CA Spectrum®

QoS Manager User Guide

Release 9.4

CA Technologies Product References

This document references the following CA Technologies products:

- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA Spectrum QoS Manager

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

This section contains the following topics:

About Quality of Service (QoS) Manager

CA Spectrum QoS Manager facilitates IP fault and performance management of networks that are configured for Quality of Service. QoS is deployed in IP data networks that carry traffic from services such as Voice Over IP (VoIP), order processing, and video conferences. QoS on routers lets the infrastructure serve the unique performance requirements of each service.

The QoS Manager performs the following tasks:

- Provides visibility into the health and performance of QoS traffic classes across the network.
- Automatically discovers QoS classes and policies on your network and maps them to the associated physical routers and interfaces.
- Creates models to represent each QoS policy, QoS traffic class, and QoS behavior.
- Creates traffic-class collections so you can view all identical traffic class models implemented on devices across the landscape.

QoS Manager also lets you drill down to per-class statistics such as packet drops, queue size, and pre-policy rates. You can view the individual performance statistics based on the QoS configuration type.

This guide explains how to configure, discover, and manage the QoS elements in your network using CA Spectrum.

Note: Only Cisco devices that feature CISCO-CLASS-BASED-QOS MIB are supported.

Access the QoS Manager Interface

You can access the QoS Manager interface through the OneClick Console.

Follow these steps:

1. Launch the OneClick console from the OneClick homepage

   The OneClick Navigation panel displays.

2. Expand the appropriate landscape in the Explorer tab and select QoS Manager.

   The QoS Manager interface appears.

Note: For information on using the OneClick Console, see the *Operator Guide.*

Model Types

The following model types are available in the hierarchical view of the QoS Manager interface:

QosManager

Identifies the specific QoS Manager installation for a CA Spectrum landscape. Use this model type to configure alarm thresholds, launch QoS Discovery, and enable performance and report functionality.

Note: You need administrator privileges to use these configuration options.

QosPolicy

Defines the QoS policies that are set on your network. You can view general information, associated devices, and associated traffic classes of these models.

QosClassCollection

Lets you view all identical traffic class models across devices on your network. You can view general information, associated devices, and associated traffic classes of these models.

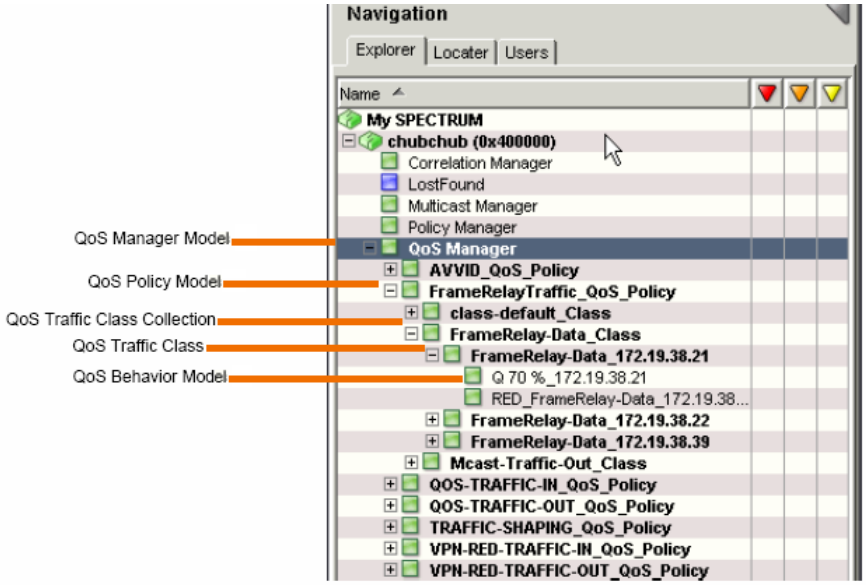
QosTrafficClass

Identifies the traffic classes that are defined on your network. You can view general information, associated devices, and associated behaviors of these models.

Behavior

Represents the behaviors per each hop defined on your network. There are four behavior model types: QosQueueing, QosRandomDetect, QosPolicing, and QosTrafficShaping. You can view the general information and performance statistics of these model types.

The following diagram shows the QoS Manager navigation hierarchy:



Search Options

The following search options are available on the OneClick Locater tab:

All Behaviors

Finds all QoS behaviors defined on selected landscapes.

All QoS Managers

Finds all QoS Manager models.

All QoS Policy Models

Finds all QoS policies defined on selected landscapes.

All QoS Services

Currently, this search is not enabled.

All Traffic Class Collections

Finds all Traffic Class Collection models defined on selected landscapes.

All Traffic Classes

Finds all Traffic Class models defined on selected landscapes.

Behavior By

Finds Behavior models by behavior, interface, name, or router.

QoS Policy By

Finds QoS Policy models by behavior, interface, name, or router.

Traffic Class By

Finds Traffic Class models by behavior, interface, name, or router.

Note: For more information on the Locater tab and performing a search, see the *Operator Guide*.

Chapter 2: QoS Manager Configuration

This section contains the following topics:

Access Configuration Parameters

The QoS Manager configuration parameters are provided in the Component Detail panel of the QoS Manager model. The Component Detail panel has three sections:

- General Information
- Configuration
- Traffic Behavior Alarm Thresholds

You should review these configuration parameters before you begin working with the QoS Manager to help ensure that the QoS Manager is set up to meet your network management needs.

Note: You need administrator privileges to make configuration changes.

QoS Manager Models

The following information can be accessed from the Information tab in the Component Detail panel for each QoS Manager model:

General Information

Displays the following general information about traffic class:

Model Class

Indicates the model class for the QoS Manager model.

Note: For more information on a model type's model class, see the *Concepts Guide*.

Creation Time

Indicates the date and time that this QoS Manager model was created.

Security String

Indicates the security string for the QoS Manager model. If you have the required privileges, you can modify the security string by clicking Set, entering the security string into the available field, and clicking Save.

Notes

Indicates the notes available for the QoS Manager. If you have the required privileges, you can add notes by clicking Set, entering the notes into the available field, and clicking Save.

Management Configuration

The Configuration section has the following parameters:

Enable Port Polling

Determines if the ports on a QoS-enabled device are polled.

Default: Yes

Enable Performance Alarms

Lets you enable or disable the generation of performance alarms. Performance alarms are generated when a threshold defined in a Behavior model's Performance Component Detail has been violated.

Default: Yes

Enable Device Alarms

Enables or disables the generation of alarms on QoS-enabled devices.

Default: Yes

Enable Statistic Polling

Enables the Performance Collection system.

Default: No

Statistic Polling Interval

Controls how frequently statistical information is obtained for use in performance calculations. However, this polling interval will have no effect unless Enable Statistic Polling is set to Yes.

Default: 300

Log Statistics to File

Enables you to send the performance statistics to a log file. No statistics will be captured and logged unless the Enable Statistic Polling parameter is set to Yes.

Default: True

Minutes Per Log File Cycle

Specifies how often a new log file is created. No statistics can be logged unless the enable Statistic Polling parameter is set to Yes. The frequency at which statistics are written to the log file is defined by the Statistic Polling Interval described above.

Traffic Class Percent Dropped Thresholds

The Traffic Class Percent Dropped Thresholds section lets you define the critical threshold, major threshold, and minor threshold for violations based on percentage of packets dropped in any traffic class.

These thresholds indicate when critical, major, and minor alarms will be generated on a traffic class model. The default values are as follows:

- Five percent for a critical alarm
- Three percent for a major alarm
- One percent for a minor alarm

QoS Manager Traffic Behavior Alarm Thresholds

The Traffic Behavior Alarm Thresholds section lets you set the critical threshold, major threshold, and minor threshold for each type of traffic behavior, including policing percent dropped, queueing percent dropped, random early detect percent dropped, and traffic shaping percent dropped.

Each threshold sets percentage level of packets dropped that will cause a specific level of alarm. The default values are as follows:

- Five percent for a critical alarm
- Three percent for a major alarm
- One percent for a minor alarm

Chapter 3: QoS Manager Discovery and Modeling

This section contains the following topics:

Device Discovery

CA Spectrum discovers and models the physical network infrastructure through OneClick Discovery, manual modeling, or the Modeling Gateway. Before using QoS Discovery, use one of these methods to model the physical components of your network in CA Spectrum.

Note: Only Cisco devices that feature CISCO-CLASS-BASED-QOS MIB are supported. For more information, see the *Certification User Guide*, the *Administrator Guide*, and the *Modeling Gateway Toolkit Guide.*

QoS Manager requires that each QoS class have a unique name.

Reconfigure a QoS Device

If any of the QoS devices on your network were modeled before you installed QoS Manager, reconfigure them to create application models. Run the Reconfigure Model command on each of these models. Reconfiguration creates the CiscoCBQoSApp model, which supports the CISCO-CLASS-BASED-QOS MIB. This application provides necessary information to the QoS Manager.

Follow these steps:

1. Select the device model on the Contents panel.
2. Expand the Reconfiguration option on the Information tab in the Component Detail panel.
3. Click the Reconfigure Model button.

   The QoS application model is created for the device.

Run an On-Demand QoS Discovery

Use the QoS Discovery feature to discover and model the QoS policies, traffic classes, and behaviors defined on your network.

Note: If a QoS network element discovered and modeled by the QoS Manager is deleted from the network configuration, manually remove it from the modeled QoS hierarchy. It is not automatically removed by QoS Manager.

Follow these steps:

1. Select the QoS Manager model in the Explorer.
2. Select the Information tab in the Component Detail panel.
3. Select the Configuration option in the Component Detail panel.
4. Select the QoS Discovery option and click Run.

   The status bar indicates that the Discovery is running. Once the Discovery is complete, status returns to idle.

Note: Administrator privileges are required to run QoS Discovery.

More information:

Filter Traffic Class Names During Discovery (see page 16)

Filter Traffic Class Names During Discovery

The QoS Manager lets you filter the Traffic Class during Discovery.

Follow these steps:

1. Select QoS Manager in the Explorer tab.
2. Select the Information tab in the Contents panel.

   The configuration options for QoS Manager appear.
3. Expand the QoS Discovery subview.

   The Discovery options that are available include the following settings:

   Traffic Class Filter Type

   Determines if the Traffic Class in the 'Traffic Class Filter' field are included or excluded from modeling. Options include the following:

   - Exclusive
   - Inclusive

Traffic Class Filter

Lists the Traffic Classes to be included or excluded when the QoS Discovery is run. This field is used with the 'Traffic Class Filter Type' field.

Note: The Traffic Classes are not filtered and saved unless you add them in the Traffic Class Filter. Even if the Traffic Class Filter Type is inclusive and the Traffic Class Filter is empty, all Traffic Classes are discovered.

More information:

Run an On-Demand QoS Discovery (see page 16)

QoS Manager Model Naming Convention

During QoS Discovery, the QoS Manager assigns model names to policy, class collection, traffic class, and behavior models using the following conventions:

QoS Policy models

<*xxx*>_QosPolicy where <*xxx*> is the policy name assigned by the user who created the policy in the device's IOS Configuration.

Traffic Class Collection models

<*xxx*>_Class where <*xxx*> is the name of the traffic class assigned by the user who configured it.

Traffic Class models

<*xxx*>_QosPolicy_<yyy>_<*DeviceModelName*>, where:

- <*xxx*> is the policy name assigned by the user who created the policy in the IOS Configuration of the device.
- <*yyy*> is the name of the traffic class assigned by the user who configured it.
- <*DeviceModelName*> is the device model name the user assigned to the device model using the traffic class.

Behavior models

Behavior models can be one of the following:

Queuing Behavior Models

Q <*Bandwidth Units*> <*DeviceModelName*> where <*Bandwidth Units*> is the units of bandwidth used for queuing and <*DeviceModelName*> is the device model name the user assigned to the device model using the traffic class.

RED Behavior Models

RED_<*ParentModelName*> where <*ParentModelName*> is the name of the parent traffic class model.

Policing Behavior Models

Policing <Rate> <*DeviceModelName*> where <*Rate*> is the assigned policing rate and <*DeviceModelName*> is the device model name the user assigned to the device model using the traffic class.

Traffic Shaping Behavior Models

TrafShaping <*Rate*> <*DeviceModelName*> where <*Rate*> is the assigned traffic shaping rate and <*DeviceModelName*> is the device model name the user assigned to the device model using the traffic class.

Change Policy and Class Model Names

You can change the default name that is assigned to a policy or class model.

Follow these steps:

1. Click the set link next to the model name on the Information tab.
2. Enter the new model name in the text box provided.

   The default name is changed.

Run QoS Discovery on Selected Models

You can configure the QoS Network Services Discovery from the OneClick views that display models. Then run QoS Network Services Discovery on selected models.

Follow these steps:

1. Select the models.
2. Click Tools, Utilities, Network Services Discoveries, QoS Discovery.

   The Discovery process is initiated. You can check the status in the Configuration subview.

Configuring QoS Discovery During Modeling

CA Spectrum lets you configure Network Services Discoveries, including QoS, during modeling. As a part of modeling configuration, you can specify which network service discoveries to run with the modeling process.

Note: For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide.*

Chapter 4: Model Types

This section contains the following topics:

QoS Policy Models

The following information can be accessed from the Information tab in the Component Detail panel for each QoS policy model.

General Information

Displays the following general information about a QoS policy model:

Condition

Defines the condition of the QoS policy model, which reflects the alarms that may be present on the model.

Entity Condition

Indicates the calculated value of the model condition, which is based on the models that make up the QoS policy.

Model Class

Specifies the model class of the QoS policy model.

Policy ID

Indicates the policy identifier defined when the policy was created.

Policy Type

Indicates the policy type selected when the policy was created.

Security String

Defines the security string for this model. To change this value, click Set and enter the changes you want to make in the field provided. You must have administrator privileges to make changes to this field.

Landscape

Defines the CA Spectrum landscape on which the policy exists.

Description

Defines the description entered when the policy was created.

Associated Devices

Displays a table that shows all the devices that use this policy.

Associated Traffic Classes

Displays a table that shows all the traffic classes that are affiliated with this policy.

Traffic Class Collection Models

The following information can be accessed from the Information tab in the Component Detail panel for each traffic class collection model.

General Information

Displays the following general information about a traffic class collection model:

Condition

Defines the condition of the traffic class collection model. This condition reflects the alarms that may be present on the model.

Entity Condition

Indicates the calculated value of the model condition, which is based on the models that make up the traffic class collection.

Traffic ID

Indicates the identifier defined when the traffic class collection was created. It uniquely identifies this traffic class collection.

Model Class

Defines the model class of the traffic class collection model.

Security String

Defines the security string for this model. To change this value, click Set and enter the changes you want to make in the field provided. You must have administrator privileges to make changes to this field.

Landscape

Defines the CA Spectrum landscape on which this traffic class collection exists.

Description

Indicates the description entered for this traffic class collection when it was defined.

Associated Devices

Displays a table that lists all of the devices that use the traffic classes contained in this traffic class collection.

Associated Traffic Classes

Displays a table that lists all of the traffic class models that make up this collection.

Traffic Class Models

The following information can be accessed from the Information tab in the Component Detail panel for each traffic class model.

General Information

Displays the following general information about a traffic class model:

Condition

Defines the condition of the traffic class model. This condition reflects the alarms that may be present on the model.

Entity Condition

Indicates the calculated value of the model condition, which is based on the models that make up the traffic class.

Model Class

Defines the model class of the traffic class model.

Traffic ID

Indicates the identifier defined when the traffic class was created. It uniquely identifies this traffic class. This is made up of the traffic class collection ID and the IP address of the interface that implements this traffic class.

Security String

Defines the security string for this model. To change this value, click Set and enter the changes you want to make in the field provided. You must have administrator privileges to make changes to this field.

Landscape

Defines the CA Spectrum landscape on which this traffic class exists.

Match Statement

Defines the match statement defined for this traffic class. A match statement defines specific match criteria to identify packets for classification purposes.

Description

Indicates the description entered when this traffic class was created.

Drop Rate

Specifies the rate of packets dropped aggregated across all interfaces supporting this traffic class.

No Buffer Drops

Indicates the drop packet count, aggregated across all interfaces supporting this traffic class, which occurred due to a lack of SRAM buffers during output processing on this interface.

Associated Devices

Displays a table that lists all of the devices that use this traffic class.

Associated Behaviors

Displays a table that lists all of the behaviors that are applied to this traffic class.

Behavior Models

The following information can be accessed from the Information tab in the Component Detail panel for each behavior model.

General Information

Displays the following general information about a Behavior model:

Condition

Defines the condition of the Behavior model. This condition reflects the alarms that may be present on the model.

Entity Condition

Indicates the calculated value of the model condition, which is based on the interface models that use the behavior.

Model Class

Indicates the model class of the Behavior model.

Security String

Defines the security string for this model. To change this value, click Set and enter the changes you want to make in the field provided. You must have administrator privileges to make changes to this field.

Behavior ID

Indicates the identifier defined when the behavior was defined. It uniquely identifies this behavior.

Landscape

Defines the CA Spectrum landscape on which this behavior exists.

Performance

See Behavior Model Performance (see page 26) for the parameters provided in this selection.

QoS Alarms

QoS Manager generates alarms based on the configuration parameters you define. These alarms help define the status or condition of each of the modeled QoS components.

You can set a critical, major, and minor threshold for each type of behavior and traffic class model. Each threshold sets percentage level of packets dropped that will cause a specific level of alarm.

You can also enable the generation of alarms on QoS-enabled device models by setting the Enable Device Alarms parameter in the QoS Policy Manager model's Management Configuration to yes. The QoS Manager also generates alarms if there are problems logging statistical data.

The QoS Manager generates the following alarms:

0x4b30401

Defines the alarm generated on a QoS-enabled device model if one of the QoS Components exceeds a defined threshold.

0x4b30506

Defines the alarm generated on a behavior or traffic class model if the threshold set for a critical alarm is violated.

0x4b3050a

Defines the alarm generated on a behavior or traffic class model when the threshold set for a minor alarm is violated.

0x4b30000

Indicates that the statistics log file could not be opened for writing. Because of this, at least one polling cycle's statistics will not be logged. This data is needed by other applications to determine the status of the network.

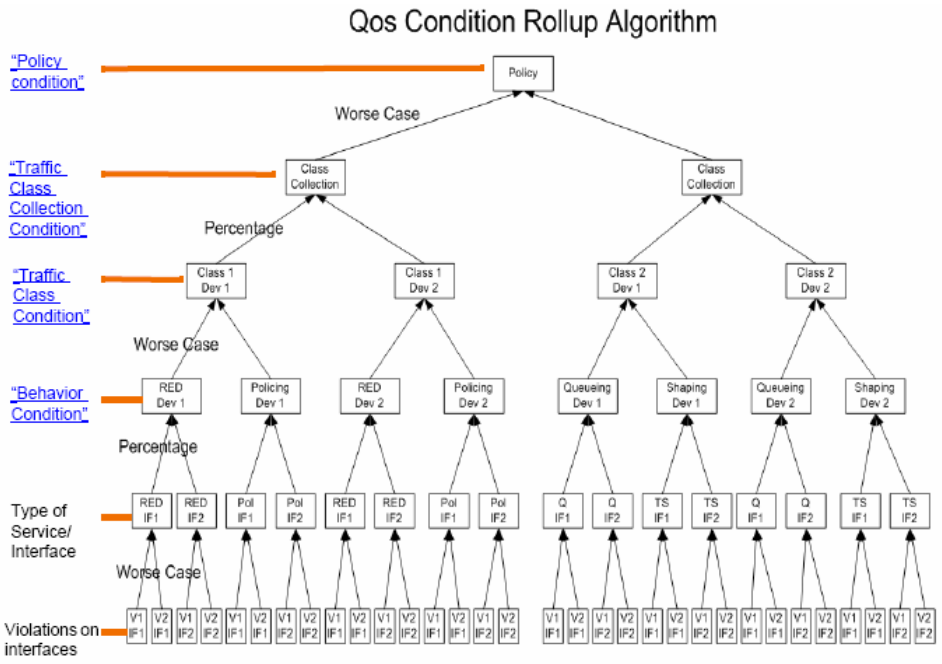
0x4b30001

Indicates that the statistics log file could not be closed. This may cause the statistical data to be lost and unused by other applications that may need it.

QoS Conditions

QoS Manager uses the QoS Condition Rollup algorithm to determine the entity condition of policy, traffic class collection, traffic class, and behavior models.

The following diagram illustrates the QoS Condition Rollup algorithm:



The conditions are as follows:

Policy

Is computed based on the status of the Class Collections contained in the policy. The condition of the Policy model is the worst condition found among all of the Traffic Class models monitored by the policy.

Traffic Class Collection

Is based on the status of the Traffic Class models contained in the collection. QoS Manager finds the condition that exists on the highest percentage of traffic classes contained in the collection. This predominant condition becomes the condition of the Traffic Class Collection model.

For example, if 45 percent of the traffic class models in the collection had a green condition, 10 percent had a red condition, and 20 percent had an orange condition, and 25 percent had a yellow condition, the condition of the collection would be green.

Traffic Class

Is based on the status of the Behavior models that are associated with the Traffic Class model. The condition of the traffic class model is the worst condition, or “worst case” found amongst all of the Behavior models in the traffic class.

Behavior

Is determined by the thresholds settings defined in QoS Manager traffic behavior alarm thresholds. These thresholds watch the percentage of dropped packets on a device for each specific service (queueing, random early detection, policing, or shaping) and designate what percentage level will generate a critical, major, and minor alarm condition.

The percentage measurement used for these thresholds is derived from the average percentage of packets dropped for a particular service across all interfaces of the device. The percentage of packets dropped on each interface is equal to the worst percentage drop for a particular type of service on an interface.

QoS Performance

QoS Manager presents performance analysis information at both the traffic class and behavior level. In order for any of these statistics to be available, you must set the Enable Statistic Polling to Yes and set a value for the Statistic Polling Interval. These parameters can be found in the QoS Policy Manager model's Management Configuration.

View Traffic Class Performance Graphs

For each traffic class model, you can access graphed performance analysis based on Packet Drops and Pre-Policy Rate. The statistics for the graphs are derived from values in the CISCO-CLASS-BASED-QOS MIB.

To view traffic class performance graphs

1. Click the appropriate traffic class model in the OneClick Navigator.
2. Click the Performance tab in the Component Detail panel.
3. Select a graph from the drop-down list.

   The performance graph opens.

Behavior Model Performance

Performance information is available for each behavior model. The performance statistics provided depend on the type of service monitored by the behavior. These types of services are:

- queueing
- shaping
- policing
- random early detection

The statistics are derived from values in the individual service's Configuration and Statistics tables in the CISCO-CLASS-BASED-QOS MIB.

Note: The statistics provided for queueing (Mean Queue Depth), random early detection (Mean Queue Size), and shaping (Current Queue Size) are averages of the values gathered from each interface passing traffic for the given the service on the device. All other statistics are totals of values gathered from each interface passing traffic for the given service on the device.

Each behavior model has two ways to access performance information. The first method is to access the Information tab in the behavior model's Component Detail panel. This tab has a selection called Performance, which displays different statistics depending on the type of service the behavior model monitors. The data in this section does not refresh dynamically. To refresh the data, click the Refresh button.

This section also shows the critical, major, and minor percent violation thresholds for the behavior. These thresholds are set in the section QoS Manager traffic behavior alarm thresholds.

In addition, you can display the behavior model's performance information graphically by choosing the Performance tab in the behavior model's Component Detail panel. The graphs depend on the type of service the behavior model monitors. The data in these graphs refreshes dynamically.

Queueing Behavior Models

The following performance statistics are available on the Information tab for a queueing behavior model:

Configured Bandwidth

Indicates the configured bandwidth allocated to this traffic class.

Total Discarded Packets

Indicates the number of packets, associated with this class, that were dropped by queueing.

Average Queue Depth

Indicates the average queue depth in packets. This is an average of an average, because each value averaged by this statistic is based on the average queue depth for each interface.

The following performance graphs are available on the Performance tab for a queueing behavior model:

Queue Depth

Displays the value of the Average Queue Depth statistic over time.

Discard Rate

Displays the value of the Total Discarded Packets statistic over time.

Shaping Behavior Models

The following statistics are available in the Performance section of the Information tab for a shaping behavior model:

Configured Burst Size

Indicates the amount of traffic, in bits, in excess of the committed traffic-shaping rate that is instantaneously permitted.

Configured Extended Burst Size

Indicates the amount of traffic, in bits, in excess of the burst limit, which may be conditionally permitted.

Configured Traffic Shaping Rate

Displays the current adaptive traffic shaping rate.

Total Delayed Packets

Displays the total number of packets delayed.

Total Dropped Packets

Displays the total number of packets dropped.

Average Queue Size

Displays the traffic shaping queue depth in packets. Note that this is actually an average of an average, since each value averaged by this statistic is based on the average queue size for each interface.

The following performance graphs are available in the Performance tab for a shaping behavior model:

Queue Size

Displays the value of the Average Queue Size statistic over time.

Delays and Drops

Displays the values of the Total Delayed Packets and Total Dropped Packets statistics over time.

Policing Behavior Models

The following statistics are available in the Performance section of the Information tab for a policing behavior model:

Configured Burst Size

Indicates the amount of traffic, in bytes, in excess of the committed policing rate that is permitted.

Configured Extended Burst Size

Indicates the amount of traffic, in bytes, in excess of the burst limit, which may be conditionally permitted by the policing feature. The probability that the traffic is not permitted increases as the received burst size increases.

Configured Policing Rate

Indicates the committed policing rate. This is the sustained rate permitted by policing.

Total Exceeded Packets

Indicates the number of packets treated as non-conforming by the policing service.

Total Violated Packets

Indicates the number of packets treated as violated by the policing service.

The Violated and Exceeded Packets graph is available in the Performance tab for a policing behavior model. This graph shows the values of the Total Exceeded Packets and the Total Violated Packets over time.

Random Early Detection Behavior Models

The following statistics are available in the Performance section of the Information tab for a random early detection behavior model:

Configured Decay Factor

Indicates the decay factor for the queue average calculation. The decay factor is equal to raising 2 to the power of N, where N could be up to 16. The smaller the number, the faster the decay.

Configured Mean Queue Size

Indicates the configured average queue size computed and used by the WRED algorithm.

Mean Queue Size

Indicates the average queue size computed and used by the WRED algorithm.

Total Random Drops

Indicates the number of packets dropped when the number of packets in the associated queue was greater than the minimum configured threshold and less than the maximum configured threshold.

Total Tail Drops

Indicates the number of packets dropped when the number of packets in the associated queue was greater than the maximum configured threshold.

The Mean Queue Size and Drops graph is available in the Performance tab for a random early detection behavior model. This graph shows the Mean Queue Size, Total Random Drops, and Total Tail Drops over time.

Index