



# Release Notes for the Cisco Bandwidth Quality Manager, Release 4.0

---

September 21, 2007, OL-14122-01

These release notes provide information about known issues in Cisco Bandwidth Quality Manager 4.0.

Cisco Bandwidth Quality Manager (BQM) is a network application congestion management tool that provides outstanding visibility and analysis of traffic, bandwidth and QoS on IP access networks. BQM continuously monitors traffic with microsecond per-packet resolution. BQM can detect short-lived network events and identify the traffic impacted and responsible for the congestion. BQM can also be used before deployment of TelePresence to ensure the existing network resources are sufficient to deliver adequate QoS for TelePresence sessions without adversely impacting existing network traffic.

## What's New in this Release?

BQM 4.0 introduces key new features that extend the capabilities of BQM:

- Passive Network Quality Monitoring (PNQM) technology enables end-to-end per-packet quality monitoring, to complement the WAN-access Expected Queuing measurement in BQM 3.x.
- Customised dashboard for at-a-glance view of the network service quality level of selected applications, for example, TelePresence, market data.
- Realtime monitoring, with per second updates, gives unique view of the live network conditions.
- Richer QoS targets allow configuration of latency, jitter and loss targets both for expected WAN-access congestion and measured end-to-end quality.

BQM 4.0 helps assure the optimum network service level in a number of ways:

- By continuous monitoring of both new and existing applications after deployment to ensure required service levels are maintained. With its microsecond visibility and QoS-aware threshold settings, it will give early warning of approaching quality degradation.
- By using end-to-end passive monitoring (PNQM) to reliably detect if even a single packet exceeds configured end-to-end latency thresholds.
- By comparing and contrasting WAN-access congestion and end-to-end latency and loss to identify the dominant cause of network performance issues.
- By validating the behavior and performance of an application before it is deployed over the network.

### **Passive Network Quality Monitoring**

BQM 4.0 introduces Passive Network Quality Monitoring (PNQM), Corvil's passive monitoring technology. With PNQM deployed, a full picture emerges of the end-to-end delay, jitter and loss experienced for TelePresence and each other class of traffic. PNQM complements the existing Expected Queuing (EQ) information: PNQM highlights traffic that is experiencing network service level problems, and EQ determines whether local or end-to-end congestion is the likely cause.

PNQM is fully integrated with the existing features of BQM, including the ability to view the end-to-end delays experienced by individual packets, generate SNMP traps when end-to-end delay exceeds configured thresholds, and rank interfaces according to the quality of the end-to-end network service achieved.

PNQM requires deployment of a Cisco Application Deployment Engine (ADE) at each endpoint (for example, each TelePresence site). Packets are observed leaving and arriving from each end point and the timing information is exchanged between the Cisco ADE, allowing the one-way delays to be determined.

### **Custom Dashboard**

BQM 4.0 introduces a customizable monitoring dashboard. The custom monitoring dashboard allows an at-a-glance view of the network service level being achieved by traffic (for example, TelePresence). The service level is resolved into end-to-end latency, jitter and loss in each direction.

When configured, the custom dashboard comprises a list of classes and associated end-to-end monitoring results:

- the Network Service Index summarizes the long-term quality achieved in each direction. Values above 1.0 indicate the configured targets were not met.
- Outbound end-to-end delay, delay variation and loss.
- Inbound end-to-end delay, delay variation and loss.

You choose which graphs to display when configuring the dashboard.

### **Live View**

The purpose of the realtime monitoring view is to enable you to troubleshoot current performance issues on the network. When you launch the realtime monitoring view a new window is opened displaying graphs for the interface and classes under separate tabs. All graphs update every second giving you a unique insight into the traffic currently being measured.



---

**Note** For more information on release 4.0 software installation, see the “Cisco Bandwidth Quality Manager 4.0 Installation Guide.”

For detailed initial setup and configuration information, see the “Getting Started Guide for the Cisco Bandwidth Quality Manager, Release 4.0”.

---

The following table indicates the upper limits on the number of sites and classes that can be configured on each of the supported platforms and the maximum WAN bandwidth that can be monitored with each.

**Table 1** *Maximum Sites, Classes, and Monitored WAN Bandwidth per Cisco ADE Platform*

Item	Cisco ADE 1010	Cisco ADE 2120 (Single Port)	Cisco ADE 2120 (Two/Four Port)	Cisco ADE 2130 (Two/Four Port)	Cisco ADE 2140
Sites	20	250	250	500	500
Classes	100	1000	1000	2000	2000
Maximum Monitored WAN Bandwidth	100 Mbps	100 Mbps	2 Gbps/4 Gbps	2Gbps/4 Gbps	20 Gbps

## System Requirements

This section describes the hardware and browser requirements for BQM 4.0.

### Hardware Requirements

BQM 4.0 software runs on the Cisco ADE 1010, Cisco ADE 2120, Cisco ADE 2130, and Cisco ADE 2140. BQM 4.0 also supports upgrades for the Cisco 1180 platform from 3.x to 4.0. See the “Cisco Bandwidth Quality Manager 4.0 Installation Guide” for more information on hardware specifications, or contact your sales representative for more information about hardware requirements.

### Browser Requirements

The following table describes the browser requirements for all platforms.

**Table 2** *Browser Requirements*

Browser	Version	Platform
Internet Explorer	6.0	Windows XP



**Note** Javascript should be enabled for the browser. We also recommend that you configure the browser to enable pop-ups.

## Related Documentation

The following is a list of the documentation for Cisco BQM Release 4.0:

- Cisco Bandwidth Quality Manager 4.0 Installation Guide
- Getting Started Guide for Cisco Bandwidth Quality Manager Release 4.0
- Cisco Bandwidth Quality Manager 4.0 User Guide

## Release 3.x to 4.0 Upgrade

This section describes the steps involved in upgrading from each 3.x release to release 4.0.



---

**Note** Performing a CD installation of release 4.0 on a BQM running release 3.x will result in all data collected using version 3.x being lost.

---

BQM 4.0 supports upgrades for the Cisco 1180 platform from 3.x to 4.0.

### Release 3.1 to 4.0 Upgrade

To perform an upgrade from version 3.1 to version 4.0 you do the following:

- Step 1** Obtain the release 4.0 upgrade image.
- Step 2** Before performing the upgrade, it is advisable to stop any manual packet captures that are operating. You should also shut down all measurement ports (using the shutdown command in the config/port context) to effectively disable traffic measurement and any associated event detection packet capture.
- Step 3** For safety, initiate a backup of the current 3.1 system.



---

**Note** When selecting desired backup destination, ensure that there is enough space on destination system and that the backup time is acceptable.

---

- Step 4** Use the following command to start the 3.1 to 4.0 upgrade: `ssh admin@probe_name install system < image_name`

So, for example to load the image file named `CBQM-v4.0.0.28-D4.9.29237_RELEASE.upgrade` on to a BQM named `data_center` you would use the following:

```
ssh admin@data_center install system < CBQM-v4.0.0.28-D4.9.29237_RELEASE.upgrade
```



---

**Note** The database upgrade process can take up to five hours when converting a large configuration with a 60 day history.

---

The machine reboots. On reboot, the partition with the new image is loaded (system software is now upgraded) and the database upgrade script is invoked. You can see on the terminal/console that the database is being upgraded. When the Cisco ADE restarts, you are prompted to log in.

Alternatively, you can copy the upgrade image to a tftp server and use the BQM copy command to send the image to the Cisco ADE:

```
copy tftp://[hostname|A.B.C.D]/CBQM-v4.0.0.28-D4.9.29237_RELEASE.upgrade
standby-system-image
```

In this case you then use the reload command to reboot the Cisco ADE with the upgrade image:

```
reload standby-system-image
```

When the Cisco ADE restarts, the upgrade is completed and you are prompted to log in.



---

**Note** In general, we recommend that, when you have verified an upgrade of system image, you repeat the procedure to copy the chosen system image to the standby system image in order to avoid a subsequent accidental reload of an older version of the system image. Reloading an older build number will result in loss of data.

---



---

**Note** For more information on release 4.0 software installation, see the “Cisco Bandwidth Quality Manager 4.0 Installation Guide.”

For detailed initial setup, licensing, and configuration information, see the “Getting Started Guide for the Cisco Bandwidth Quality Manager, Release 4.0”.

---

## Release 3.2 to 4.0 Upgrade

To perform an upgrade from version 3.2 to version 4.0 you do the following:

- 
- Step 1** Obtain the release 4.0 upgrade image.
  - Step 2** Before performing the upgrade, it is advisable to stop any manual packet captures that are operating. You should also shut down all measurement ports (using the shutdown command in the config/port context) to effectively disable traffic measurement and any associated event detection packet capture.
  - Step 3** For safety, initiate a backup of the current 3.2 system.



---

**Note** When selecting desired backup destination, ensure that there is enough space on destination system and that the backup time is acceptable.

---

- Step 4** Use the following command to start the 3.2 to 4.0 upgrade: `ssh admin@probe_name install system < image_name`

So, for example to load the image file named `CBQM-v4.0.0.28-D4.9.29237_RELEASE.upgrade` on to a BQM named `data_center` you would use the following:

```
ssh admin@data_center install system < CBQM-v4.0.0.28-D4.9.29237_RELEASE.upgrade
```



---

**Note** The database upgrade process can take up to five hours when converting a large configuration with a 60 day history.

---

The device reboots. On reboot, the partition with the new image is loaded (system software is now upgraded) and the database upgrade script is invoked. You can see on the terminal/console that the database is being upgraded. When the device restarts, the upgrade is completed and you are prompted to log in.

Alternatively, you can copy the upgrade image to a tftp server and use the BQM copy command to send the image to the device:

```
copy tftp://[hostname|A.B.C.D]/ CBQM-v4.0.0.28-D4.9.29237_RELEASE.upgrade
standby-system-image
```

In this case you then use the reload command to reboot the Cisco ADE with the upgrade image:

```
reload standby-system-image
```

When the device restarts, the upgrade is completed and you are prompted to log in.



---

**Note** In general, we recommend that, when you have verified an upgrade of system image, you repeat the procedure to copy the chosen system image to the standby system image in order to avoid a subsequent accidental reload of an older version of the system image. Reloading an older build number will result in loss of data.

---

When the device restarts, the upgrade is completed and you are prompted to log in.

---



---

**Note** For more information on release 4.0 software installation, see the “Cisco Bandwidth Quality Manager 4.0 Installation Guide.”

For detailed initial setup, licensing, and configuration information, see the “Getting Started Guide for the Cisco Bandwidth Quality Manager Release 4.0”.

---

## Caveats

This section provides information about known issues in the BQM 4.0 software.

### Default Configuration

The default BQM configuration contains a default router and interfaces to measure traffic on each management port and their aggregate. If these default interfaces are removed, there is no trivial way to restore them. Please see the section “Default BQM Configuration” in the Cisco Bandwidth Quality Manager 4.0 User Guide for details of the default configuration.

### Backup, Restore and Packet Captures

Before performing a backup or restore, it is advisable to stop any manual packet captures that are operating. You should also shut down all measurement ports (using the shutdown command in the config/port context) to effectively disable traffic measurement and any associated event detection packet capture.

### Packet Fragmentation

Any fragmentation caused by exceeding path MTU (not LFI) is not supported by the system for sizing or in PNQM. Fragmentation can be an issue with encrypted packets where encryption overhead leads to large packets being greater than the MTU and also DSL type networks with PPPoE overhead. For PNQM, fragmented packets are classified as loss or as re-routed.

## Known Issues

The following section identifies software issues that are known to exist in this release of the BQM product and workarounds for issues, where applicable.

The known software issues are grouped under the following areas:

- Configuration
- Dashboard
- Traffic Insight
- Event Analysis
- Quality Alarms and System Alerts
- CLI

**Table 3**      **Configuration Issues**

<b>Description</b>	<b>Resolution</b>
In general, newly created interfaces only appear after a summary update. When a new interface is created, it is displayed immediately in the dashboard tree view but doesn't appear in the other screens until the next 5-minute update.	In general, when creating a new interface, wait at least five minutes before looking for results in all screens.
The default configuration sets the displayed local port capacities (PortA, PortB, PortC, PortD) at 1Gbs and the aggregate PortABCD is set at 4Gbps. These figures may not reflect the negotiated speed of the link being monitored.	The default values can be configured to match the actual link speed.

Editing class-map match rules in the GUI that have been created using the CLI may lead to inconsistent results.	We recommend that having defined class-map match rules in the GUI that you edit them using the GUI, or if you define them using the CLI, you edit them using the CLI.
A remote site has the subnet-filtering option turned on by default. If you want a given site to match all traffic regardless of subnet, you must use the no subnet-filtering command on the CLI.	Use the no subnet-filtering command from the CLI.
After an interface is created with the GUI, you cannot change its WAN Connectivity type from ATM, FR, Metro Ethernet, Leased Line to MPLS VPN, Internet VPN Private VPN and vice versa.	Use the CLI to do one of the following as required:  edit the directly-connected interface (ATM, FR...) and define a peer-interface (MPLS...), or delete the peer-interface (MPLS...) and define a directly-connected interface (ATM, FR...)

The following table describes known issues with the dashboard.

**Table 4**      **Dashboard Issues**

Description	Resolution
The dashboard is blank in the first five minutes of use.	The dashboard data is populated after five minutes of use, after the first data rollup.

The following table describes known issues with the Network Service Quality tab.

**Table 5**      **Network Service Quality Issues**

Description	Resolution
Only remote sites appear on the custom dashboard.	This will be added to the documentation..
With uni-directional traffic, a PNQM channel can take several hours to reach optimum accuracy. Accuracy during this period can be affected by up to about 2-4 milliseconds.	Configure once-per-second ICMP pinging between the two BQMs to improve accuracy during the startup phase.

The following table describes known issues with the Traffic Insight tab.

**Table 6** *Traffic Insight Issues*

Description	Resolution
<p>DNS currently holds resolved hostnames on a per session basis.</p> <p>When viewing Top-N results you are able to resolve to display hostnames, but you cannot switch back to view IP addresses.</p>	<p>When a Top N table has been resolved and the IP addresses replaced with names, the IP address is still available as a tool tip, if you hover the mouse over the name.</p> <p>Alternatively, you must log out and back in again to return to the original display of IP addresses.</p>

The following table describes known issues with the Event Analysis tab.

**Table 7** *Event Analysis Issues*

Description	Resolution
<p>It is possible for 5-minute end-to-end jitter plot values to exceed the configured threshold but without any corresponding events or event analysis drill-down data. This is because jitter is calculated over a five minute period in the main product screens, but over one second in the event analysis screens.</p>	<p>In future versions of the product all jitter calculations will be based on one-second calculations.</p>
<p>If you create a sufficiently large number of classes in a given policy-map (for example, greater than fifteen), they will not all be accessible in the event analysis window.</p>	<p>This will be resolved in future releases.</p>

The following table describes known issues with the Quality Alarms and System Alerts tabs.

**Table 8** *Quality Alarms and System Alerts Issues*

Description	Resolution
<p>There is no alert raised if a manual capture stops due to a full disk.</p>	<p>Use the CLI <code>dir capture:</code> and <code>status</code> commands to check the available capture disk space.</p>

The following table describes known issues with the CLI.

**Table 9**      **CLI Issues**

<b>Description</b>	<b>Resolution</b>
When PNQM is used in auto-configuration mode with directly-connected interfaces (the ATM, FR, Leased Line network model), the remote BQM may generate too many signatures, including signatures of LAN traffic.	Use MPLS connectivity (with or without auto-configuration mode), or directly-connected connectivity without auto-configuration mode.
The show (peer-)interface ... pnqm command does not display the channel destination status correctly; it duplicates the source status. This can lead to the remote server being reported as working when it is in fact down and to the remote server being reported as down when it is working.	When checking PNQM channel status, check both directions.
When configuring packet capture, it is possible to see the following error message, even if the interface in question is not already attached to a packet capture:  <code>Error: Interface is already attached to a capture instance</code>	Reboot the device.
When using the status command on the Cisco ADE 2130, the number of CPUs may be misreported.	Resolved in the next release.

## 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.

Copyright © 2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0708R)