Getting Started Guide for the Cisco Bandwidth Quality Manager, Release 3.2

May 14 ,, 2007, OL-11095-03

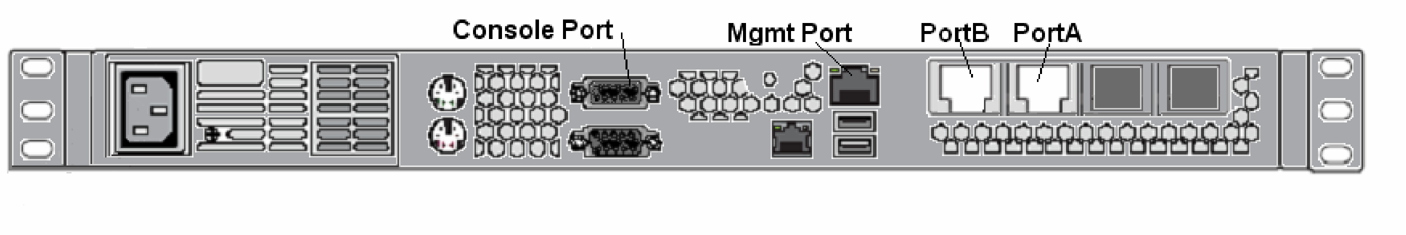
Overview

This release of Cisco Bandwidth Quality Manager (BQM) software runs on the following platforms:

- Cisco Application Deployment Engine 1010
- Cisco Application Deployment Engine 2120

The Cisco Application Deployment Engine (ADE) 1010 and the Cisco Application Deployment Engine (ADE) 2120 have the capability to monitor Fast Ethernet and Gigabit Ethernet links. For monitoring Gigabit Ethernet, the Cisco ADE 2120 also supports optical interfaces (SX). Figure 1 shows the two-port Cisco ADE 2120 back panel, highlighting the Cisco ADE 2120 measurement ports, the console port and Ethernet management port.

Figure 1 Cisco ADE 2120 Two-Port Rear Panel Features



Corporate Headquarters:
Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA

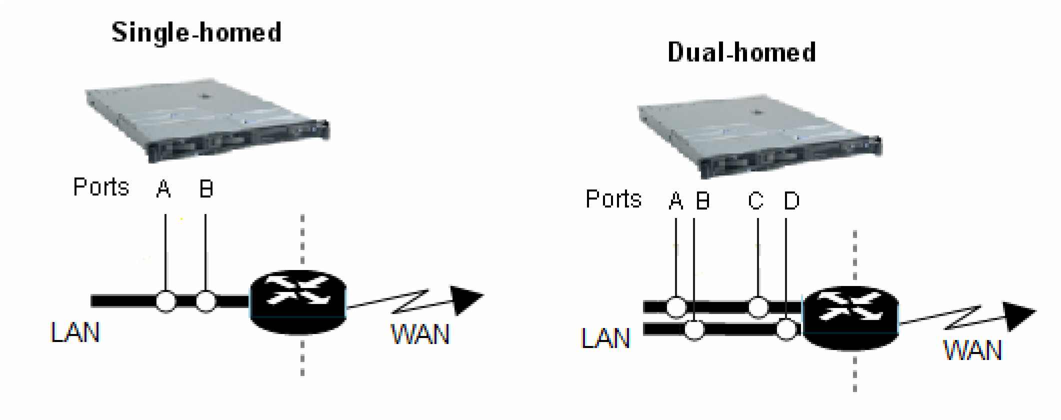
The following table describes the two-port Cisco ADE 2120 rear panel ports, connectors, and controls:

Table 1 Cisco ADE 2120 Two-Port Rear Panel Ports and Connectors

Item	Description
Measurement Ports	Measurement ports (PortA, PortB). For FastE/GigE electrical deployments: 100/1000 Ethernet. RJ-45 connector. For optical deployments: Gigabit Fiber SC connector. This diagram shows the two-port electrical model. For more information on the ports and connectors on the Cisco ADE 1010 and the single-port, two-port optical, and four-port Cisco ADE 2120 models, see the Installation Guide.
Console Port	The console port (DTE) supports a DB-9 connector with the following settings: 8 data bits, no parity, 1 stop bit, and the speed is 9600 bps. Use a null-modem cable when connecting to a laptop serial port to perform initial configuration.
Ethernet Management Port	Use the upper Ethernet connector as a management port to connect the device to an Ethernet network. You can also use a CAT5 cable to connect a laptop to the management port to perform initial configuration. The lower Ethernet port is not used.

The two-port Cisco ADE 2120 monitors the links either using passive taps or in a SPAN configuration. In dual-homed deployments, the four-port Cisco ADE 2120 model is used.

Figure 2: Two-port and Four-port Cisco ADE 2120 Deployments and Physical Measurement Ports



When you log in to the BQM GUI and view the default monitoring screens, information shown for the interface PortA is all the traffic being measured by the physical Port A on the Cisco ADE 2120. The interface PortAB displays information for all traffic in aggregate being measured by the Cisco ADE 2120 across both physical ports.

If you have received the Cisco ADE 2120 or Cisco ADE 1010 with a software installation CD, the next task is to install the BQM software. For instructions on software installation, see the Installation Guide.

If you have received the Cisco ADE 2120 or Cisco ADE 1010 with the BQM software preinstalled, see the following section on configuring an IP address for the device and installing a license.

Setting Up the Cisco ADE

You need to get the correct network addresses from your system administrator or consult your network plan to determine correct addresses before you set up the Cisco ADE:

- **IP Address** - IP address to be assigned to the Cisco ADE, for example 10.1.2.3. Consult your network administrator to obtain an unassigned address.
- **Net Mask** - Subnet mask for the subnet on which the Cisco ADE resides, for example 255.255.255.0
- **Gateway IP address** – IP address the Cisco ADE uses to reach other networks, for example 10.1.2.254. The gateway address is often the same as the site router address.
- **Domain Name Server** (optional) – IP address of the domain name server (DNS) the Cisco ADE can use to resolve host names. DNS requests are only sent on user demand.
- **Network Time Protocol Server** (optional) – IP address of the network time protocol (NTP) source the Cisco ADE can use to synchronize its clock.

Connecting to the Console Port

To perform the software installation procedure, you make a direct connection from a laptop to the Cisco ADE console port (DTE). You will need a null-modem cable to connect the laptop and Cisco ADE console ports.

The Cisco ADE console port supports a DB-9 interface with the following settings:

Bits per Second:	9600
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	Hardware

Examples of supported terminals include:

- tip (UNIX)
- minicom (Linux)
- HyperTerminal (Win32 with VT100 emulation)
- teraterm (Win32)

The following steps describe the procedure to set up the Cisco ADE on the first day of service:

Step 1 Log in as the admin user. The default admin password is ‘admin’. Only the admin user can configure the system for use.

Step 2 Use the **setup** command to perform basic configuration. You are prompted for each piece of configuration information required by the Cisco ADE to complete the configuration process.

```
host(config)$ setup
Please enter setup information ...

                     IP Address: 192.168.2.71
                        Netmask: 255.255.0.0
                         Prefix: 16
                         Router: 192.168.1.10
  Domain-Name-Server [optional]:
          Ntp server [optional]:
                       Hostname: nyc_hq
     current time and timezone :
14:39:37 19 October 2006 UTC  (UTC)
```

If you are setting up the Cisco ADE 1010, the single-port, two-port electrical, or four-port Cisco ADE 2120 models, you can skip the following step and go straight to the next section, “Setting System Time.”

Step 3 By default on the two-port Cisco ADE 2120 model, the release 3.2 software is configured to use electrical measurement ports. If you are setting up the two-port optical model of the Cisco ADE 2120, you need to specify that you will be using the two optical ports for traffic measurement. To do this you use the **media** command from the port context of the CLI.

```
host(config)$ port portA
host(config-port)$ media sfp
host(config-port)$ end
host(config)$ port portB
host(config-port)$ media sfp
host(config-port)$ end
```

The initial configuration is complete. The next task is to configure the system time, if required.

Setting System Time

The current system time and timezone are displayed when you complete the initial setup configuration. Check the displayed time to see if it is accurate. If you have configured a valid outside timing mechanism, such as a Network Time Protocol (NTP) source, during the setup procedure you need not set the software clock. Use the **clock set** command if no other time sources are available. The time specified in this command is assumed to be in the time zone specified by the configuration of the **clock timezone** command.

Setting the clock results in the Cisco ADE being rebooted to ensure consistency.

clock set *hh***:***mm***:***ss day month year*

The following example manually sets the software clock to 7:29 p.m. on January 13, 2007:

```
host(config)$ clock set 19:29:00 13 January 2003
```

Setting the Time Zone

To set the time zone for display purposes, use the **clock timezone** command. To set the time to Coordinated Universal Time (UTC), use the **no** form of this command:

clock timezone *zone*

For a full list of valid time zones, see the User Guide.

Installing a License

If the BQM software is unlicensed, the major features of the product are disabled. You are notified when you log in to the BQM CLI or GUI if there is no valid license.

Requests for licenses must be accompanied by the system ID. The System ID may be retrieved using the **status** command.

Licenses consist of a plain text file (file extension `.lic`) that must be installed on the Cisco ADE. If there is an attempt to install an invalid license, or a license that doesn't match the system ID, an error is reported and no license is installed.

To install the BQM license you use the **license** command from the CLI. You must be logged in to the CLI as an admin user to use this command.

license install tftp://[<hostname> | <A.B.C.D>]/*remote_filename*

For example, to install the specified license file from tftp host 192.168.10.1, use the following:

```
host(config)$ license install
tftp://192.168.10.1/BQM_license/BQM_0E456de6556aaa.lic
```

If the license has been installed, this command displays the text of the BQM license agreement when no arguments specified. To display the license agreement, you do the following:

```
host(config)$ license
```

Installing a License Using SSH

It is possible to install the license file directly using SSH. To perform the license installation procedure you need an ssh client. For Windows users, we recommend the OpenSSH client. The OpenSSH client may be downloaded from: http://sshwindows.sourceforge.net/download/

Note The 'plink' client (part of the puTTY distribution) is not suitable for this purpose). Also, if you already have an ssh client such as cygWin installed, attempting to install OpenSSH may cause problems.

Having received the license file, save it to your desktop.

On Windows, open a command prompt (Start >Run >'cmd');

On Linux, Solaris, or other Unix system, open a terminal window.

In either case, then run the following command:

```
ssh admin@name install license < licensefile.lic
```

where you should replace `name` with the DNS name or IP address of the Cisco ADE, and replace `licensefile.lic` with the full path and filename of the license file you receive. After entering the admin user password, the license will be installed. If there are any problems, you will see an error message.

Other Tasks

For more information on performing other initial tasks such as changing passwords and restricting access to the Cisco ADE, see the User Guide.

Accessing BQM

The first task is to open the BQM GUI. You need to use a Microsoft Windows machine with Internet Explorer 6.0 installed for this step. You open Microsoft Windows Internet Explorer 6.0, type in the following URL and press Enter or click the **Go** button on the browser:

```
http://<bqm_IP address>
```

If you have a DNS entry configured for the BQM, then you can use the configured DNS hostname:

```
http://<bqm_hostname>
```

This URL is not case sensitive.

For example, if the host name of the BQM is bqm_nyc, then the URL is as follows:

```
http://bqm_nyc
```

Logging in to BQM

The next step is to log in to BQM. The BQM software supports multiple simultaneous users. There are three user types (or roles) with different privileges and default passwords:

User name	Default Password
admin	admin
monitor (GUI only)	monitor
config	config

You must provide the correct user name and password combination to log in successfully.

Note It is strongly recommended that you change the default passwords. For more information on changing passwords, see the User Guide.

Alternatively, to perform configuration and system administration tasks, you can use telnet or ssh to access the BQM CLI. In this case you can use the same administrator user (admin) and default password (admin).

Verifying the Installation

If you have logged in to the GUI, you can verify the cabling of the physical hardware installation from the **Traffic Insight** tab.

When you first log in, and assuming the appliance has been measuring traffic for at least 15 minutes, open the **Traffic Insight** tab. To check the traffic being seen by PortA, select the interface **Local-site – bqm – PortA**. Select the **Talkers** tab and verify that the IP addresses of the listed talkers match those you would expect. You can do the same to check the traffic being measured by the other physical ports (PortB, PortC, PortD).

Performing Basic Configuration

The components of the network model configuration include the following:

- Local site
- Remote site(s)
- Site subnet(s)
- Router(s)
- Interface(s)

The following table describes the main components of the network model:

Table 2: Network Model Components

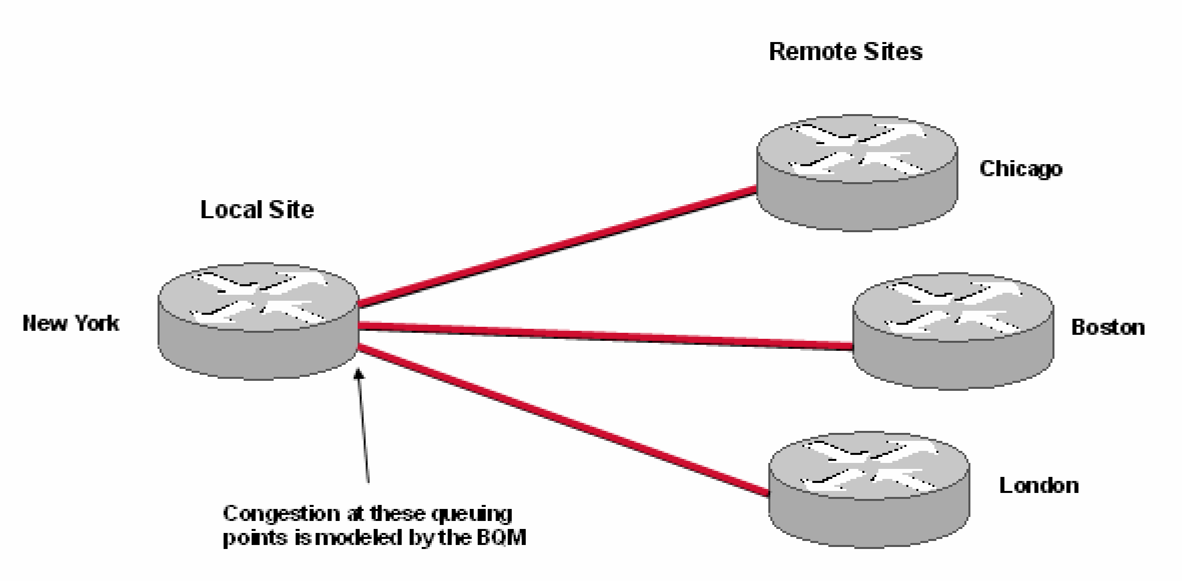
Component	Description
Local Site	A representation of a physical site where the Cisco ADE is installed in the network of interest. A local site is defined in the network model (at a minimum) by specifying network subnets.
Remote Site	A representation of a physical site that is connected to, but remote from, the local site in the network of interest. A remote site is defined (at a minimum) by specifying network subnets.
Site subnet	The subnet address that identifies a site. Traffic with the same destination address as the configured subnet address is considered to be inbound to the site. Traffic with the same source address as the configured subnet address is considered to be outbound from the site.
Router	A representation of a physical router installed in a location that is being represented in the network model by a local or remote site.
Interface	A representation of the interface(s) on a site router. The interface attributes configured should match those on the router being modeled as closely as possible. Interface results in Network Monitoring mode represent the traffic outbound from sites.
Peer-interface	A representation of the Service Provider router interface(s) to which local and remote site interfaces connect in an MPLS or Metro Ethernet network model. The peer-interface attributes configured should match those on the router being modeled as closely as possible. Peer-interface results in Network Monitoring mode represent the traffic inbound to sites.

The network model is used to take knowledge of the network topology and apply the BQM technology within it. You choose the supported network model deployment that most accurately captures the network configuration. The purpose of a local site is to represent the physical site where the Cisco ADE is installed in the network of interest. A local site is defined in the network model (at a minimum) by specifying network subnets.

The purpose of a remote site is to represent a physical site in the network that is connected to, but remote from, the local site. A remote site is defined (at a minimum) by specifying network subnets.

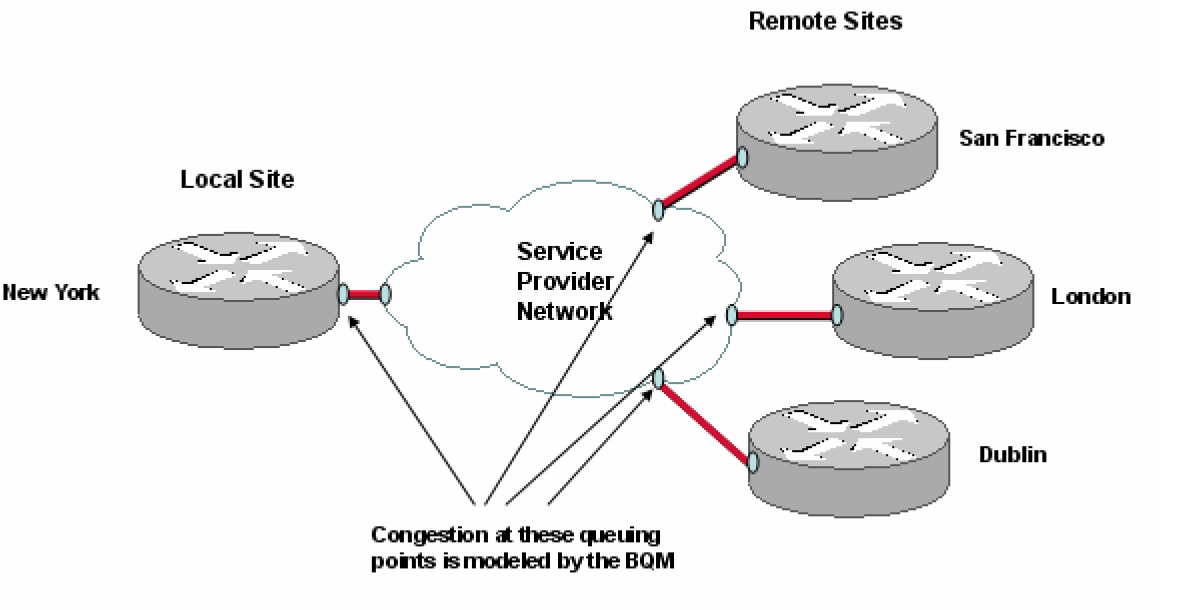
Each site comprises at least one router and its associated interfaces, configured to match the details of the network devices being modeled.

Figure 3: ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line (Point-to-Point) Network Model



In the example shown here, the local site is connected directly to three remote sites. The local site router has three interfaces being represented, with each interface connected to a single remote site router interface. All sites are identified by subnet addresses. The policy-maps configured on each router interface reflect the policy configurations on the physical routers being modeled. The Cisco ADE models and reports on congestion at the queuing points at local site interfaces.

Figure 4: MPLS VPN, Internet VPN, Private VPN Network Model



In the example shown here, the local site is connected via a Service Provider network to three remote sites. The local site router has one interface being represented, to the SP PE router. Similarly, the remote sites are each connected to an SP PE router on the other side of the network cloud. All sites are identified by subnet addresses.

The figure indicates that the interfaces on the SPN routers to which the local and remote sites connect are also modeled. They are called peer-interfaces in the BQM network model. When you are monitoring the network with BQM, the peer-interfaces represent the traffic inbound to sites, whereas the interfaces represent the traffic outbound from sites. The policy-maps configured on each router interface should reflect as closely as possible the policy configurations on the physical routers being modeled. BQM models and reports on congestion at the queuing points at the local site interface and remote site peer-interfaces.

Editing the Local Site

To configure BQM, you must log in as an admin user, and switch to **System Administration** mode.

Note If you are logged in as the admin user, you can switch back and forth to **Bandwidth Quality Manager** mode by selecting it from the **Mode** list.

The **Sites/Interfaces** page on the **Configuration** tab is displayed by default and shows the details of the default local site. You can change the default configuration of the local site by editing it.

Note The default local site cannot be deleted.

To edit the default local site configuration, you do the following:

Step 1 Click the named local site link or the **edit** link.

Step 2 The **Edit Local Site** page is displayed.

Step 3 Edit the name in the **Site Name** field as required.

Step 4 Enter a brief description of the site in the **Site Description** field.

Step 5 Enter the site subnet address and prefix in the **Subnet** field.

Note LAN subnets of the local site are only required if BQM will receive traffic from these subnets that is not destined for the WAN.

Step 6 To configure a router for the local site, click **Add Router**.

Editing the Default Local Site Router

To edit the default local site router, you do the following:

Step 1 From the **Edit Sites/Interfaces** screen, click the **edit** link for the router named default.

Step 2 Enter the required name in the **Router Name** field.

Step 3 Enter a brief description in the **Router Description** field.

Step 4 Check each of the Cisco ADE physical ports from the **Physical Ports Monitoring this Router** field that are being used to measure traffic for this router.

Step 5 To configure an interface for the router, click **Add Interface**.

Editing the Default Local Site Router Interface

To edit the default interface, you do the following:

Step 1 Click the **edit** link for the interface named default.

Step 2 Enter a name in the **Interface Name** field.

Step 3 Enter a brief description in the **Description** field.

Step 4 Enter a link bandwidth for the interface in kbps or Mbps in the **Bandwidth** field to match the capacity of the real interface being modeled.

Step 5 Leave the default policy-map selected in the **Policy Map** field.

Note For more information on configuring advanced options for an interface, see the User Guide.

Step 6 Select the **Connectivity** type relevant to the deployment. The choice you make here reflects the type of network topology you are using BQM to model.

Select **ATM PVC, FR PVC, Metro Ethernet, Lease Line** to model a point-to-point topology, where queuing occurs in the local site router. If you have selected **ATM PVC, FR PVC, Metro Ethernet, Lease Line** as the **Connectivity** type, you do not need to configure any more information.

Select **MPLS VPN, Internet VPN, Private VPN** to model a topology including a service provider cloud, where queuing occurs in the service provider router. If you have selected **MPLS VPN, Internet VPN, Private VPN** as the **Connectivity** type, enter a bandwidth value and select the default policy-map for the Service Provider WAN interface (peer-interface) to which this local site interface connects.

Note For more information on deployment types, see the User Guide.

Step 7 Click **Save**.

The **Router** page is displayed. To add an additional interface to the router model, click **Add Interface** and repeat steps 2 to 6. Then click **Save**.

Step 8 Click **Save**.

The **Edit Sites/Interfaces** page is displayed. To add an additional router to the site model, click **Define Router** and fill in the new router details.

Step 9 Click **Save**.

The new local site configuration is saved and the **Sites/Interfaces** page is displayed.

Configuring a New Remote Site

In summary, the following tasks are involved in configuring a new remote site:

1. Create the new site with a unique name, a subnet address, an ICMP responder address for end-to-end measurements, and assign a suitable set of parameters and thresholds for the ICMP pings.

2. Define a router for the site.

3. Define the router interface(s) and attach a predefined traffic policy (policy-map).

4. For point-to-point deployments, specify the local site router interface to which the configured remote site interface is connected. For MPLS deployments, specify the Service Provider peer-interface to which the configured remote site interface is connected.

The following steps describe how to configure a new remote site:

Step 1 In **System Administration** mode, click the **Configuration** tab, click **Sites/Interfaces** and click **Define Remote Site**.

Step 2 Enter a unique name in the **Site Name** field.

Step 3 Enter a brief description of the site in the **Site Description** field.

Step 4 Enter the site subnet address and prefix in the **Subnet** field.

Note The subnet address you configure here is used as a match rule to classify traffic. Packets with a source address matching the subnet address are identified as outbound traffic leaving the site; packets with a destination address matching the subnet are identified as inbound traffic to the site.

Step 5 Enter the IP address of a reliably contactable host on the site subnet in the **Ping Address** field.

Step 6 Select a previously defined end-to-end queuing map from the **Monitor End to End Map** list. There are a number of predefined end-to-end maps available by default. Choose the map that is most appropriate for the location of the remote site. The default set of end-to-end maps define various parameters and quality thresholds for pinging the local site to derive end-to-end quality results.

Step 7 To configure a router for the site, click **Add Router**.

Configuring Remote Site Router(s) and Interfaces

As part of the configuring the network model, you configure at least one router and associated interfaces for a remote site. You define routers and interfaces for a remote site in the same way as for the local site. See the preceding sections “Editing the Default Local Site Router” and “Editing the Default Local Site Router Interface” for detailed instructions.

Configuring Custom Applications

You can define custom applications that will be automatically discovered and reported by BQM. Alternatively, they can also be used within class-maps for traffic classification. A custom application definition comprises the following: a name, match rule(s).

The system provides a default set of auto-discovered applications as listed on the **Applications** page on the **Configuration** tab in **System Administration** mode. These pre-defined applications cannot be edited or deleted.

You can define custom applications in the GUI from the **Applications** page. The **Applications** page displays the current list of auto-discovered and configured custom applications in the system.

To define a custom application, you do the following:

Step 1 Click **Add Custom Application**.

Step 2 Enter a unique name for the custom application in the **Name** field.

Note If you configure a custom application with the same name as a pre-defined application on the system, the custom application takes precedence.

Step 3 Enter a brief text description for the custom application in the **Description** field.

Step 4 To enable Auto-Discovery of the custom application when it is defined and saved, check the **Enable Auto Discovery** check box.

Step 5 To define match rules for the custom application, click **Define Rule for Application**.

Step 6 To add match rules for **TCP/UDP** source and destination addresses and ports, then select and fill out the source and destination port and address fields as required.

Step 7 To add advanced match rules, select TOS, Protocol or Applications from the **Advanced** panel, and then select or enter the required values as appropriate.

Step 8 Click **Add Rule**.

Step 9 Click **Save**.

The new custom application is saved and displayed on the **Applications** page. The custom application is available to select when defining class maps that match applications.

Viewing the Monitoring Dashboard

When you have completed the initial configuration tasks, you can switch back to **Bandwidth Quality Manager** mode to starting viewing results based on your configuration. If you are still logged in as an admin user, you choose **Bandwidth Quality Manager** from the **Mode** list. If you have logged out after performing the configuration tasks, you can log back in as either a monitor or admin user.

The first place to check for results is the **Dashboard** tab. When you open the dashboard, the navigation tree contains the new sites that you have configured. Click **expand all** to display all the nodes in the navigation tree.

Note If you have switched immediately from configuration to monitoring, you need to wait at least five minutes for the new configuration to be displayed. The first graph results will be available after five minutes; the first chart results (for example, top applications, top talkers and so on) will be available after 15 minutes.

From this point on, the information displayed in the dashboard reflects the configuration you have made.

As you configure more remote sites, the amount of traffic falling into the Unmatched Traffic site decreases.

The dashboard is one of five tabbed screens of results in **Bandwidth Quality Manager** mode. The other tabs are as follows:

- Congestion Analysis – displays information about events in the network
- Traffic Statistics – displays traffic data including top talkers, listeners and conversations
- Bandwidth Sizing – displays sizing information and upgrade recommendations
- Alerts – displays active and cleared alerts arising from network events

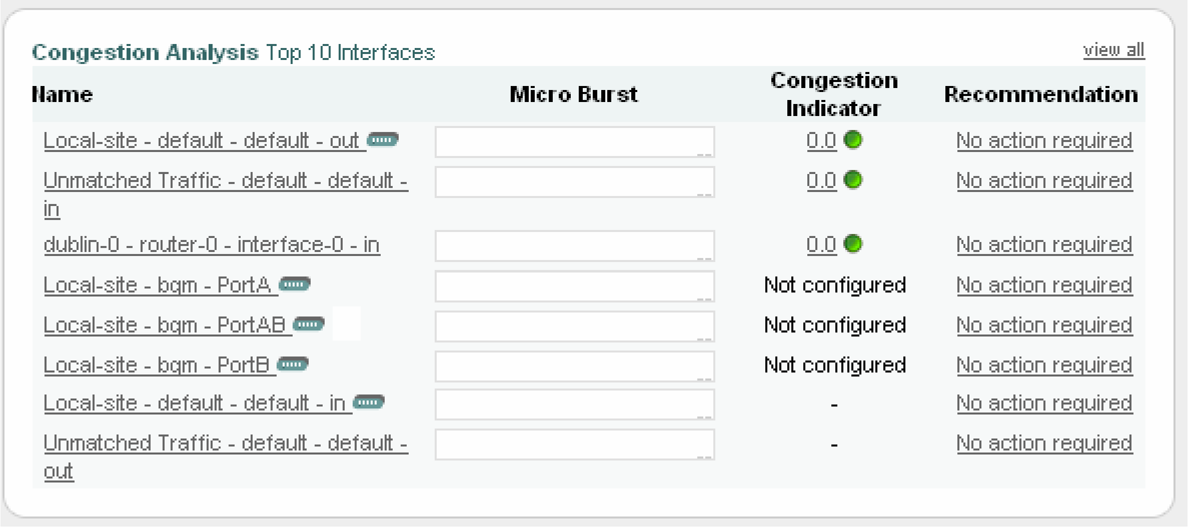
The information available from the dashboard includes:

- Top Congested Interfaces
- WAN Traffic Leaders
- Recent Alerts

Top Congested Interfaces

The **Congestion Analysis Top 10 Interfaces** lists the physical ports, and their combinations, that are seeing the most traffic.

Figure 5: Dashboard - Congestion Analysis Top 10 Interfaces



Congestion Analysis Top 10 Interfaces

view all

Name	Micro Burst	Congestion Indicator	Recommendation
Local-site - default - default - out		0.0 ●	No action required
Unmatched Traffic - default - default - in		0.0 ●	No action required
dublin-0 - router-0 - interface-0 - in		0.0 ●	No action required
Local-site - bqm - PortA		Not configured	No action required
Local-site - bqm - PortAB		Not configured	No action required
Local-site - bqm - PortB		Not configured	No action required
Local-site - default - default - in		-	No action required
Unmatched Traffic - default - default - out		-	No action required

The information displayed on the dashboard is based on the initial configuration you have made.

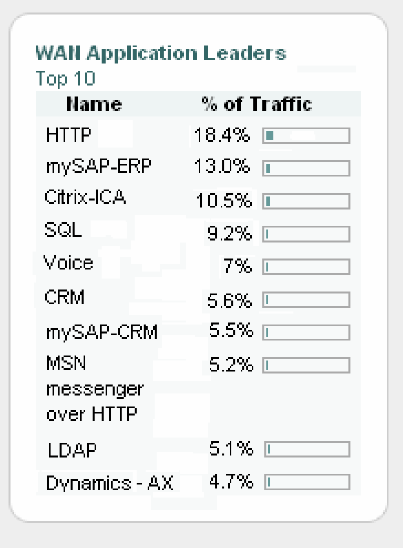
Note The example shown in Figure 5 displays initial results for a two-port Cisco ADE 2120 (PortA, PortB, and the aggregate PortAB).

Clicking on an interface name, the Micro Burst graphic, or the Congestion Indicator value in the list of top congested interfaces opens the **Congestion Analysis** tab results for the chosen interface. Alternatively, clicking **view all** opens the Congestion Analysis tab for all configured interfaces. Clicking on a recommendation opens the **Bandwidth Sizing** tab for the selected interface.

WAN Traffic Leaders

The default BQM configuration enables you to determine the network-wide top applications from all the traffic being measured. The **WAN Application Leaders** displays the top ten applications that are automatically discovered by BQM for all traffic.

Figure 6: Dashboard – WAN Application Leaders



WAN Application Leaders

Top 10

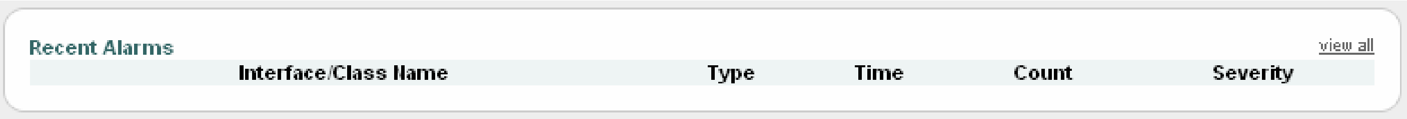
Name	% of Traffic
HTTP	18.4%
mySAP-ERP	13.0%
Citrix-ICA	10.5%
SQL	9.2%
Voice	7%
CRM	5.6%
mySAP-CRM	5.5%
MSN messenger over HTTP	5.2%
LDAP	5.1%
Dynamics - AX	4.7%

The system maintains a database of application signatures and port numbers against which all traffic is compared. It is possible to add custom applications to the database but because of the large library supported out of the box you should be able to see the top 10 applications that have the highest average volume over a five-minute period listed here when you first login. If applications do not match any signatures currently recognised by BQM, they are classed as “Unknown”. Applications falling outside the top 10 are collected under a separate heading named ‘Others.’

Recent Alarms

The **Recent Alarms** displays a list of the most recent alerts arising from events in the network, if any.

Figure 7: Dashboard – Recent Alarms



Recent Alarms

view all

Interface/Class Name	Type	Time	Count	Severity

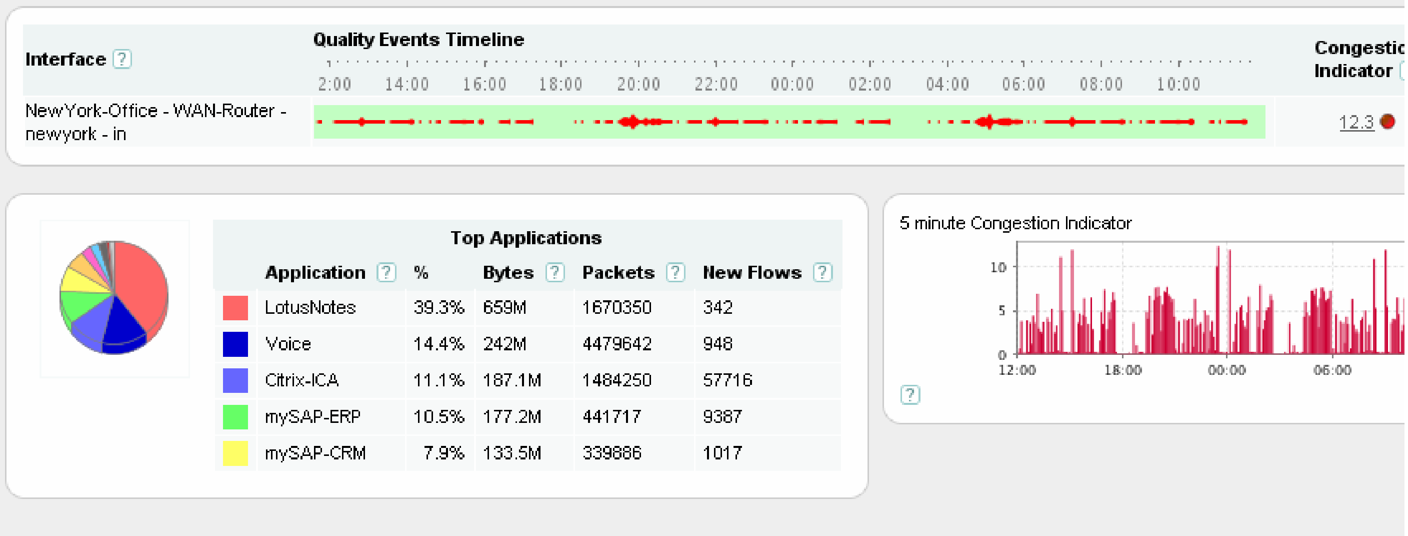
Clicking **view all** opens the **Quality Alarms** tab, containing details of all active and cleared alerts triggered by network events.

Viewing Summary Interface Results

The **Dashboard** screen is divided between a navigation pane on the left and a main page.

You can expand and collapse the navigation tree to click on the preconfigured navigation links on the left of the screen to display summary results for the chosen interface.

Figure 8: Dashboard – Summary Interface Results



Interface ?	Quality Events Timeline	Congestic Indicator
NewYork-Office - WAN-Router - newyork - in		12.3 ●

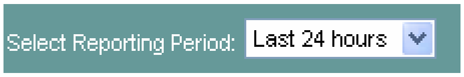
	Top Applications				
	Application ?	%	Bytes ?	Packets ?	New Flows ?
🟥	LotusNotes	39.3%	659M	1670350	342
🟦	Voice	14.4%	242M	4479642	948
🟦	Citrix-ICA	11.1%	187.1M	1484250	57716
🟩	mySAP-ERP	10.5%	177.2M	441717	9387
🟨	mySAP-CRM	7.9%	133.5M	339886	1017

The dashboard now displays the top applications for the chosen interface and congestion indicator measurements.

Changing the Reporting Period

The default view shows results for the previous 24 hours. To change the view to a different period of interest, select a reporting period from the **Select Reporting Period** list.

Figure 9: Selecting a Reporting Period



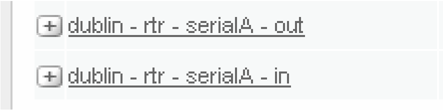
Select Reporting Period: Last 24 hours

For example, you can choose the last 12 hours or last hour reporting periods when getting started. The information onscreen refreshes with data updates every five minutes. The current system time and date is displayed at the top of the screen. You can pause the system screen refresh by clicking ⏸. To resume the five minute screen updates or to force a screen refresh, you click ⟳.

Viewing Traffic Statistics

To see more information relating to the new configuration, click the **Traffic Insight** tab. By default the **Traffic Insight** tab lists all of the interfaces you have configured in the BQM network model. The summary table information for all interfaces is sorted by interface name and provides a variety of statistics (such as maximum microburst and Congestion Indicator) for each interface. Each listed interfaces name has the following structure: site name – router name – interface –direction.

Figure 10: Traffic Statistics Tab – Configured Interfaces



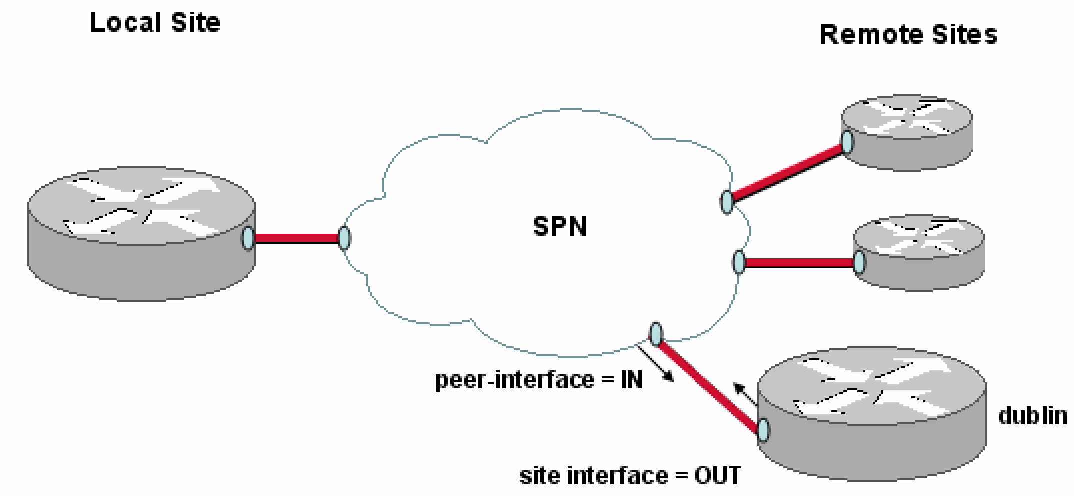
⊞ dublin - rtr - serialA - out

⊞ dublin - rtr - serialA - in

In the example configuration shown above, the default configuration has been extended. The new remote site named dublin has one router named rtr defined, and this router has one interface named serialA defined.

Notice that although one interface has been configured, there are two interfaces listed: one is labeled with direction ‘out’ and the other is labeled direction ‘in’. In this case, the configuration is based on an MPLS VPN, Internet VPN, Private VPN network model and each site interface has been configured with a matching peer-interface.

Figure 11: MPLS or Metro Ethernet Network Model



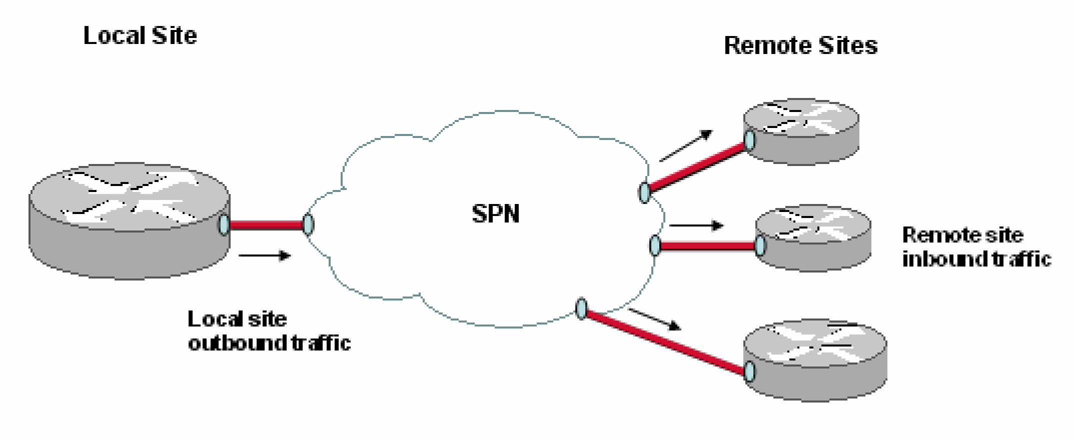
The figure illustrates the network model configuration equivalent to the details shown the in the example interface list on the **Traffic Statistics** tab. For each pair of listed interfaces, the configured interface is labelled with direction ‘out’ and represents traffic outbound from the site to the SPN cloud, and the configured peer-interface is labelled with direction ‘in’ and represents traffic inbound from the SPN cloud to the site.

The BQM features available depend on whether you are looking at the inbound or outbound directions of a given interface. This is directly related to the fact that most BQM features are supported only for traffic that is measured before queuing has occurred (pre-queuing). Some features are also supported for traffic that is measured after queuing has occurred (post-queuing).

In the BQM network model, pre-queuing traffic is represented by the following interfaces:

- Local site interface – outbound
- Remote site interface – inbound

Figure 12: Pre-queuing Traffic in the Network Model

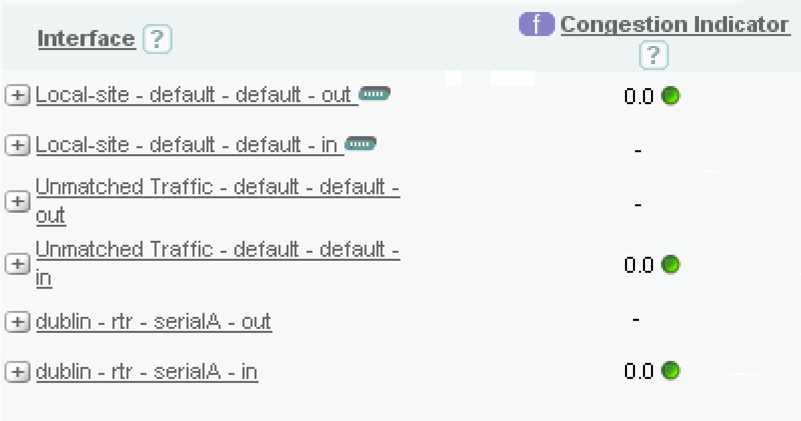


So, assuming that all BQM features are otherwise enabled in the current configuration, the following information is available only for the outbound direction of local site interfaces in and the inbound direction of remote site interfaces:

- Congestion Indicator values on the **Dashboard**, **Congestion Analysis**, and **Traffic Statistics** tabs.
- Corvil Bandwidth, Expected Queuing Delay, Expected Queuing Loss, and Congestion Indicator graphs on the **Congestion Analysis** tab
- Bandwidth Sizing – post-queuing interfaces are not displayed on the **Bandwidth Sizing** tab

For example in the figure below you can see that there are no Congestion Indicator results displayed for post-queuing interfaces in the **Traffic Statistics** tab.

Figure 13: Congestion Indicator Results Available for Pre-queuing Interfaces Only



Interface ?	f Congestion Indicator ?
⊞ Local-site - default - default - out	0.0 ●
⊞ Local-site - default - default - in	-
⊞ Unmatched Traffic - default - default - out	-
⊞ Unmatched Traffic - default - default - in	0.0 ●
⊞ dublin - rtr - serialA - out	-
⊞ dublin - rtr - serialA - in	0.0 ●

All other graphs, charts and results on the **Traffic Statistics** tab are available for both directions of traffic. When you click on an interface name, the traffic statistic graphs displayed for the interface are as follows:

- Micro Burst Detection
- Average Bit Rate
- Packet Rate
- Peak-to-Mean Ratio
- Packet Size Distribution

Along with the traffic statistics graphs, there are other tabs with further details that you can view for the interface:

- Applications
- Talkers
- Listeners
- Conversations

You can use these charts to identify the applications comprising the largest share of network traffic and the hosts transmitting and receiving the most traffic over the chosen reporting period.

In each chart the colors match each colored segment of the chart to a listed application.

Availability and Precision statements provide information on the amount of traffic on which the results are based.

Viewing Congestion Analysis Results

By default the **Congestion Analysis** tab lists all of the interfaces you have configured in the BQM network model. This tab provides a visual guide to congestion events for each of these interfaces.

For each congested interface you can analyze more information to troubleshoot a congestion event that is impacting on quality of service.

You can use the displayed Congestion Indicator values to identify the congestion level on each interface. A Congestion Indicator value greater than 1 means that loss or delay is above an acceptable level, as specified in the BQM configuration. A Congestion Indicator of less than 1 means the loss or delay is better than that specified.

Identifying Events

The Quality Events Timeline identifies events by displaying a bar on the timeline at the time the event took place. Events are triggered when a measured value, or a value calculated by BQM based on traffic measurements, exceeds its associated threshold value, as specified in the BQM configuration. The default BQM configuration enables event detection based on the following:

- Queuing delay exceeds 500 milliseconds
- Loss due to queue tail drops detected
- Millisecond microburst exceeds the configured interface capacity
- Corvil Bandwidth exceeds the configured class capacity
- Expected delay or loss detected
- End-to-end packet loss detected

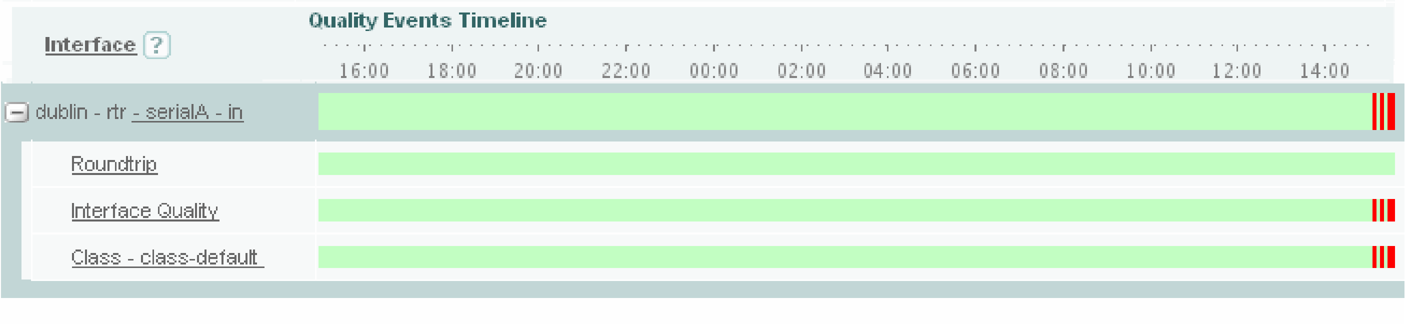
Threshold values for each of these event triggers are configurable and are specified as part of the BQM configuration in monitor queuing maps.

When an event has been detected, the system automatically saves a packet capture file for the interval during which the event occurred. This packet capture file provides the data to support detailed analysis of the event. The system employs a rolling packet capture mechanism in order to cover the whole period of time over which the event was detected.

If you do not see any events, you can configure more sites and continue to monitor the situation.

If the Quality Events Timeline indicates an event, you can expand the affected interface to get an initial idea of where the problem lies.

Figure 14: Events Indicated on the Quality Events Timeline

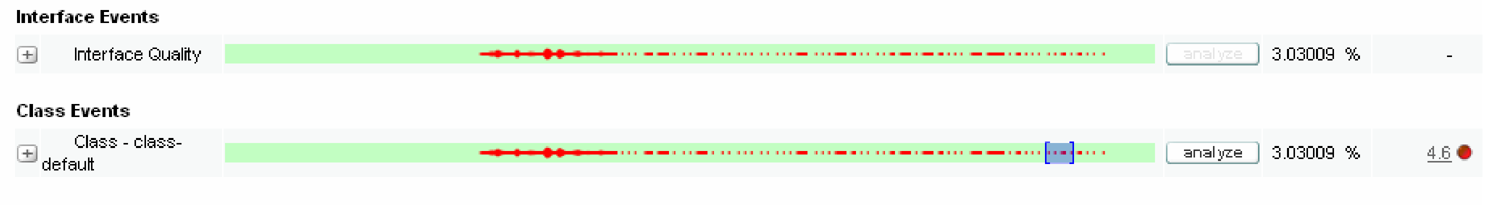


Click the interface name, or the **Interface Quality** or **Class – class-defaul**t links to open the congestion analysis screen for the chosen interface.

You can use the **Select Reporting Period** list to view a shorter timescale or define a custom period that includes the indicated event.

When you have narrowed the timescale closer to the event, you zoom in on the required event(s) and click **analyze** for the chosen interface or the default class.

Figure 15: Analyzing Interface and Default Class Events



The event inspection window is launched. If you have redefined the reporting period to a shorter timescale around the original event of interest, you may find that the event timeline now displays a number of events at this shorter timescale.

The set of graphs displayed in the event inspection window are as follows:

- Average Bit Rate
- Packet Rate
- The Micro Burst Detection graph includes four sources of data:
- Corvil Bandwidth – Delay
- Corvil Bandwidth – Queue Length
- Expected Delay
- Expected Queue Length
- Expected Loss

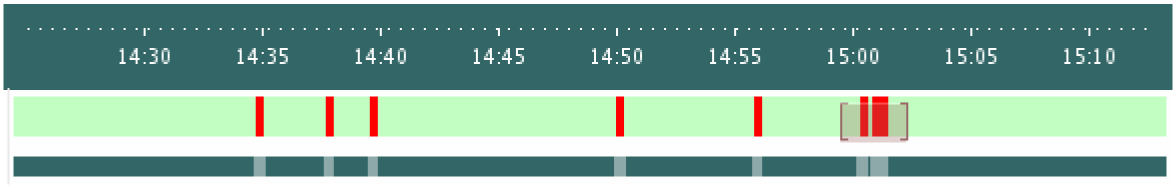
The charts for identifying event traffic leaders are as follows:

- Top applications
- Top talkers
- Top listeners
- Top conversations

You can use these charts to identify the applications comprising the largest share of network traffic and the hosts transmitting and receiving the most traffic as you zoom in on a particular event. Once the inspection window is open you can click and drag over an event or group of events on the Quality Events Timescale to effectively zoom in to shorter and shorter timescales, down to millisecond levels.

As you zoom in (or zoom out), the graphs and traffic leader charts are all redrawn to display only the data relevant to the timescale you are viewing.

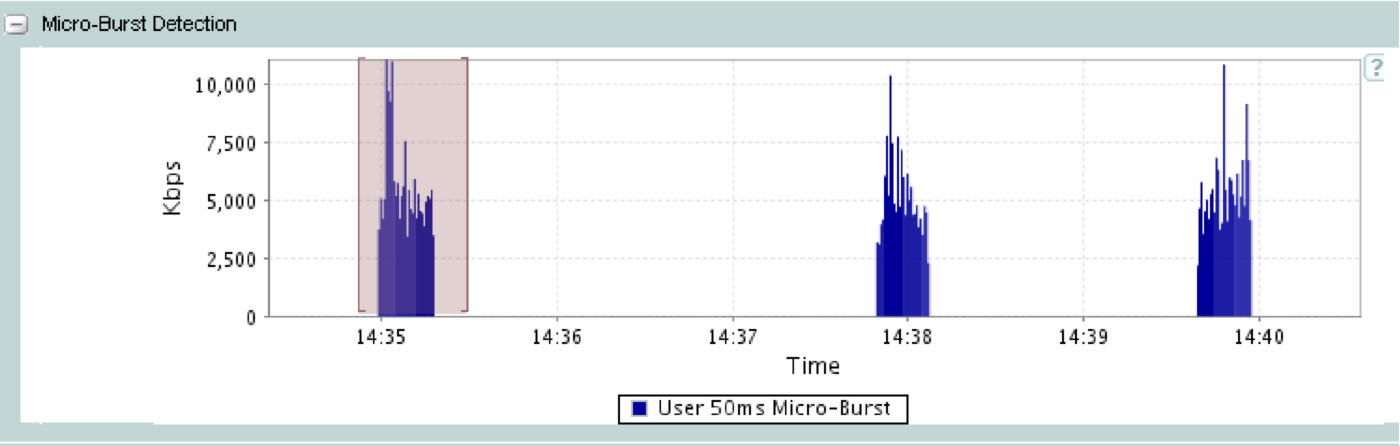
Figure 16: Zooming in on Events using the Quality Event Timeline



Note The gray bars beneath the events timeline indicate the events for which a packet capture is available.

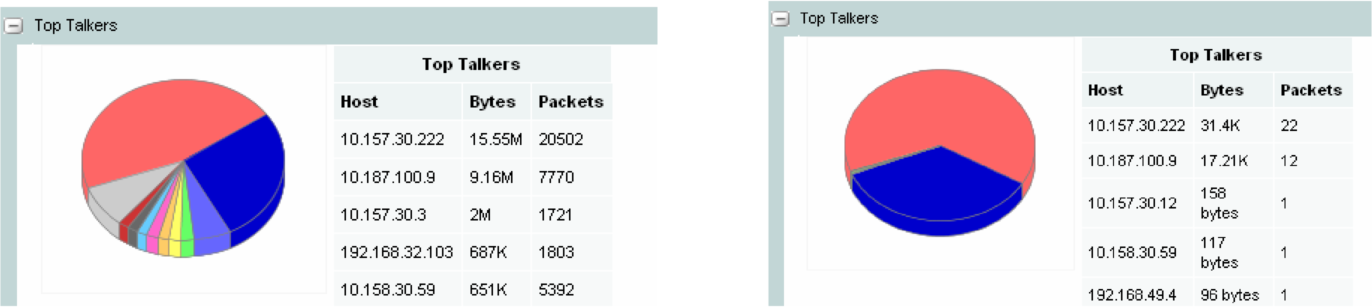
You can also zoom in to shorter timescales by clicking and dragging across an area of interest in any of the graphs.

Figure 17: Zooming in on Graph Details



Again, all other graphs and traffic leader charts are redrawn to reflect the timescale to which you have zoomed. In the examples shown below, the top talkers chart on the left is displayed when the event inspection window is first launched. By the time you have zoomed in on the details of the event, the top talkers chart on the right is displayed.

Figure 18: Top Talkers Before and After Zooming



Top Talkers

Host	Bytes	Packets
10.157.30.222	15.55M	20502
10.187.100.9	9.16M	7770
10.157.30.3	2M	1721
192.168.32.103	687K	1803
10.158.30.59	651K	5392

Top Talkers

Host	Bytes	Packets
10.157.30.222	31.4K	22
10.187.100.9	17.21K	12
10.157.30.12	158 bytes	1
10.158.30.59	117 bytes	1
192.168.49.4	96 bytes	1

When you are zooming in, you can return to any of the previous zoom levels by clicking the relevant links in the **Timeline History** field. To return immediately to the level at which you opened the event inspection window, click **Reset**.

Filtering Event Data

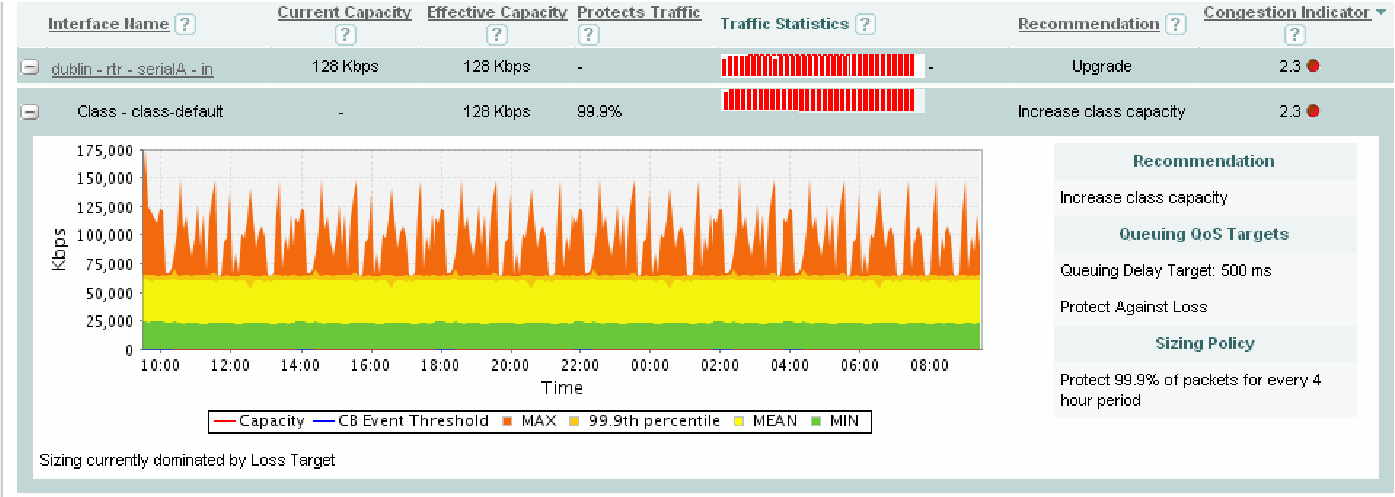
You can perform filtering of the packet trace on which the event analysis is based. Simple filters, similar to Cisco access control lists (ACLs) based on subnet addresses and application ports numbers and names are supported. You click **New** at the **Traffic Filter** field to start the process of defining a new filter. When you have defined a filter and saved it, you select it from the **Traffic Filter** list. The filter is then applied to the traffic on which the event analysis is being performed and the graphs and charts are all updated to reflect the new traffic.

Viewing Bandwidth Sizing Results

By default the **Bandwidth Sizing** tab lists all of the network model pre-queuing interfaces (local site outbound and remote site inbound) you have configured in the BQM network model. Bandwidth Sizing results are not available for post-queuing interfaces (local site inbound and remote site outbound). The summary table information is sorted by interface name and provides a guide to bandwidth utilization on network links.

After you have completed configuration of the BQM network model to reflect your network, you typically should allow the system to measure traffic for at lest a week before considering the bandwidth sizing results. In many cases, you would wait until the system has accumulated a month's worth of measurements.

Figure 19: Class Bandwidth Sizing



Interface Name ?	Current Capacity ?	Effective Capacity ?	Protects Traffic ?	Traffic Statistics ?	Recommendation ?	Congestion Indicator ?
⊟ dublin - rtr - serialA - in	128 Kbps	128 Kbps	-	-	Upgrade	2.3 ●
⊟ Class - class-default	-	128 Kbps	99.9%		Increase class capacity	2.3 ●

Recommendation

Increase class capacity

Queuing QoS Targets

Queuing Delay Target: 500 ms

Protect Against Loss

Sizing Policy

Protect 99.9% of packets for every 4 hour period

Sizing currently dominated by Loss Target

Recommendations are made on a per-class basis and these drive the recommendation for the associated interface. In the single-class example shown above, the recommendation is to increase the class capacity to relieve congestion on the interface.

The sizing graph plots Corvil Bandwidth values over the selected reporting period. The Corvil Bandwidth values represent the bandwidth required to prevent an acceptable proportion of all traffic from experiencing queuing delay or packet loss due to congested queues. The calculated Corvil Bandwidth values depend on configurable parameters, namely the configured queuing QoS targets and sizing policy. The current configured values for each are displayed with the graph.

The queuing targets specify the amount queuing delay (in milliseconds) that can be tolerated by the traffic, and also whether any packet loss is acceptable or not. Depending on the traffic being monitored, either protecting against loss or protecting against delay will usually dominate the presented Corvil Bandwidth and therefore the sizing recommendation.

The sizing policy specifies the proportion of all traffic (for example 99.9%) which must meet the queuing targets and a period of time, the busy period, for which the highest traffic volumes have previously been seen.

Working with Multiclass Configurations

So far we have looked at making basic changes to the default BQM configuration to edit local site details and configure remote sites with default, single-class configurations. This section describes how to configure BQM to model multiclass configurations.

As in the case of configuring a Cisco router, you configure multiple class maps and a policy map to implement a multiclass configuration. You also need to set different QoS parameters and thresholds for each class so that BQM treats them differently.

To begin, get your multiclass router configuration. You need to use the router configuration as a basis for configuring the BQM multiclass model. To build the BQM configuration, you configure the following:

- Class-maps
- Monitor queuing maps
- Policy-map

You then edit an existing site or define a new site, and attach the new policy-map to the site interface.

Configuring Class Maps

Go to **System Administration** mode, and with the **Configuration** tab open, click **Class Maps**.

The class-map screen opens. You need to define a class-map for each class in the router configuration you are modelling, naming each class as per the configuration.

Note If you are using Network-Based Application Recognition (NBAR) on the router being modeled in the BQM configuration, you need to convert the NBAR match rules from the router configuration to equivalent BQM match rules. For more information, see the User Guide section “Converting Network-Based Application Recognition (NBAR) Configurations” in the chapter “Using the Command Line Interface (CLI).”

To define a class-map, you do the following:

Step 1 Click **Define Class Map**.

The **Add Class Map** page is displayed.

Step 2 Enter a unique name for the class-map in the **Name** field.

Step 3 Enter a brief text description for the class-map.

Step 4 Click **Define Rule for Class Map**.

The **Define Match Rule** page is displayed.

Step 5 Select the match rule type from the list.

Step 6 Select and fill out the configuration fields as required.

To match all traffic except the parameters you specify, check the box labeled **Match all traffic except the following**.

Step 7 Click **Add Rule**.

Step 8 Select the appropriate radio button to define whether you want traffic to match ANY of the defined match rules or to match ALL of the defined match rules.

Step 9 Click **Save Class Map**.

The configured class-map is saved and the **Class Maps** page is displayed.

Repeat the steps to configure all the class-maps in your configuration.

Configuring Monitor Queuing Maps

Go to the **Queuing Maps** screen on the **Configuration** tab. For each class, you create a queuing map with parameters and event detection thresholds appropriate to each class.

To define a monitor queuing map, you do the following:

Step 1 Click **Add Monitor Queuing Map**.

Step 2 Enter a unique name for the monitor queuing map in the **Name** field.

Step 3 Enter a brief text description for the monitor queuing map in the **Description** field.

Step 4 Configure the combination of parameters that will enable the monitoring features you want to set:

Configuring Expected Delay and Loss and Congestion Indicator

To enable the calculation of expected delay and loss results, check the **Expected Loss and Delay** check box.

To configure queuing QoS targets for the expected loss and delay calculations, enter a queuing delay target in milliseconds in the **Queuing Delay Target** field [Range: 5 - 10000 ms].

To configure Congestion Indicator (CI) calculation, you configure a sizing policy (also used for bandwidth sizing). Enter a percentage value in the **Protect** field [Range: 0.0-100.0000%. (Six significant figures)]. This value determines the percentage of traffic (for example 99.9999%) that must meet the configured queuing targets (both delay and loss).

Next, select a busy period from the list on which to base the policy. The busy period is the timescale that has historically seen the greatest volumes of traffic. To enable event detection when the calculated delay exceeds the configured delay target, check the **Generate Events when Delay Exceeds Threshold** check box. The queuing delay target you configure sets the threshold value that must not be exceeded. Similarly, check the **Generate Events when Loss occurs** check box to enable event detection if the expected loss calculation indicates any packet loss.

Configuring Corvil Bandwidth (CB) Measurement

To enable calculation of Corvil Bandwidth values for bandwidth sizing, check the **Calculate CB** check box. If you have already enabled expected loss and delay calculation with defined queuing targets and sizing policy values, these values are automatically populated in the relevant fields for Corvil Bandwidth calculation. Only one set of queuing targets and sizing policy values can be specified in a single monitor-queuing-map.

If you are enabling bandwidth sizing with Corvil Bandwidth but are not enabling expected loss and delay calculation, then to configure queuing QoS targets for the Corvil Bandwidth calculations, enter a queuing delay target in milliseconds in the **Queuing Delay Target** field [Range: 5 - 10000 ms].

To configure a sizing policy for bandwidth sizing, enter a percentage value in the **Protect** field [Range: 0.0-100.0000%. (Six significant figures)]. This value determines the percentage of traffic (for example 99.9999%) that must meet the configured queuing targets (both delay and loss). Next, select a busy period from the list on which to base the policy. The busy period is the timescale that has historically seen the greatest volumes of traffic.

To set a Corvil Bandwidth threshold, at which event detection is triggered, enter a value in the **Generate Events when CB Exceeds** field as a percentage of the link bandwidth [Range: 1 - 1000] or in kbps [Range: 1 - 10000000].

Configuring Microburst Detection

To enable Micro Burst Detection, check the **Micro Burst Detection** check box.

To enter a minimum millisecond resolution for peak measurements in the **Micro Burst minimum duration** field [Range: 5 - 10000 ms].

To configure a threshold value at which to trigger event detection, enter a value in the **Trigger Micro burst events above** field as either a percentage of the link bandwidth [Range: 1 - 1000] or in kbps [Range: 1 - 10000000].

The **Use Shaping Detection Algorithm** check box is checked by default. We recommend that you leave this feature enabled.

Step 5 Click **Save**.

The new monitor queuing map is saved with default settings and displayed on the **Monitor Queuing Maps** page.

The monitor queuing map is available to select when defining policy maps.

Configuring a Multiclass Policy Map

Go to the **Policy Maps** screen on the **Configuration** tab. The system supports configuration of the following multi-class router queuing types:

- Strict priority queuing (PQ)
- Weighted fair queuing (WFQ)
- Low latency queuing (LLQ)

Define the policy map for the required multiclass configuration, following the relevant Cisco CLI conventions and save it. The policy-map will now be available to select when editing or defining a site interface.

Attaching the Policy Map to a Site

The next task is to either edit a site and attach the new policy-map to the site interface, or create a new site and attach the new policy map to the site interface. See the chapter "Performing Basic Configuration" for more information on editing or defining sites and their associated routers and interfaces.

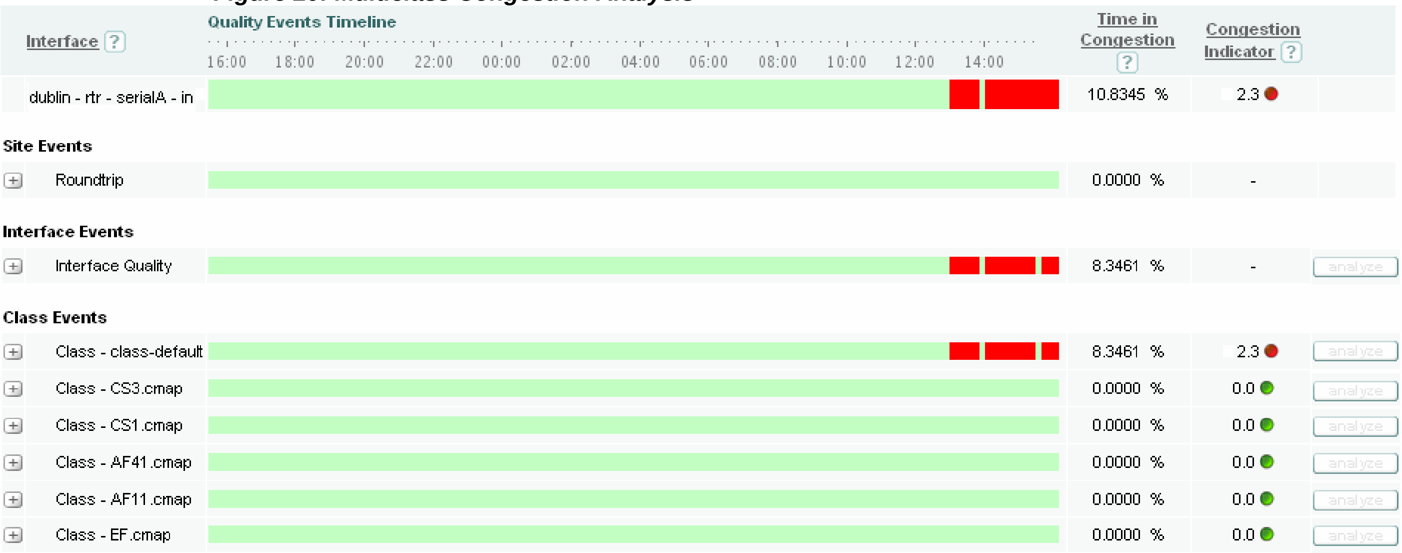
Viewing Multiclass Monitoring Results

If you switch back to Network Monitoring mode, and wait at least five minutes, you can start to see the results for the multiclass configuration.

In the **Dashboard** tab, you can use the navigation tree to view summary results for each class. You expand the tree and click a class to view the available dashboard results for the class traffic.

In the **Congestion Analysis** tab, the per-class information is rolled up into an interface events tab. The Congestion Indicator value displayed for the interface now represents the highest Congestion Indicator value calculated from among the classes.

Figure 20: Multiclass Congestion Analysis

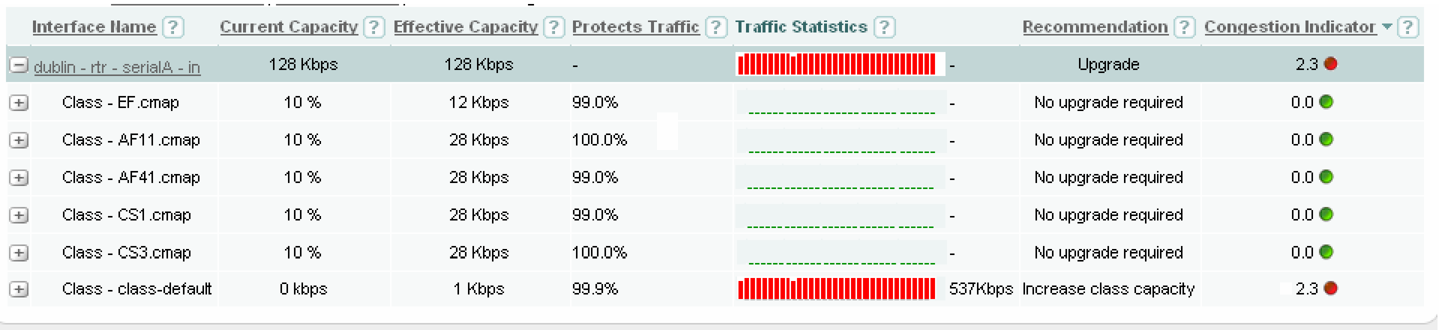


Interface ?	Quality Events Timeline	Time in Congestion ?	Congestion Indicator ?	
dublin - rtr - serialA - in		10.8345 %	2.3 ●	
Site Events				
⊞ Roundtrip		0.0000 %	-	
Interface Events				
⊞ Interface Quality		8.3461 %	-	analyze
Class Events				
⊞ Class - class-default		8.3461 %	2.3 ●	analyze
⊞ Class - CS3.cmap		0.0000 %	0.0 ●	analyze
⊞ Class - CS1.cmap		0.0000 %	0.0 ●	analyze
⊞ Class - AF41.cmap		0.0000 %	0.0 ●	analyze
⊞ Class - AF11.cmap		0.0000 %	0.0 ●	analyze
⊞ Class - EF.cmap		0.0000 %	0.0 ●	analyze

If you expand the interface or drill down into the interface page you should see the class with that Congestion Indicator value. You can then investigate and analyze any reported congestion events for each class.

The **Bandwidth Sizing** tab now has recommendations for each class.

Figure 21: Multiclass Bandwidth Sizing



Interface Name ?	Current Capacity ?	Effective Capacity ?	Protects Traffic ?	Traffic Statistics ?		Recommendation ?	Congestion Indicator ▾ ?
⊟ dublin - rtr - serialA - in	128 Kbps	128 Kbps	-		-	Upgrade	2.3 🔴
⊞ Class - EF.cmap	10 %	12 Kbps	99.0%		-	No upgrade required	0.0 🟢
⊞ Class - AF11.cmap	10 %	28 Kbps	100.0%		-	No upgrade required	0.0 🟢
⊞ Class - AF41.cmap	10 %	28 Kbps	99.0%		-	No upgrade required	0.0 🟢
⊞ Class - CS1.cmap	10 %	28 Kbps	99.0%		-	No upgrade required	0.0 🟢
⊞ Class - CS3.cmap	10 %	28 Kbps	100.0%		-	No upgrade required	0.0 🟢
⊞ Class - class-default	0 kbps	1 Kbps	99.9%		537Kbps	Increase class capacity	2.3 🔴

In the example shown here, the default class is experiencing the congestion, whereas the other classes are not.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.