar chart format.
Units	Select the units to display in the graphs: • Packets/second—Displays data flow rates in packets per second. • Bits/second—Displays data flow rates in bits per second.
Vertical Axis	Select the vertical scale for graphs: • Linear—Displays the vertical scale of charts in linear format (the distance between units remains constant). • Logarithmic—Displays the vertical scale of charts in logarithmic format (the distance between units gets smaller as the total gets higher). • Percentage—Displays the vertical scale of charts as a percentage of the total bandwidth available on the interface.
Group	Select how to group the objects that are displayed in the graphs: • Policy—Organizes the report according to policies. • Interface—Organizes the report according to interfaces.
From Time and To Time	Select the period of time you want to view in the report: • Enter dates in the first From Time and To Time fields in the format *mm/dd/yyyy*, or click the calendar icons to select dates from the Calendar dialog box. • Enter times in the second From Time and To Time fields in 24-hour format.
Apply button	Click this button to view only data collected during the period defined by the From Time and To Time controls.
Reset button	Click this button to reset the time period displayed in the From Time and To time controls to the collection period defined for the analysis task.
Policy/Interface selection table	Select which policies or interfaces (depending on the selection in the Group list box) to display in the report. You can check the check box next to the policies or interfaces you want to view.
Show Graphs button	Click to update the graphs to display the policies and interfaces selected using the policy-interface selection table
Matching Traffic Per Class Prior to QoS Actions graphs	Displays the traffic that matched each policy group's traffic classifiers, before any policy actions were performed. This data is obtained from the cbQosCMPrePolicyPkt and cbQosCMPrePolicyByte MIB variables.

Table D-8 Policies Graphs - Matching and Dropped Traffic for Policies Page (continued)

Field	Description
Matching Traffic Per Class After QoS Actions	Displays the traffic that matched each policy group's traffic classifiers and was transmitted (not dropped) by the configured QoS policies. This data is obtained as follows: • The bits data is obtained from the cbQosCMPostPolicyByte MIB variable. • The packets data is obtained by subtracting the cbQosCMDropPkt MIB variable from the cbQosCMPrePolicyPkt MIB variable.
Matching Traffic Per Class Discarded by QoS Drop Actions	Displays the traffic that matched each policy group's traffic classifiers and was dropped (not transmitted) by QoS policy drop actions. This data is obtained from the cbQosCMDropPkt and cbQosCMDropByte MIB variables.
Policies Graphs button	Click to open the Policies Graphs: Matching and Dropped Traffic for Policies Page.
Filters Graphs button	Click to open the Filters Graphs: Matching Traffic for Filter Conditions Page
Actions Graphs button	Click to open the Actions Graphs: Policy Actions on Matching Traffic Page
Back to Task List button	Click to open the Historical Monitoring Page.

Filters Graphs: Matching Traffic for Filter Conditions Page

Use this page to view data that shows how matching traffic was distributed among the policy traffic classifier conditions. You can customize the page with the customization controls.

To open this page, click **Filters Graphs** in any historical monitoring report page that is generated for class based monitoring.

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 up to several hours to see graphed data, due to 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.

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.

Table D-9 describes the Filter Graphs - Matching Traffic for Filter Conditions page.

Table D-9 Filters Graphs - Matching Traffic for Filter Conditions Page

Field	Description
Graph Type	Select the graph type: • Line—Presents data in a line chart format. • Bar—Presents data in a bar chart format.
Vertical Axis	Select the vertical scale for graphs: • Linear—Displays the vertical scale of charts in linear format (the distance between units remains constant). • Logarithmic—Displays the vertical scale of charts in logarithmic format (the distance between units gets smaller as the total gets higher). • Percentage—Displays the vertical scale of charts as a percentage of the total bandwidth available on the interface.
Group	Select how to group the objects that are displayed in the graphs: • Policy—Organizes the report according to policy groups. • Interface—Organizes the report according to interfaces.
From Time and To Time	Select the period of time you want to view in the report: • Enter dates in the first From Time and To Time fields in the format *mm/dd/yyyy*, or click the calendar icons to select dates from the Calendar dialog box. • Enter times in the second From Time and To Time fields in 24-hour format.
Apply button	Click to view only data collected during the period defined by the From Time and To Time controls.
Reset button	Click to reset the time period displayed in the From Time and To time controls to the collection period defined for the analysis task.
Filters graphs	Displays how much traffic in each class matched the traffic classifiers of each class. Each graph includes a legend that shows the time period represented by each point on the poll time (horizontal) axis. The correlation between the filters shown in this graph and the traffic classifier rules configured in the policy is not exact. Whenever possible, QPM translates the traffic classifier rules configured in QPM to modular CLI match statements. In some cases, only ACL translation can reflect the traffic classifier definition, resulting in multiple traffic classifier rules being combined into one match statement (rules combined by OR become separate match statements; rules combined by AND are combined into one match statement). This data is obtained from the cbQosMatchPrePolicyPkt and cbQosMatchPrePolicyByte MIB variables.

Table D-9 Filters Graphs - Matching Traffic for Filter Conditions Page (continued)

Field	Description
Policies Graphs button	Click to open the Policies Graphs: Matching and Dropped Traffic for Policies Page.
Filters Graphs button	Click to open the Filters Graphs: Matching Traffic for Filter Conditions Page
Actions Graphs button	Click to open the Actions Graphs: Policy Actions on Matching Traffic Page
Back to Task List button	Click to open the Historical Monitoring Page.

Actions Graphs: Policy Actions on Matching Traffic Page

Use this page to view data that shows the policy actions that were taken on matching traffic. You can customize the page with the customization controls.

To open this page, click **Actions Graphs** in any historical monitoring report page.

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 up to several hours to see graphed data, due to 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.

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.

Table D-10 describes the Actions Graphs - Policy Actions on Matching Traffic page.

Table D-10 Actions Graphs - Policy Actions on Matching Traffic Page

Field	Description
Graph Type	Select the graph type to display: • Line—Presents data in a line chart format. • Bar—Presents data in a bar chart format.
Units	Select the units to display in the graphs: • Packets/second—Displays data flow rates in packets per second. • Bits/second—Displays data flow rates in bits per second.

Table D-10 Actions Graphs - Policy Actions on Matching Traffic Page (continued)

Field	Description
Vertical Axis	Select the vertical scale for graphs: • Linear—Displays the vertical scale of charts in linear format (the distance between units remains constant). • Logarithmic—Displays the vertical scale of charts in logarithmic format (the distance between units gets smaller as the total gets higher). • Percentage—Displays the vertical scale of charts as a percentage of the total bandwidth available on the interface.
Group	Select how to group the objects that are displayed in the graphs: • Policy—Organizes the report according to policy groups. • Interface—Organizes the report according to interfaces.
From Time and To Time	Select the period of time you want to view in the report: • Enter dates in the first From Time and To Time fields in the format *mm/dd/yyyy*, or click the calendar icons to select dates from the Calendar dialog box. • Enter times in the second From Time and To Time fields in 24-hour format.
Apply button	Click to view only data collected during the period defined by the From Time and To Time controls.
Reset button	Click to reset the time period displayed in the From Time and To time controls to the collection period defined for the analysis task.
Policy Actions graphs	See Policy Actions Graphs, page D-16.
Policies Graphs button	Click to open the Policies Graphs: Matching and Dropped Traffic for Policies Page.
Filters Graphs button	Click to open the Filters Graphs: Matching Traffic for Filter Conditions Page
Actions Graphs button	Click to open the Actions Graphs: Policy Actions on Matching Traffic Page
Back to Task List button	Click to open the Historical Monitoring Page.

Policy Actions Graphs

Policy actions graphs display information about traffic that was dropped because of policy actions. Only actions that are configured in a policy will appear in this page.

For example, if a policy has queuing and policing actions assigned, only actions graphs for queuing and policing will appear.

The following actions can appear in the graphs:

- Policing—Displays the following traffic amounts:
  - Conformed—Traffic that conformed to the rate limit.

    This data is obtained from the cbQosPoliceConformedPkt and cbQosPoliceConformedByte MIB variables.

  - Exceeded—Traffic that exceeded the rate limit.

    This data is obtained from the cbQosPoliceExceededPkt and cbQosPoliceExceededByte MIB variables.

  - Violated—Traffic that violated the rate limit.

    This data is obtained from the cbQosPoliceViolatedPkt and cbQosPoliceViolatedByte MIB variables.

- Queuing—Displays the amount of traffic dropped due to queuing.

  This data is obtained from the cbQosQueueingDiscardByte and cbQosQueueingDiscardPkt MIB variables.

- WRED—Displays counts of the following per precedence level:
  - Random drop—Traffic exceeded minimum but was less than maximum count.

    This data is obtained from the cbQosREDRandomDropPkt and cbQosREDRandomDropByte MIB variables.

  - Tail drop—Traffic exceeded maximum count.

    This data is obtained from the cbQosREDTailDropPkt and cbQosREDTailDropByte MIB variables.

  - Transmit counter—Traffic was transmitted.

    This data is obtained from the cbQosREDTransmitPkt and cbQosREDTransmitByte MIB variables.

- Traffic Shaping—Displays counts of the following:
  - Delayed traffic.

    This data is obtained from the cbQosTSStatsDelayedByte and cbQosTSStatsDelayedPkt MIB variables.

  - Traffic drop due to traffic shaping.

    This data is obtained from the cbQosTSStatsDropByte and cbQosTSStatsDropPkt MIB variables.

- CAR action (non-modular QoS)—Displays counts of the following:
  - Bytes/packets that conformed to rate limit.
  - Packets/bytes that exceeded rate limit.

Historical Report Page for Port QoS Analysis

Use this page to:

- Select DSCP and CoS values based on which you want to monitor the interfaces that support Port QoS monitoring
- View graphs for matching DSCP and CoS values for the traffic in both directions (In and Out)
- View graphs for the policing action on the traffic through the interface
- View graphs for dropped traffic through the interface

To open this page, click **View Report** corresponding to a task that shows the Task Type as “Port QoS”.

The historical analysis graphs do not show the effect of traffic dropping for reasons other than QoS policy actions, such as dropping because of full queues.

Table D-11 describes the fields in the Historical Report page for Port QoS Analysis.

Table D-11 Historical Report Page for Port QoS Analysis

Field	Description
Graph Type	Select the graph type to display: • Line—Presents data in a line chart format. • Bar—Presents data in a bar chart format.
From Time and To Time	Select the period of time you want to view in the report: • Enter dates in the first From Time and To Time fields in the format *mm/dd/yyyy*, or click the calendar icons to select dates from the Calendar dialog box. • Enter times in the second From Time and To Time fields in 24-hour format.
Apply button	Click to view only data collected during the period defined by the From Time and To Time controls.
Reset button	Click to reset the time period displayed in the From Time and To time controls to the collection period defined for the analysis task.
Device/Interface	Displays the device and the interface that you selected while creating the task.
Matching DSCP Traffic	Displays the graph of DSCP traffic that matched the first eight non-zero DSCP values.
Matching CoS Traffic	Displays the graph of CoS traffic that matched the first five non-zero CoS values.
Dropped Traffic	Displays the graph of dropped traffic in both directions (In and Out).
Policied Traffic	Displays the graph of traffic for policing action on the interface, for both conforming and exceeding traffic.

Thresholds Configuration

The following topics describe the pages that are accessed from the Thresholds Configuration option:

- Threshold Sets Page, page D-19
- 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

Threshold Sets Page

Use this page to:

- Clone a Threshold Set using ClassmapMetrics (MIB objects)
- Set the High Water Mark and Low Water Mark levels for the metrics
- Delete a Threshold Set

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

To open the Threshold Sets page (Table D-12), choose **Monitor > Thresholds Configuration**.

Table D-12 Threshold Sets Page

Field	Description
Threshold Sets	Lists the Threshold Sets. When you select the radio button next to a Threshold Set, the associated ClassmapMetrics (MIB objects), High Water Mark levels, and Low Water Mark levels appear on the right area of the pane.
New Set Name field	Enter a name for the new Threshold Set you want to create.
Metric	MIBs associated with the selected Threshold Set to collect the required data. See the table below for more information about each MIB.
High Water Mark	High water mark level for the MIB. This is an editable field.
Low Water Mark	Low water mark level for the MIB. This is an editable field.
Clone button	Click this button to create a new Threshold Set after entering a name in the New Set Name field.
Save button	Click this button to save changes you made for the High and Low Water Mark levels for each metric, corresponding to the selected Threshold Set.
Delete button	Click this button to delete the selected Threshold Set.

Table D-13 describes the MIBs in Threshold Sets page.

Table D-13 MIBs in Threshold Sets page

MIBs in Threshold Sets page	Description
cbQosCMPrePolicyPkt64	64 bits count of inbound packets prior to executing any QoS policies. This metric is a counter.
cbQosCMDropPkt64	64 bits counter of dropped packets per 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.

Table D-13 MIBs in Threshold Sets page (continued)

MIBs in Threshold Sets page	Description
cbQosCMDropByte64	64 bits counter of dropped bytes per 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	Bit rate (in bits per second) of the drops per 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.
cbQosCMPostPolicyByte64	64 bits count of outbound octets after running QoS policies. This metric is a counter.
cbQosCMPrePolicyBitRate	Bit rate (in bits per second) of the traffic after running any QoS policies. This metric is a gauge.
cbQosCMPrePolicyByte64	64 bits count of inbound octets before running any QoS policies. This metric is a counter.
cbQosCMPostPolicyBitRate	Bit rate (in bits per second) of the traffic after running QoS policies. This metric is a gauge.
cbQosCMNoBufDropPkt64	64 bits drop packet count that occurred because of non-availability of SRAM buffers during output processing on an interface. This metric is a counter.

Related Topics

- Threshold Assignment Page, page D-20

Threshold Assignment Page

Use this page to:

- Assign/Unassign a Threshold Set to a traffic direction (inward/outward) of a device interface (under the active device group) with monitorable policies attached for the traffic direction.
- View all the device interfaces to which a Threshold Set is assigned for a particular traffic direction

To open the Threshold Assignment page (Table D-14), choose **Monitor > Thresholds Configuration** and select **Threshold Assignment** from the TOC.

Table D-14 Threshold Assignment Page

Field	Description
Threshold Sets	Select the required Threshold Set.
Device Interfaces	Displays the device interfaces under the active device group. Select the direction of traffic (Inward or Outward) to be monitored on the device interfaces (with inward or outward traffic rules defined for the assigned monitorable policies).
Show Selected button	Click to view all the device interfaces with the selected Threshold Set assigned, for a particular traffic direction (inward or outward).

Table D-14 Threshold Assignment Page (continued)

Field	Description
Assign button	Click to assign the selected Threshold Set to the selected traffic direction of the respective interfaces.
Unassign button	Click to unassign the selected Threshold Set from the selected traffic direction of the respective interfaces.

Related Topics

- Threshold Sets Page, page D-19
- Pending Jobs Page, page D-21
- Completed Jobs Page, page D-22

Pending Jobs Page

Use this page to:

- View all the pending Threshold Assignment jobs on different devices
- Control the Threshold Assignment job
- Redeploy the Threshold Assignment job

To open the Pending Jobs page (Table D-15), choose **Monitor > Thresholds Configuration** and select **Pending Jobs** from the TOC.

Table D-15 Pending Jobs Page

Field	Description
Job Name	Name of the Threshold Assignment job. Click the Job Name link for a selected job to open the Job Details report for that job.
Start Time	Start time of Threshold Assignment job.
Job Status	Status of the selected job (Pending, In Progress, Paused, Aborted, Completed, No Devices, or Failed).
Devices Pending	Number of devices that are waiting to be assigned.
Devices In Progress	Number of devices whose Threshold Assignment is in-progress.
Devices Completed	Number of devices whose Threshold Assignment is completed successfully.
Devices Failed	Number of devices whose Threshold Assignment failed.
Total	Total number of devices in the current job. (This number is the sum of the four previous status fields.)
Refresh	Click this button to force a manual update of the displayed data. The display is automatically refreshed every ten seconds.
Pause	Click this button to pause a job during its assignment to devices. Any devices that are being configured when the Pause command is issued will be finished. Devices for which the assignment has not yet begun, will remain with the status “Pending”.

Table D-15 Pending Jobs Page (continued)

Field	Description
Resume	Click this button to resume the configuration of devices for a job that was paused.
Redeploy	Click this button to manually request that Threshold Assignment be re-tried for a specific failed or aborted device or all failed or aborted devices in the selected job. Another assignment is created for the job.
Remove From Display	Click this button to remove a completed or failed job from the table. When removed, the job is moved to the Completed Jobs Page.
Abort	Click this button to terminate a job that is currently in progress or has been paused. Any devices that were not configured when the Abort command was issued will not be deployed. They will be set as Failed. A terminated deployment cannot be resumed.

Related Topics

- Threshold Assignment Page, page D-20
- Completed Jobs Page, page D-22

Completed Jobs Page

Use this page to:

- View the results of a DNS host name resolution check for a Threshold Assignment job
- View the history details of Threshold Assignment jobs
- Restore a historical version for editing and deploying
- Delete Threshold Assignment jobs
- Lock and unlock jobs for deletion
- Download the configuration files of a Threshold Assignment job
- View a Job Details report for a Threshold Assignment job
- View a Threshold Assignment History report for a job

To open the Completed Jobs page (Table D-16), choose **Monitor > Thresholds Configuration** and select **Completed Jobs** from the TOC.

Table D-16 Completed Jobs Page

Field	Description
Job Name	Name of the Threshold Assignment job. Click the Job Name link for a selected job to open the Job Details report for that job.
Deployment Time	Time the last Threshold Assignment occurred for the job.

Table D-16 Completed Jobs Page (continued)

Field	Description
Deployments	Number of Threshold Assignment that were made for the job. Click the Deployments link of a job whose Threshold Assignment details you want to view to open a Threshold Deployment History report for the selected deployment.
Status	Assignment status of the selected job (Pending, In Progress, Completed, Paused, Aborted, or Failed).
Lock Job	Lock or Unlock, depending on whether the job is locked to prevent deletion when the history cache becomes full.
Files	Click this link to download the zip file containing the individual configuration files for a device to your desktop.
Details	Click the Details icon for a job to open its Job Details report in which you can view the status of devices related to the Threshold Assignment job.
DNS Resolution	Click to view the results of a DNS host name resolution check for a selected Threshold Assignment job.
Restore	Click to restore a selected historical version for editing and deploying. The Restore Threshold Deployment Group page appears.
Delete	Click to delete a selected historical version from the Job History list. After its deletion, you cannot restore it.
Lock Job	Click to prevent a selected historical version from being automatically deleted when the history cache is full.
Unlock Job	Click to unlock a historical version, making it available for deletion.

Related Topics

- Pending Jobs Page, page D-21
- Threshold Assignment Page, page D-20

Threshold Job Details Page

Use this page to view:

- The final status of all the Threshold Assignment of a selected job
- The current Threshold Assignment status of a job that is still in progress
- A table of all the devices related to the Threshold Assignment job
- The CLI commands that were used to configure a device

To open the Threshold Job Details page (Table D-17), do either of the following:

- In the Pending Jobs page, click the Job Name link for a job.
- In the Completed Jobs page, click the Job Name link of the job whose details you want to view, or click the Details icon for the job.

Table D-17 Threshold Job Details Page

Field	Description
Job Name	Name of the Threshold Assignment job.
Device Group	Device group that contains the Threshold Assignment job.
Job Status	Status of the Threshold Assignment job (Pending, In Progress, Paused, Aborted, Completed, or Failed).
Owner	Person who last saved the Threshold Assignment job.
Creation Time	Date and time the job was created.
Job Description	Description of the job, if any.
Device Name	Name of the device.
Status	Threshold Assignment status of the device.
Status Time	Time the device received its status.
Errors/Warnings	An error string, if available. In the case of a FAILED status, the CLI command that caused the error will also be displayed. If the error string for a Failed job displays “Internal error - unknown device state”, some of the job’s devices might be stuck in progress. In such a case, QPM will not be able to determine what was configured on these devices. You should contact Cisco technical support for help.
View CLI Commands	Click to view the CLI commands that were used to configure the device. A Device Configuration window opens.

Related Topics

- Pending Jobs Page, page D-21
- Completed Jobs Page, page D-22

Threshold Errors and Warnings Page

Use this page to view details about any errors, warnings, or notifications that resulted from the Threshold Assignment of a device.

To open this page, click the Errors/Warnings link for a threshold job, in the Threshold Job Details page.

Table D-18 describes the fields in the Threshold Errors and Warnings page.

Table D-18 Threshold Errors and Warnings Page

Field	Description
Type	Displays message type—Notify, Exception, Error, Fatal Error, or Warning.
Message	Displays the reason for the message.
Message Time	Displays the time the error or warning occurred.

Related Topics

- Threshold Job Details Page, page D-23

Threshold Deployment History Page

Use this page to view the Threshold Assignment history details of a selected deployment.

To open the Threshold Deployment History page (Table D-19), in the Completed Jobs page, click the Deployment link of the job whose assignment details you want to view.

Table D-19 Threshold Deployment History Page

Field	Description
Job Name	Name of the Threshold Assignment job.
Device Group	Device group that contains the Threshold Assignment job.
Creation Time	Date and time the job was created.
Job Description	Description of the job, if any.
Threshold Assignment Type	Threshold Assignment type - Normal or Redeploy. Click this link to view the Job Details report of the selected deployment.
Start Time	Date and time at which the Threshold Assignment started.
End Time	Date and time at which the Threshold Assignment ended.

Related Topics

- Threshold Job Details Page, page D-23

Monitoring QoS Events

This following topics describe the pages that can be accessed from the QoS Events option:

- Historical Event Browser Properties Page, page D-26
- Live Event Browser Properties Page, page D-28

Historical Event Browser Properties Page

Use this page to select a device and specify a time period to view a snapshot of events on the device in the specified event filter.

To open this page, choose **Monitoring > QoS Events > Historical**.

Table D-20 describes the fields in the Historical Event Browser Properties page.

Table D-20 Historical Event Browser Properties Page

Field	Description
Start Time and End Time	Select the time period for which you want to view in the report: • Enter dates in the first fields in the format *mm*/*dd*/*yyyy*, or click the calendar icons to select dates from the Calendar dialog box. • Enter times in the second fields in 24-hour format.
Devices	This area consists of two tab screens: • All—Select to open a tab screen with all the devices under the active device group displayed. You can select the devices by clicking the corresponding check boxes. • Selection—Select to open a tab screen with all the devices you selected under the All tab screen.You can deselect the devices by clicking the corresponding check boxes. If no device is selected, the result will show the events for all devices.
Submit button	Click to view the Historical event browser for the selected device, or all devices.

The following topics describe the pages that are accessed from the Historical Event Browser Properties page.

- Historical Event Browser Page, page D-26
- Exporting Report Dialog Box, page D-27
- Printing Report Dialog Box, page D-28

Historical Event Browser Page

Use this page to view the events that have occurred on a device in a specified time interval.

To open the Historical Event Browser page (Table D-21), select a device and a time interval, and click **Submit** in the Historical Event Browser Properties page.

Table D-21 Historical Event Browser Page

Field	Description
Timestamp	Timestamp of Historical event occurrence for threshold crossing or falling event
Device	Device for which the Historical event capture is applied

Table D-21 Historical Event Browser Page (continued)

Field	Description
Interface	Interface of the device for which Historical event capture is applied
Metric	CBQoS metric defined as part of threshold configuration
Value	Actual value of the metric for a particular device/interface that caused the threshold crossing or falling alarm event to be generated.
Threshold	Threshold level that was set to the interface and the metric (it would be high or low watermark value) during Threshold Configuration. You can compare this with the entry in the Value column.
Properties icon	Click this icon to go back to the Historical Event Browser Properties page to select more devices or deselect the devices.
Export icon	Click this icon to export a report of Historical Events, in PDF or CSV format. The Exporting Report dialog box opens.
Printer icon	Click this icon to print a report of Historical Events. The Printing Report dialog box opens.

Related Topics

- Exporting Report Dialog Box, page D-27
- Printing Report Dialog Box, page D-28

Exporting Report Dialog Box

Use this dialog box to export the report of Historical events or Live events in PDF or CSV format.

To open the Exporting Report dialog box (Table D-22), click the Export icon in the Historical Event Browser or Live Event Browser.

Table D-22 Exporting Report Dialog Box

Field	Description
Select a format	Click the PDF or CSV radio button to select the format in which you want the report to be exported.
Rows	Enter the row numbers (which represent the events) for which you want to generate report. You can mention the row numbers separated by commas (like 2,5,8) or as a range (like 3-7)

Related Topics

- Printing Report Dialog Box, page D-28

Printing Report Dialog Box

Use this dialog box to print a report of Historical events or Live events.

To open the Printing Report dialog box (Table D-23), click the Print icon in the Historical Event Browser or Live Event Browser.

Table D-23 Printing Report Dialog Box

Field	Description
Rows	Enter the row numbers (which represent the events) for which you want to generate report. You can mention the row numbers separated by commas (like 2,5,8) or as a range (like 3-7).

Related Topics

- Exporting Report Dialog Box, page D-27

Live Event Browser Properties Page

The Live Event Browser displays events as they occur on the server.

To open this page, choose **Monitoring > QoS Events > Live**.

Table D-24 describes the fields in the Live Event Browser Properties page.

Table D-24 Live Event Browser Properties Page

Field	Description
Maximum Events	Select the maximum number of events to be displayed from the list.
Refresh Rate	Select a page refresh rate from the list. The refresh rate determines how often the page refreshes with updated information.
Devices	This area consists of two tab screens: • All—Opens a tab screen with all the devices under the active device group displayed. You can select the devices by clicking the corresponding check boxes. • Selection—Opens a tab screen with all the devices you selected under the All tab screen. You can deselect the devices by clicking the corresponding check boxes. If no device is selected, the result will show the events for all devices.
Submit button	Click to view the live event browser for the selected device.

Related Topics

Live Event Browser Page, page D-29

Live Event Browser Page

Use this page to view the events as they occur on a device at the current time.

To open the Live Event Browser page (Table D-25), select a device and the number of events to be displayed, and click **Submit** in the Live Event Browser Properties page.

Table D-25 Live Event Browser Page

Field	Description
Timestamp	Timestamp of live event occurrence for threshold crossing or falling event.
Device	Device for which the live event capture is applied.
Interface	Interface of the device for which live event capture is applied.
Metric	CBQoS metric defined as part of threshold configuration.
Value	Actual value of the metric for a particular device/interface that caused the threshold crossing or falling alarm event to be generated.
Threshold	Threshold level that was set to the interface and the metric (it would be high or low watermark value) during threshold configuration. You can compare this with the entry in the Value column.
Maximum Events To Show	Select the maximum number of events to be displayed from the list.
Refresh Rate	Select a page refresh rate from the list. The refresh rate determines how often the page refreshes with updated information.
Properties icon	Click to go back to the Live Event Browser Properties page to select more devices or deselect the devices.
Export icon	Appears only if you selected any of the two options–Now or Never–among the options available for Refresh Rate. Click to export a report of Live Events, in PDF or CSV format. The Exporting Report dialog box opens.
Printer icon	Appears only if you selected any of the two options–Now or Never–among the options available for Refresh Rate. Click to print a report of Snapshot Events. The Printing Report dialog box opens.

Related Topics

- Exporting Report Dialog Box, page D-27
- Printing Report Dialog Box, page D-28

Monitoring NCM Events

The following topics describe the pages that can be accessed from the NCM Events option:

- NCM Events: Historical Event Properties Page, page D-30
- NCM Events: Live Event Properties Page, page D-34

NCM Events: Historical Event Properties Page

Use this page to select a device and specify a time period to view a snapshot of NCM events from the device.

To open this page, choose **Monitoring > NCM Events > Historical**.

Table D-26 NCM Events: Historical Event Properties Page

Field	Description
Start Time and End Time	Select the time period for which you want to view NCM Events in the report: • Enter dates in the first fields in the format *mm/dd/yyyy*, or click the calendar icons to select dates from the Calendar dialog box. • Enter times in the second fields in 24-hour format.
Devices	This area consists of two tab screens: • All—Select to open a tab screen with all the devices under the active device group displayed. You can select the devices that are registered with NCM, by clicking the corresponding check boxes. • Selection—Select to open a tab screen with all the devices you selected under the All tab screen.You can deselect the devices by clicking the corresponding check boxes. If no device is selected, the result will show the events for all devices registered with NCM.
Submit button	Click to view the Historical Events page, which shows events from the selected devices, or from all devices.

NCM Events: Historical Events Page

Use this page to view the events that have occurred in a specified time interval on a device registered with NCM.

To open the Historical Events page (Table D-27), in the Historical Event Browser Properties page, select the devices (registered with NCM) and the time interval, and click **Submit**.

Table D-27 NCM Events: Historical Events Page

Field	Description
Network Compliance Manager Host	NCM Server IP address or DNS hostname from where events are sent to QPM
Device Group	Name of the active device group in QPM. The events shown in this page are from devices in this device group only.
Policy Group	Name of the active policy group in QPM. The policy group acts like a filter for events from devices. QPM identifies the devices for which the QoS configuration is not part of the currently active policy group, and marks those events with ** symbol. When you choose a different policy group, the Historical Events page is updated.
Timestamp	Time at which the event occurred on the device.
Type	Type of the event type. • Config—This event type is generated when the device configuration is modified. When device configuration differs from QPM stored configuration, QPM monitoring and provisioning features are affected. For this event type, you can use all the available options–Rediscover, Import, and Deploy. • IOS—This event type is generated when the device image is upgraded or modified. Any change in device image affects device monitoring from QPM. For this event type, you can use the available options Rediscover and Import. The Deploy option is not applicable to this event type.

Table D-27 NCM Events: Historical Events Page (continued)

Field	Description
Modification	One of the following: • Configuration link—Link to CLI commands in the device configuration The View CLI Commands window appears showing the latest device configuration, and the following buttons: – Show Run—Click to view the device's running configuration sent with the NCM event message. – Configuration Diff—Click to view the configuration diff data sent with the NCM event. This is the device configuration change that triggered the event message. – Incremental Telnet—Click to view the difference in configuration between QPM stored device configuration and device's running configuration. In this case, QPM connects to the device and display the difference between device running configuration and QPM stored device configuration. This button is disabled if the device is not managed from QPM (the device name ends with "*") or not managed from current policy group (the device name ends with "**"). – Close—Click to close the window. These configuration change details help you to to identify whether the device configuration change is desirable or not. – If the changes are not desirable, you can restore the configuration stored with the QPM, using the Deploy option. – If the changes are desirable and affect QPM, you can update QPM with device configuration changes, using the Import option. • Image upgrade data sent with the NCM event
Last Action	Last action that you performed after the event appeared in QPM. The following actions (if you have performed any) are shown: • Rediscover • Import • Deploy For new events, this field shows `No action`.

Table D-27 NCM Events: Historical Events Page (continued)

Field	Description
Rediscover	Click to rediscover the devices corresponding to the selected events. The Discovery Status page appears. The Rediscover action is needed, since any change in the device image or configuration can affect the monitoring of the device from QPM. The Discovery Status page shows only one Job Type even if you chose to rediscover more devices. You can find the number of devices being discovered from the In Progress column.
Import	Click to import the QoS configuration from the devices (corresponding to selected events) to QPM. The Import QoS from Devices page appears. You can perform this action when you find that the device configuration change will affect the device provisioning and monitoring from QPM. Even if you select multiple events from the same device, and click Import, only one Import QoS task is launched for the device.
Deploy	Click to deploy the QoS configuration from QPM to the devices corresponding to the selected events. The Pending Jobs page appears. The Deploy action helps you to restore the device configuration from QPM if you feel that the configuration change that occurred on the device is wrong. Even if you select multiple events from the same device, and click Deploy, only one policy deployment task is launched for the device.

NCM Events: Live Event Properties Page

Use this page to view the live NCM events (events for the day) of a selected device.

To open this page, choose **Monitoring > NCM Events > Live**.

Table D-28 describes the fields in the NCM Events: Live Event Properties page.

Table D-28 NCM Events: Live Event Properties Page

Field	Description
Devices	This area consists of two tab screens: • All—Select to open a tab screen with all the devices under the active device group displayed. You can select the devices that are registered with NCM, by clicking the corresponding check boxes. • Selection—Select to open a tab screen with all the devices you selected under the All tab screen.You can deselect the devices by unchecking the corresponding check boxes. If no device is selected, the result will show the events for all devices registered with NCM.
Submit button	Click to view the Live Events page.

NCM Events: Live Events Page

Use this page to view the events that have occurred on a device registered with NCM.

To open the Live Events page (Table D-29), in the Live Event Browser Properties page, select a device (registered with NCM), and click **Submit**.

Table D-29 NCM Events: Live Events Page

Field	Description
Maximum Events	Choose the maximum number of events that you want to view
Refresh Rate	Choose the screen refresh rate to view the latest events
Network Compliance Manager Host	NCM Server IP address or DNS hostname from where events are sent to QPM
Device Group	Name of the active device group in QPM. The events shown in this page are from devices in this device group only.
Policy Group	Name of the active policy group in QPM. The policy group acts like a filter for events from devices. QPM identifies the devices for which the QoS configuration is not part of the currently active policy group, and marks those events with ** symbol. When you choose a different policy group, the Live Events page is updated.
Timestamp	Time at which the event occurred on the device.

Table D-29 NCM Events: Live Events Page (continued)

Field	Description
Type	Event type. One of the following: • Config This event type is generated when the device configuration is modified. When device configuration differs from QPM stored configuration, QPM monitoring and provisioning features are affected. For this event type, you can use all the available options–Rediscover, Import, and Deploy. • IOS This event type is generated when the device image is upgraded or modified. Any change in device image affects device monitoring from QPM. For this event type, you can use the available options Rediscover and Import. The Deploy option is not applicable to this event type.

Table D-29 NCM Events: Live Events Page (continued)

Field	Description
Modification	One of the following: • Configuration link—Link to CLI commands in the device configuration The View CLI Commands window appears showing the latest device configuration, and the following buttons: – Show Run—Click this button to view the device's running configuration sent with the NCM event message. – Configuration Diff—Click this button to view the configuration diff data sent with the NCM event. This is the device configuration change that triggered the event message. – Incremental Telnet—Click this button to view the difference in configuration between QPM stored device configuration and device's running configuration. In this case, QPM connects to the device and display the difference between device running configuration and QPM stored device configuration. This button is disabled if the device is not managed from QPM (the device name ends with "*") or not managed from current policy group (the device name ends with "**"). – Close—Click this button to close the window. These configuration change details help you to to identify whether the device config change is desirable or not. – If the changes are not desirable, you can restore the configuration stored with the QPM, using the Deploy option. – If the changes are desirable and affect QPM, you can update QPM with device configuration changes, using the Import option. • Image upgrade data sent with the NCM event
Last Action	Last action that you performed after the event appeared in QPM. The following actions (if you have performed any) are shown: • Rediscover • Import • Deploy For new events, this field shows `No action`.

Table D-29 NCM Events: Live Events Page (continued)

Field	Description
Rediscover	Click to rediscover the devices corresponding to the selected events. The Discovery Status page appears. The Rediscover action is needed, since any change in the device image or configuration can affect the monitoring of the device from QPM. The Discovery Status page shows only one Job Type even if you chose to rediscover more devices. You can find the number of devices being discovered from the In Progress column.
Import	Click to import the QoS configuration from the devices (corresponding to selected events) to QPM. The Import QoS from Devices page appears. You can perform this action when you find that the device configuration change will affect the device provisioning and monitoring from QPM. Even if you select multiple events from the same device, and click Import, only one Import QoS task is launched for the device.
Deploy	Click to deploy the QoS configuration from QPM to the devices corresponding to the selected events. The Pending Jobs page appears. The Deploy action helps you to restore the device configuration from QPM if you feel that the configuration change that occurred on the device is wrong. Even if you select multiple events from the same device, and click Deploy, only one policy deployment task is launched for the device.

Baseline Monitoring

The following topics describe the pages that can be accessed from the Baseline Monitoring option:

- Baseline Monitoring: Historical Monitoring Page, page D-37
- Baseline Monitoring: Real Time Monitoring, page D-41

Baseline Monitoring: Historical Monitoring Page

Use this page to:

- View, create, edit, delete, and stop historical monitoring tasks that conform to NBAR PD (Protocol Discovery)
- View NBAR PD historical monitoring charts
- Export collected data from tasks.

To open this page, choose **Monitoring > Baseline Monitoring > Historical Monitoring**.

Historical monitoring tasks collect data for historical monitoring charts.

When the historical QoS analysis data collected by QPM reaches the configured disk space limit, the following happens:

- All running monitoring tasks are stopped automatically, and are set to the status "Stopped due to out of disk space."
- The next time you open the Historical Monitoring page, a message notifies you that the disk space limit was reached and provides recover instructions. This message only appears on the Historical Monitoring page. You will not receive notification that the disk space limit was reached until you open this page.

All data collected before the tasks were stopped is available for display in reports. To free the necessary disk space and continue monitoring, you must delete the stopped tasks and run the database rebuild utility. Then you can recreate the deleted tasks to resume running them.

Table D-30 describes the fields in the Baseline Monitoring: Historical Monitoring page.

Table D-30 Baseline Monitoring: Historical Monitoring Page

Field	Description
Name	Name of the NBAR PD monitoring task. If you have selected the Job Frequency as daily, weekly, bi-weekly, or monthly, this column displays multiple tasks with the same name. You can differentiate the tasks by looking at the Start Time and End Time.
Description	Task description.
Start Time	Start time of the corresponding task.
End Time	End time of the corresponding task.
Task Type	Type of monitoring task—NBAR
Status	Task status. The following are the possible statuses: • Processing—The initial status for tasks, indicating the task is being created. • Running—Task is running correctly and collecting data. • Stopped—Task was stopped by user request. • Stopped due to disk space limit—The amount of collected data reached the configured disk space limit. • Collector Error—Task could not be created because of a data collection error. One possible reason of this error is that the SNMP community string has been changed directly on the device while the device is undergoing a monitoring task. • In Edit—The task is disabled, and has not started yet. • Finished—The task successfully finished. It will not collect any more data.
View Report button	Click to view the Historical Monitoring charts of the selected task.
Create button	Click to create a new task. The Create Task window appears.

Table D-30 Baseline Monitoring: Historical Monitoring Page (continued)

Field	Description
Edit button	Click to edit a task with an error status. The Task Definition page appears. You can edit tasks with the following statuses: • Collector Error • In Edit
Delete button	Click to delete the selected task. A confirmation dialog box opens.
Stop button	Click to stop a running task.
Export Data button	Click to export a task's collected monitoring data to a zip file that contains a set of XML data files. The browser file download process starts. Ensure that you have the unzip application to recreate the folder structure of the zipped files when unzipping them. Each interface has a separate folder. Within each folder is a separate file for each policy defined on the interface.
Refresh Rate	Select a page refresh rate from the list. The refresh rate determines how often the page refreshes with updated information.

The following topics describe the pages that are accessed from the Baseline Monitoring: Historical Monitoring page:

- Baseline Monitoring: Create Task Dialog Box, page D-39
- Baseline Monitoring: Historical Charts Page, page D-40

Baseline Monitoring: Create Task Dialog Box

Use this dialog box to create Historical Monitoring tasks for NBAR PD (Protocol Discovery).

To open the Create Task dialog box (Table D-31), in the Baseline Monitoring: Historical Monitoring page, click **Create**.

Table D-31 Create Task Dialog Box

Field	Description
Name	Enter the name of the Historical Monitoring Task
Start Time	Enter the start date and time for the task. You should enter the date in MM/DD/YYYY format, or you can use the calender icon to select the date. You should enter the time in a 24-hour format.
End Time	Enter the end date and time for the task. You should enter the date in MM/DD/YYYY format, or you can use the calender icon to select the date. You should enter the time in a 24-hour format.
Polling Interval	Select the polling interval (in minutes) for the monitoring task

Table D-31 Create Task Dialog Box (continued)

Field	Description
Job Frequency	Select the frequency of the monitoring job as daily, weekly, bi-weekly, or monthly. QPM creates separate monitoring tasks based on this frequency, so that you can view separate Historical Monitoring reports for specific periods. If you select the Default option for Job Frequency, you will be able to see only one historical monitoring report for the entire period.
Description	Enter a description for the task
Enabled	Check this to enable historical monitoring at the specified period
Create Task button	Click this to save and apply the task details
Object Selector	Lists all the devices and interfaces that are compatible with NBAR PD monitoring. Select the interface that you want to monitor.

Baseline Monitoring: Historical Charts Page

Use this page to monitor protocols in the In and Out directions of the traffic through the interface.

To open the Historical Charts page (Table D-32), select a monitoring task, and click **View Report**.

Table D-32 Historical Charts Page for NBAR PD Analysis

Field	Description
Graph Type	Select the graph type to display: • Line—Presents data in a line chart format. • Bar—Presents data in a bar chart format.
Data Type	Select the units to display in the graphs: • Packets—Displays the packet count of the data. • Bytes—Displays the byte count of the data. • Bits—Displays data flow rate in bits per second.
Device/Interface	Displays the device and the interface that you selected while creating the task.
Protocol Name row	Displays the names of the top 10 protocols at the last polling time.
Byte Count Sum (In and Out) row	Displays the sum of in and out byte count corresponding to the protocol displayed in the Protocol Name row

Table D-32 Historical Charts Page for NBAR PD Analysis (continued)

Field	Description
NBAR Protocol Selection	• Available—Displays all the protocols present in the traffic Select the protocols that you want to monitor through the graph, and move it to Selected. You can select maximum 10 protocols for monitoring. If you move a protocol to Selected list, it is no longer displayed in the Available list. • Selected—Displays the protocols you selected for monitoring through the graphs. The maximum number of protocols allowed in this list is 10. You can remove a protocol from the list by moving it to Available.
NBAR Historical In Direction Report	Displays the graph of inbound traffic based on the protocols available in the Selected list. The Y-axis values depends on the Data Type you selected. The X-axis shows the Poll Time (in minutes) based on the polling interval you selected for the task. This graph refreshes to show the correct data whenever you change the protocol selection.
NBAR Historical Out Direction Report	Displays the graph of outbound traffic based on the protocols available in the Selected list. The Y-axis values depends on the Data Type you selected. The X-axis shows the Poll Time (in minutes) based on the polling interval you selected for the task. This graph refreshes to show the correct data whenever you change the protocol selection.
Traffic Distribution Chart - Top 10	Displays a pie chart of the first ten protocols that passed through the interface during the selected time interval. The data shown in the graph is the sum of ingress and egress (In and Out) data for the protocols, based on the selected data unit.

Baseline Monitoring: Real Time Monitoring

Use this page to view the real-time chart of protocols for a selected device interface that supports NBAR PD (Protocol Discovery) monitoring .

To open this page, choose **Monitoring > Baseline Monitoring > Real Time Monitoring**.

The Real Time Monitoring page allows you to select devices only from the active device group.

Note For NBAR PD monitoring of the supported devices , you should configure the SNMP RW community string on the device.

To view the real-time chart for a device interface, select the interface from the Select Device Interface pane and click **Show Real Time Chart**. The Real Time Charts window appears.

Real Time Charts Window

Use this window to view a real-time monitoring report of the protocols on a device interface that supports NBAR PD monitoring.

To open this window, select a device interface from the Select Device Interface pane, and click **Show Real Time Chart** in the page.

If a device is not successfully polled (for example, when a device is unreachable, or the SNMP community string has been changed on the device directly while being polled), 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.

Table D-33 NBAR PD: Real Time Charts window

Field	Description
Graph Type	Select the graph type to display: • Line—Presents data in a line chart format. • Bar—Presents data in a bar chart format.
Units	Select the units to display in the table and the graphs: • Packets—Displays the packet count of data flow • Bytes—Displays the byte count of data flow • Bits/second—Displays data flow rate in bits per second
Task Name	Displays the name of the task.
Task Start Time	Displays the start time of the task (when the report was run).
Device	Displays the device name of the device that is monitored in the report.
Interface	Displays the interface name of the interface that is monitored in the report.
Actual Polling Interval	Displays the polling interval at which the task polls for data. This interval might be different than the polling interval configured for the task. If QPM is not able to poll at the interval configured for the task, it will determine the shortest interval at which it can poll. This value is displayed in this field.
Protocol Selection table	Displays all the protocols traversing the interface and the difference in the traffic rate for each protocol. The traffic rate displayed for each protocol depends on the unit you selected. To analyze any particular protocol, click the name of the protocol. The corresponding charts are displayed for both in and out directions.

Table D-33 NBAR PD: Real Time Charts window (continued)

Field	Description
Traffic Distribution Chart - Top 10	Displays a pie chart of the first ten protocols passing through the interface. The data shown in the graph is the sum of ingress and egress (In and Out) data for the protocol, based on the selected data unit.
Selected Protocol In Direction Report based on *units*	Displays the chart of the inbound traffic through the interface corresponding to the selected protocol. The value displayed in the graph is the difference in the traffic rates for the selected protocol. This is same as the value displayed in the table.
Selected Protocol Out Direction Report based on *units*	Displays the chart of the outbound traffic through the interface corresponding to the selected protocol. The value displayed in the graph is the difference in the traffic rates for the selected protocol. This is same as the value displayed in the table.
Close Window button	Click this button to close the chart window.