



# Release Notes for the Cisco Bandwidth Quality Manager, Release 4.0.4

---

April 3, 2008

These release notes contain Cisco Bandwidth Quality Manager (BQM) release 4.0.4:

- System requirements
- 4.0 to 4.0.4 upgrade procedure
- Resolved and known issues

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.

Table 1 indicates the upper limits on the number of sites and classes that can be configured on each of the supported Cisco Application Deployment Engine (ADE) platforms and the maximum measurement port bandwidth that can be monitored with each.

**Table 1** *Maximum Sites, Classes, and Total Measurement Port 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	3000	3000
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 4.0.4.

### Hardware Requirements

BQM 4.0.4 software runs on the Cisco ADE 1010, Cisco ADE 2120, Cisco ADE 2130 and Cisco ADE 2140. The product also supports upgrades for the Cisco 1180 platform. For more information, refer to the *Cisco Bandwidth Quality Manager 4.0 Installation Guide*. For more information on hardware requirements, contact your sales representative.

### Browser Requirements

Table 2 describes the browser requirement for all platforms.

**Table 2**      **Browser Requirement**

Browser	Version	Platform
Internet Explorer	6.0	Windows XP



---

**Note** Javascript should be enabled for the browser. Cisco recommends that you configure the browser to enable pop-ups.

---

## Related Documentation

The following product documentation is available for BQM 4.0.4:

- *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*

## BQM 4.0 to BQM 4.0.4 Upgrade

This section describes the steps to upgrade from BQM 4.0 (or BQM 4.0.3) to BQM 4.0.4.



---

**Caution** If you have a BQM 3.x release, you must first upgrade to BQM 4.0. For information on upgrading from BQM 3.x to BQM 4.0, refer to the *Release Notes for Cisco Bandwidth Quality Manager, Release 4.0*.

---

When upgrading a hub and spoke PNQM configuration to BQM 4.0.4, upgrade the spoke devices first, and then the hub. This will maximize the PNQM measurement uptime, as BQM 4.0.4 systems cannot receive PNQM signatures from BQM 4.0.3 or earlier systems.



---

**Note** You should stop any active manual packet captures before you perform the upgrade.

---

To upgrade from BQM 4.0 or BQM 4.0.3 to BQM 4.0.4:

---

**Step 1** Backup the current BQM 4.0 or BQM 4.0.3 system.



---

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

---

**Step 2** Obtain the BQM 4.0.4 upgrade image.

**Step 3** Use the following command to start the upgrade:  
`ssh admin@probe_name install system < image_name`

For example, to load the image named `CBQM-v4.0.4.853-GA.3311_RELEASE.upgrade` to a BQM named `data_center` specify:

```
ssh admin@data_center install system < CBQM-v4.0.4.853-GA.3311_RELEASE.upgrade
```



---

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

---

Once the device reboots, 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 or console that the database is being upgraded. When the device restarts, the upgrade is complete and you are prompted to log in to the system.

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-v4.0.4.853-GA.3311_RELEASE.upgrade standby-system-image
```

Use the reload command to reboot the Cisco ADE with the upgraded system image:

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

When the device restarts, the upgrade is complete, and the system prompts you to log in.



---

**Note** Cisco recommends that after you verify the system image upgrade, you should copy the chosen system image to the standby system image. This avoids subsequent accidental reload of an older version of the system image. Reloading an older version of the system image results in loss of data.

---



---

**Note** For more information on BQM 4.0 software installation, refer to the *Cisco Bandwidth Quality Manager 4.0 Installation Guide*. For detailed initial setup, licensing, and configuration information, refer to the *Getting Started Guide for the Cisco Bandwidth Quality Manager Release 4.0*.

---

## Resolved Issues

The BQM 4.0.4 release resolves the following issues:

**Table 3**      **Resolved Issues**

Description	Resolution
There was a regression in PNQM packet processing performance between BQM 4.0 and BQM 4.0.3.	The current release restores the appropriate level of packet processing performance.
Event-triggered packet capture files were getting deleted after a restore data-with-captures operation.	The system no longer deletes event packet capture files after a restore data-with-captures operation.
Over-allocation of memory to the database rollup process was leading to occasional BQM restarts after months of operation.	The current release fixes the database rollup memory issue.

## Caveats

This section provides information about general caveats and known issues in the BQM 4.0.4 software.

### Default Configuration

The default BQM configuration contains a default router and interfaces to measure traffic on each management port and their aggregate. If you remove the default interfaces, it is difficult to restore them. Refer to “Default BQM Configuration” in this document for details of the default configuration.

### Backup, Restore and Packet Captures

Before you backup or restore system data you should stop any active manual packet operations.




---

**Note** Restoring data from a previous version (for example, BQM 4.0) to BQM 4.0.4 is not supported.

---

### Packet Fragmentation

Any fragmentation caused by exceeding path MTU (not LFI) is not supported by the system for sizing 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 sections identify software issues that exist in the BQM 4.0.4 release. The known software issues are grouped as follows:

- Configuration
- Dashboard
- Network Service Quality
- Traffic Insight
- Event Analysis
- Bandwidth Sizing
- Alarms
- CLI

Table 4 describes the known configuration issues.

**Table 4**      **Configuration Issues**

Description	Recommendation
<p>The default configuration sets the displayed local port capacities (PortA, PortB, PortC, PortD) at 1Gbps and the aggregate PortABCD is set at 4 Gbps. These figures may not reflect the negotiated speed of the link being monitored.</p>	<p>The default values can be configured to match the actual link speed.</p>
<p>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.</p>	<p>Use the no subnet-filtering command from the CLI.</p>
<p>If you define a site, router and interface with PNQM enabled but forget to add subnets to the site, and then try to go back to add the missing subnets, an error is displayed.</p> <p>From Sites/Interfaces, click Add Remote Site.  Enter a name only, then click Add Router.  Enter a name, click Add Interface.  Enter a name, bandwidth and PNQM address only, then click Save.  Click Cancel to go back to add router screen.  Click Cancel to go back to add site screen.  Re-enter original site name, but this time supply a subnet too.  Click Add Router.</p> <p>The following error is displayed:</p> <p>“Site was not found to update. It was probably deleted while you were viewing it. Failed to update site.”</p>	<p>When configuring PNQM, remember to define subnets for sites when initially defining them.</p>

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...)
---	--

Table 5 describes the known Dashboard issue.

**Table 5**      **Dashboard Issues**

Description	Recommendation
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.

Table 6 describes the known Network Service Quality issue.

**Table 6**      **Network Service Quality Issues**

Description	Recommendation
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 1 millisecond.	Configure once-per-second ICMP pinging between the two BQMs to improve accuracy during the startup phase.

Table 7 describes the known Traffic Insight issues.

**Table 7**      **Traffic Insight Issues**

Description	Recommendation
DNS currently holds resolved hostnames on a per session basis.  When viewing Top-N results you are able to resolve to display hostnames, but you cannot switch back to view IP addresses.	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 place the cursor over the name.  Alternatively, you must log out and back in again to return to the original display of IP addresses.

Certain applications may not be recognized by the system and will instead be listed as Unknown.	In each case you can define a custom-application to match the port number.
---	--

Table 8 describes the known Event Analysis issues.

**Table 8** *Event Analysis Issues*

<b>Description</b>	<b>Recommendation</b>
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.	In future versions of the product all jitter calculations will be based on one-second calculations.
Results for Expected Queuing and PNQM may not be available in Event Analysis for an interface where a manual packet capture has been executed and completed. When this issue occurs, the Expected Queuing and PNQM plots will all be marked with a red line where the results are missing.	The device will need to be restarted to enable these interfaces to start recording Expected Queuing and PNQM results for use in Event Analysis.
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.	This will be resolved in future releases.

Table 9 describes the known Quality Alarms and System Alerts issues.

**Table 9** *Quality Alarms and System Alerts Issues*

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

Table 10 describes the known CLI issue.

**Table 10** *CLI Issues*

<b>Description</b>	<b>Recommendation</b>
Following a clear config command, previously configured GRE protocol decapsulation is persisted. Therefore GRE traffic will continue to be listed as Unknown.	Use the <code>no decapsulate gre</code> CLI command to disable GRE decapsulation, if required.

## Default BQM Configuration

Figure 1 lists the default configuration of network service objectives, class-maps, policy-maps, sites, routers, and interfaces present in the BQM configuration when first installed. The list represents the set of CLI commands required to re-establish any of the objects in the default configuration, if necessary.

**Figure 1** *Default BQM Configuration*

```

class-map class-default
  match any
class-map unknown-applications
  match application Unknown
nso-map high-speed
  measure-microburst milliseconds 20
  queuing-targets delay-milliseconds use-one-way protect-packets use-one-way
  protect-packets percent 99.90000 busy-period minutes 5
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-icmp interval-milliseconds 1000 size 40 event-thresholds delay loss
  one-way-latency milliseconds 50
  measure-pnqm packets-per-second 100 event-thresholds latency latency-variation loss
nso-map low-latency
  measure-microburst milliseconds 10
  queuing-targets delay-milliseconds use-one-way protect-packets use-one-way
  protect-packets percent 99.90000 busy-period minutes 5
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-icmp interval-milliseconds 1000 size 40 event-thresholds delay loss
  one-way-latency milliseconds 5
  measure-pnqm packets-per-second 100 event-thresholds latency latency-variation loss
nso-map low-speed
  measure-microburst milliseconds 100
  queuing-targets delay-milliseconds use-one-way protect-packets use-one-way
  protect-packets percent 99.90000 busy-period minutes 5
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-icmp interval-milliseconds 1000 size 40 event-thresholds delay loss
  one-way-latency milliseconds 750
  measure-pnqm packets-per-second 10 event-thresholds latency latency-variation loss
nso-map network-service-objective-default
  measure-microburst milliseconds 50
  queuing-targets delay-milliseconds use-one-way protect-packets use-one-way
  protect-packets percent 99.90000 busy-period hours 4
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-icmp interval-milliseconds 10000 size 36 event-thresholds delay loss
  one-way-latency milliseconds 500
  measure-pnqm packets-per-second 100 event-thresholds latency latency-variation loss
nso-map real-time
  measure-microburst milliseconds 10
  queuing-targets delay-milliseconds use-one-way protect-packets use-one-way
  protect-packets percent 99.90000 busy-period minutes 5
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-icmp interval-milliseconds 1000 size 40 event-thresholds delay loss
  one-way-latency milliseconds 120 variation milliseconds 30
  measure-pnqm packets-per-second 100 event-thresholds latency latency-variation loss
policy-map default
  nso network-service-objective-default
  trace-events
  class class-default
    nso network-service-objective-default
    queue-limit 64
local-site Local-site
  description "site in which BQM is deployed"
  router bqm
    interface PortA

```

```
    attached-port PortA
    bandwidth 1000000
    max-reserved-bandwidth 75
    no subnet-filtering
    service-policy output default
interface PortAB
    bandwidth 2000000
    max-reserved-bandwidth 75
    no subnet-filtering
    service-policy output default
interface PortB
    attached-port PortB
    bandwidth 1000000
    max-reserved-bandwidth 75
    no subnet-filtering
    service-policy output default
interface "Unknown Applications"
    bandwidth 1000000
    max-reserved-bandwidth 75
    no subnet-filtering
    filter-class unknown-applications
    service-policy output default
router default
    interface default
        bandwidth 2000000
        max-reserved-bandwidth 75
        subnet-filtering
        service-policy output default
    peer-interface default
        bandwidth 2000000
        max-reserved-bandwidth 75
        subnet-filtering
        service-policy output default
site "Unmatched Traffic"
    description "Unmatched traffic"
    subnet unmatched-remote
router default
    interface default
        bandwidth 1000000
        max-reserved-bandwidth 75
        subnet-filtering
        service-policy output default
    peer-interface default
        bandwidth 1000000
        max-reserved-bandwidth 75
        subnet-filtering
        service-policy output default
```

## 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.

CCDE, CCENT, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0803R)