Release Notes for the Cisco Bandwidth Quality Manager, Release 3.1

February 20,, 2007, OL-11100-02

These release notes provide general information about Cisco Bandwidth Quality Manager 3.1, including upgrade instructions, resolved and known software issues, and how to obtain technical assistance.

Cisco Bandwidth Quality Manager (BQM) provides unsurpassed visibility and analysis of traffic, bandwidth and QoS on packet networks.

The Cisco BQM product offering is an essential component of Cisco's solution for the new generation in congestion monitoring, analysis and control on IP networks to enable the assured delivery of applications and services over the Internet. BQM builds on revolutionary technology to deliver the new generation in congestion monitoring, analysis and control on IP networks through the following unique capabilities:

- Mitigates network application downtime with always-on quality impact assessment of traffic to determine if current network can meet application service quality objectives
- Provides optimized bandwidth sizing and/or QoS policy design for network to meet user-specified application service quality objectives
- Rapidly pinpoints and resolves network application service quality problems which are often invisible to current network tools

What's New in this Release?

BQM software is now available on the Cisco 1180 appliance.

Configuration of site interfaces in the BQM network model has also been improved.

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

Note For more information on release 3.1 software installation, see the "Cisco Bandwidth Quality Manager 3.1 Installation Guide."

For detailed initial setup and configuration information, see the "Getting Started Guide for the Cisco Bandwidth Quality Manager, Release 3.1".

System Requirements

This section describes the hardware and browser requirements for BQM 3.1.

Hardware Requirements

BQM software runs on the Cisco 1180 appliance. Contact your sales representative for more information about hardware requirements.

Browser Requirements

The following table describes the browser requirements for all platforms.

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 3.1:

- Cisco Bandwidth Quality Manager 3.1 Installation Guide
- Getting Started Guide for Cisco Bandwidth Quality Manager Release 3.1
- Cisco Bandwidth Quality Manager 3.1 User Guide

Release 3.0 to 3.1 Upgrade

This section describes the steps involved in upgrading from release 3.0 to release 3.1.

Note Performing a CD installation of release 3.1 on a BQM running release 3.0 will result in all data collected using version 3.0 being lost.

To perform an upgrade from version 3.0 to version 3.1 you do the following:

Step 1 Obtain the 3.1 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 3.0 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 upgrade: ssh admin*@probe_name* install system < *image_name*

So, for example to load the image file named CBQM-v3.1-B6.2.24565_RELEASE.upgrade on to a BQM named data_center you would use the following:

```
ssh admin@data_center install system < CBQM-v3.1-B6.2.24565_RELEASE.upgrade
```

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 BQM 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 1180:

```
copy tftp://[hostname|A.B.C.D]/CBQM-v3.1-B6.2.24565_RELEASE.upgrade standby-
system-image
```

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

```
reload standy-system-image
```

Caveats

This section provides information about known and resolved issues in the BQM 3.1 software.

Corvil Bandwidth and Elastic Traffic
Corvil Bandwidth measures the bandwidth required by the traffic currently existing on your network to achieve the stated QoS targets. If the bandwidth available in the network changes, then the traffic may also change in response. For example, if a network is upgraded then bandwidth-limited TCP flows may increase their sending rate, or users may make more active use of particular applications. Corvil Bandwidth does not make predictions about the effect these changes could have on network QoS. Consequently, the target QoS may not be achieved after an upgrade, because of heavier network use by applications and users.

These effects are most likely to be seen in networks where QoS is currently poor, so that the network is the limiting factor for application performance. In these case the Corvil Bandwidth value does always indicate the minimum bandwidth required to meet the targets, since even the existing traffic will not achieve the targets at lower bandwidths.

If upgrading the network bandwidth results in heavier network use, so that the targets are still not achieved, then the Corvil Bandwidth value will indicate that a further upgrade is necessary. We recommend that the Corvil Bandwidth value should be monitored continuously before and after an upgrade, in order to verify that the desired network performance is achieved.

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.

Replacement Disk Requires RAID Rebuild
When a disk is removed and then replaced, disk alerts remain active and the RAID array itself needs to be rebuilt. With a connected monitor and keyboard you can use the console tools to rebuild the logical disk volumes, but you will lose all collected data.

Resolved Issues

The following issues are resolved in the 3.1 release. The issues are grouped under the following areas:

- Configuration
- General GUI issues
- Dashboard
- Traffic Insight
- Congestion Analysis
- Bandwidth Sizing
- Alarms
- CLI

The following table lists the resolved configuration issues:

Table 3 Configuration Resolved Issues

If you duplicate an interface (or a site), and then change the name of the interface, an error message is displayed indicating that the save has failed.
If you edit class-default in a Strict Priority Queuing (SPQ) configuration, the screen displays Modular QoS CLI options. When you click Cancel the policy map now has the Modular QoS CLI button set and the SPQ button is disabled. This does not affect the class-map - it saves correctly as SPQ. Note - if you edit the class-map in CLI then the GUI picks it up correctly.
If you enter a filter for custom applications on a page where there are no applications of the filtered type, the filter returns an empty list, but indicates the number of matching applications found.
If you configure a remote site with a directly connected interface to the local site, and subsequently use the GUI to remove the connection by selecting None on the Local site panel, the save is confirmed on the GUI as successful. The connection is, however, not removed.
Creating a remote site without any subnet results in the interface matching all traffic. This causes a couple of issues: one is that a user creating a set of remote sites without defining subnets will have some serious performance issues on a busy link. Another issue is that adding in the subnets later does not invalidate the previous capture data. This means sizing links to remote sites will be based on traffic data captured for all links. 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.

If you set Link Fragmentation and Interleaving (LFI) or Layer 2 overhead when configuring site interface details using the GUI, disabling these options using the check boxes does not disable the overhead configuration.
The default policy-map, monitor-queuing-map, class-map and monitor-end2end-maps cannot be edited or deleted but these options are displayed as available actions.

The following table lists the resolved GUI issues:

Table 4 GUI – General Resolved Issues

Using the options to View All, View 50 or View 100 interfaces on a screen does not get picked up by PDF generation. The PDF displays only the default 20 interfaces.
The View Outbound/Inbound link in the top right on the Traffic Insight and Congestion analysis interface screens is sometimes missing and sometimes points to the wrong interface.
If you disable monitoring graphs via the monitor queuing maps, the graphs are shown as 'Not Configured' but the values for Max/Average/Min are still displayed.
If the BQM is restarted, the GUI initially displays a page which indicates that the device is starting. This is a static page html and no progress is actually being done. You have to refresh the page to open the GUI login page.
If you pause a screen while trying to diagnose a certain event and then click the Pause button again to allow screen refreshes, you may be logged out as if the session timed out in the background.
If you leave a GUI session open overnight and then select, for example, a Traffic Insight interface and in the custom period area click on the calendar, the previous day's date is highlighted rather than the current date. Selecting the View Period button then displays an error message indicating that the date is invalid and you have selected a time in the future.

The following table lists the resolved dashboard issues:

Table 5 Dashboard Resolved Issues

When viewing graphs using a selected reporting period of twelve hours on the dashboard screen, the displayed graphs are considerably smaller when compared to other time periods.
Classes and interfaces are highlighted in the navigation tree view when the Congestion Indicator is 1.0. This should only happen when the Congestion Indicator is greater than 1.0.
The Total Congested Interfaces bar may show inconsistent results, particularly after a configuration change where interfaces have been deleted.
Due to rounding,, the percentages displayed for the Application Leaders may not always add up to 100%.

The following table lists the resolved traffic insight issues:

Table 6 Traffic Insight Resolved Issues

The pattern of details in the graphic displayed under the Microburst heading does not necessarily correspond with the actual pattern of microburst measurement as displayed in the Microburst Detection graphs.

The following table lists the resolved congestion analysis issues:

Table 7 Congestion Analysis Resolved Issues

Even if the measured roundtrip delay constantly violates the delay threshold, the Time in Events value never goes beyond 30%.
Configuration changes are not being indicated on the Event Analysis graphs.
When there is an Expected Loss value of 100%, the minimum value for Expected Delay goes to zero.
The Time In Events value may display over 100% for 30 minute custom period.
When you attempt to analyze events indicated on the interface quality timeline in the Congestion Analysis screen, there is no

corresponding event indicated in the event analysis timeline.

The following table lists the resolved bandwidth sizing issues:

Table 8 Bandwidth Sizing Resolved issues

If you reconfigure the interface capacity value, the change is updated immediately on the GUI but the class capacities are not updated until the next data rollup, five minutes later.
If you roll over the Corvil Bandwidth graphic it appears to be linked, but clicking the graphic produces no action.

The following table lists the resolved quality alarms and system alerts issues:

Table 9 Quality Alarms and System Alerts Resolved Issues

Clicking on an active alarm frequently leads to a blank page or the summary page of new alarms. If you wait for 3-6 seconds before you click an alarm it will be gone. (There is a three-second poll time for events, which is not configurable). Generating a PDF sends a request to get the page view, but this will almost always be different from the user's view. Usually a blank PDF is generated.
The header title for the acknowledged column of the tables of the active and cleared alarm pages is missing.
Using an LLQ scheduling system, when policer violations occur, they are displayed in the Quality Alarms screen as Expected Queuing Loss Threshold Exceeded.
If, with the last hour time period selected, you open Quality Alarms and expand an alarm for Expected Queuing Loss Threshold Exceeded the graph for the alarm is displayed without any data in it.

The following table lists the resolved CLI issues:

Table 10 CLI Resolved Issues

Usage help for the **measure-ping** command indicates that the allowed range for ping intervals is 10 – 1000000 ms.
If there is a CPU failure the system restarts on a single CPU. However, there is no CPU alert and the system alerts that do appear are flagged as disk alerts.
When you use the show file-systems command, the manual capture disk statistics for percentage of disk space used are not displayed or updated correctly.
If the disk utilization of disk 0 exceeds 95%, an alert is raised and further disk writes are prohibited. If this occurs while a local backup is in operation, the backup does not detect this and does not recover when the utilization returns below 95%.
If you restore a configuration onto the device that has a manual packet capture configured, it automatically starts this packet capture.
It is possible to specify more than one attach interface (or peer-interface) command for a manual packet capture. However if the device is restarted then only one of the attached interfaces is persisted.
Usage help for the **show interfaces** <*name*> **stats top N** command displays a valid range from <1-100>**.**
If you run a backup including packet capture files on a system which is currently running a packet capture, and then attempt to restore all the data, including capture files, the restore hangs.

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
- General GUI issues
- Dashboard
- Traffic Insight
- Congestion Analysis
- Bandwidth Sizing
- Alarms
- CLI

Table 3 Configuration Issues

Description	Resolution
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.
Avoid creating remote sites without defining a subnet.	Note the following recommendations when making changes to remote site subnet definitions: * adding to the range of subnets: no action required. * reducing the range of subnets: delete the site and recreate it. * reconfiguring due to misconfiguration: delete the site and recreate it.
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. After configuring sites, routers, and interfaces, it can take up to ten	In general, when creating a new interface, wait at least five minutes before looking for results in all screens.

minutes for the interface to be displayed on the Traffic Insight tab.	The Traffic Insight tab issue is a screen refresh problem. The workaround here is to go to a different page on the tab, sort or filter the page, or change tabs. The interface should then be displayed.
When configuring monitor-queuing-maps in the GUI, it is not possible to disable the queuing delay target.	Use the CLI to configure a monitor-queuing-map with a disabled queuing delay target. Use the queuing-targets command with no parameters.
There are the following issues when renaming monitor-queuing-maps using the CLI: - When you try to rename a monitor-queuing-map, the CLI displays messages relating instead to a "queuing-map". - When you do rename a monitor-queuing-map, the old name still appears in any policy-maps using that map. - There's no way to rename monitor-end-to-end-maps.	There is no workaround for this issue.
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. There is no option to do this on the GUI.	There is no workaround for this issue.
If you rename a custom application that is referenced in a class-map, and then use the show class-maps command to view the results, the new name is not displayed.	There is no workaround for this issue.
A validation error is returned when trying to add an advanced match rule with the following criteria: - Protocol set to UDP/TCP - Source Port set or Destination Port set - Any other option from VLAN, MPLS, or Ethertype set	Use the CLI to configure advanced match rules with the criteria shown.
If you are configuring a new monitor-queuing-map and select a busy-period less than 4 hours and then check or uncheck another available option (for example, Generate Events when CB exceeds), the screen redraws and the busy period value reverts to the default of 4 hours.	When configuring a monitor-queuing-map, check or uncheck the chosen options first. Then select a busy period before saving.
You cannot use the GUI to apply a different monitor-queuing-map to class-default.	Use the CLI if you want to apply a different monitor-queuing-map to class-default.

The following table describes known issues with the GUI.

Table 4 GUI – General Issues

Description	Resolution
The response times on certain GUI screens may result in long delays where large data queries are requested.	There is no workaround for this issue.
If you define a custom period to view monitoring information and leave it configured for more than an hour, navigating between different screens may result in data not being displayed.	Switch to one of the standard reporting periods from the Reporting Period list.
If you open two GUI browser sessions, logged in as admin, but with one window in System Administration mode and the other in Bandwidth Quality Manager mode, when the Bandwidth Quality Manager mode screen refreshes, the System Administration mode window also refreshes but switches to Bandwidth Quality Manager mode.	There is no workaround for this issue.
The Pause button prevents a screen refresh for the current screen only. If you move to a different screen, even though the Pause icon is still highlighted, the new screen will refresh and the data updated after five minutes.	To pause all data updates, define a custom period for the period of interest.
In some cases the help content is inaccessible because there is no vertical scrollbar on the help window.	Refer to the User Guide to see the relevant content.
Sorting by certain columns on the Edit Site and Edit Router screens causes an empty router/interface list to be displayed. Screens/columns affected: * Edit Site Screen -(local site) Port column -(remote site) Description column * Edit Router Screen -(local and remote site) Interface Name, Port, and Bandwidth columns	The correct list is displayed if another sorting column is selected.
Creating large PDF reports (50 pages) may cause a Java Heapspace OutOfMemory exception and an error message is displayed in place of the correct PDF report. If you close all browser windows and then attempt to log in, a system error message is displayed.	Wait for at least 15 minutes before attempting to log in to the GUI.
Using a text filter option as well as one or more column filters may not provide the desired results. If you first use a column filter and then try to filter using the text field, the column filters will be reset to All when you click the Filter button. Also, clicking the Clear button beside the text field at any stage, whether there is a text filter applied or not, will reset the column filters back to All.	The interface list can be filtered by typing into the text field and pressing the Filter button, and then further narrowed by cumulatively using the column filters.

The following table describes known issues with the dashboard.

Table 5 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.
Even if Congestion Indicator is not configured for a particular class, the five-minute Congestion Indicator graph does not get turned off on the dashboard. The corresponding graph is turned off on the Congestion Analysis page.	There is no workaround for this issue.
After a clear config, the total congested interfaces bar still shows the old total interfaces value.	There is no workaround for this issue.

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

Table 6 Traffic Insight Issues

Description	Resolution
Rounding of mean values displayed with the time series plots may produce zero values even when there was some data. This effect is more likely when there are gaps in time series data and most of values are near zero.	There is no workaround for this issue.
If you leave a custom period set for greater than one hour, data may no longer be displayed.	Choose a different report period.
MSN Messenger Chat application traffic may not always be correctly identified and labeled.	There is no workaround for this issue.

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

Table 7 Congestion Analysis Issues

Description	Resolution
If you select a sufficiently short period on the 30 or 60 day quality timeline, the resulting event analysis page does not give a clear indication of the date of the selected timescale.	Avoid selecting very short timescales from the 30-day or 60-day reporting periods.
If you create a sufficiently large number of classes (greater than fifteen), they will not all be accessible in the event analysis window.	There is no workaround for this issue.
If you select a custom report period and then choose an event to analyze, the event inspection window may occasionally not display event graphs.	Close the event inspection window and select the custom report period and event again.

When selecting a date using the To or From calendar widget on the inspection page, an error dialog pops up.	Click Ok to close the error message dialog. The chosen dates are populated correctly and you can ignore the error message.
It may not be possible to view event analysis information for short individual events displayed to the extreme left of the quality events timeline in the 24-hour reporting period.	There is no workaround for this issue.
The monitor queuing details, including specific delay targets and sizing policy, are displayed at the interface level in the Congestion Analysis screen, but are not relevant for an interface. They are shown correctly per class.	There is no workaround for this issue.

The following table describes known issues with the Bandwidth Sizing tab.

Table 8 Bandwidth Sizing Issues

Description	Resolution
If a packet with a size greater than the configured policer burst size (for example 200 bytes) is measured, the system correctly reports that the burst size needs to be increased, but the reported Corvil Bandwidth values on the CLI and in the GUI graph plot are not correct.	Follow the recommendation but ignore the Corvil Bandwidth as an indicator of required bandwidth.

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

Table 9 Quality Alarms and System Alerts Issues

Description	Resolution
When you generate a PDF, the Corvil Bandwidth Threshold Exceeded alarm graph is displayed as in the browser, but the Expected Queuing Loss Threshold Exceeded graph is much smaller.	There is no workaround for this issue.
If you attempt to sort on the Severity column all of the previously displayed alarms may no longer be displayed and the alarm count may be shown as "-1". Selecting any of the other columns to sort on will display the correct alarms and the correct count.	There is no workaround for this issue.
The Count value may display negative values when ports are shut down.	There is no workaround for this issue.
No graph is displayed for Expected Policing Threshold Exceeded alarms.	There is no workaround for this issue.
Reported alarms persist beyond a clear config command.	There is no workaround for this issue.

When alarms are issued for class-default, the Source field displays only the relevant interface name. Interfaces and classes have separate microburst graphs so the same alarm source is displayed for either an interface violation or class-default.	Use the Congestion Analysis tab to determine whether the microburst alarm is for an interface or class.

The following table describes known issues with the CLI.

Table 10 CLI Issues

Description	Resolution
If you perform a backup for one BQM appliance and restore this backup to a second BQM appliance, the restore operation overwrites the set of IP address settings on this second device. However, the changed IP address settings do not take effect until the next reboot of the system. So after the next reboot of the second appliance, you will have two appliances with the same IP address on the network. Similarly, a remotely-initiated restore to a BQM appliance on a different subnet may result in this appliance becoming inaccessible after its next reboot.	Following a restore operation to a second appliance, use the setup command on this second appliance to configure the appropriate IP address settings.
If you are using anonymous ftp to perform backups, the backup operations complete but a restore may fail because it sees an incomplete backup directory on the ftp server. Some ftp programs (for example, vsftp) do not allow anonymous uploaders to create or delete files or directories.	Check that you have read/write access on the target ftp server before performing backup and restore.
Large packet capture files (~16GB) can take up to 15 minutes to close when you issue a **no capture** command. If you attempt to immediately delete any such capture files, you may see the following error message: `Error: Cannot delete file because it is currently used by a packet capture instance`	Wait at least 15 minutes before attempting to delete large, recent packet capture files.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non emergencies.

- For non emergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*. Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security

Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use. If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

http://www.cisco.com/offer/subscribe

The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

http://www.cisco.com/go/guide

Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

http://www.cisco.com/go/marketplace/

Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

http://www.ciscopress.com

Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

http://www.cisco.com/ipj

Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

http://www.cisco.com/en/US/products/index.html

Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

http://www.cisco.com/discuss/networking

“What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

World-class networking training is available from Cisco. You can view current offerings at this URL:

http://www.cisco.com/en/US/learning/index.html