



Release Notes for the Cisco Multicast Manager 2.3.3

These release notes are for use with the Cisco Multicast Manager (CMM) running on Solaris 8, Solaris 9, or Red Hat Enterprise Linux AS Release 3 (Taroon Update 4).



Note

You must be running CMM version 2.3 to install the 2.3.3 upgrade.



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

© 2006 Cisco Systems, Inc. All rights reserved.

Contents

These release notes cover:

- [New Features, page 2](#)
- [Releases and Issues, page 3](#)
- [Product Documentation, page 9](#)
- [Obtaining Documentation, page 9](#)
- [Documentation Feedback, page 11](#)
- [Cisco Product Security Overview, page 12](#)
- [Obtaining Technical Assistance, page 13](#)
- [Obtaining Additional Publications and Information, page 16](#)

New Features

New features for CMM 2.3 include:

- Persistent telnet support for 6500 troubleshooting
- Top talkers for 6500 troubleshooting
- Interface descriptions to multicast forwarding trees
- Monitoring of RPF failures
- Monitoring of bps as well as pps
- View of latest events

Releases and Issues

Table 1 describes all CMM releases, associated upgrade notes, supported platforms, and all resolved or open issues known to exist in each release.



Note

To obtain more information about known problems, access the Cisco Software Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl> (you will be prompted to log into Cisco.com.)

Table 1 *CMM Releases and Issues*

Release	Upgrade Notes	Platform	Description
CMM 2.3.3	You must be running version 2.3 to install the 2.3.3 upgrade.	All IOS-based routers, including the 6500 and 12000. The CRS and blade servers are not supported.	• Persistent telnet support for 6500 troubleshooting • Top talkers for 6500 troubleshooting • Interface descriptions to multicast forwarding trees • Monitoring of RPF failures • Monitoring of bps as well as pps • View of latest events

Table 1 ***CMM Releases and Issues***

Release	Upgrade Notes	Platform	Description
CMM 2.3.2(1)	You must be running version 2.3 to install the 2.3.2(1) patch.	All IOS-based routers, including the 6500 and 12000. The CRS and blade servers are not supported.	Resolved Issues: • CSCsc24313—Database intermittently being corrupted. • CSCsc24317—Discovery takes a long time on some networks. • CSCsb51759—Trace not working when LHR is set to something other than ALL. • CSCsb45664—SNMP queries failing on *,g from trace. • CSCsb53066—Trace sometimes shows a router forwarding on *,g instead of s,g. • CSCsb52243 LTL—Check Showing False Positives. • CSCsb45715—CMM not working with IOS experimental versions. • CSCsb64157—RRD file not updating from threshold monitoring. • CSCsb69663—Remove device from database not working. • CSCsb96077—Channelized interfaces not showing up on forwarding tree. • CSCsb96086—Virtual interfaces not appearing correctly on forwarding tree display. • CSCsb96096—IOS version report not sorting by version or model.

Table 1 *CMM Releases and Issues*

Release	Upgrade Notes	Platform	Description
CMM 2.3.2	You must be running version 2.3 to install the 2.3(2) upgrade.	All IOS-based routers, including the 6500 and 12000. The CRS and blade servers are not supported.	Resolved Issues: - CSCsb45326—Polling daemon exits abnormally on certain domain names. - CSCsb45726—Discovery stops while gather IP information in some networks. - CSCsb45715—CMM not working with IOS experimental versions. Unresolved Issues: - CSCsb45664—SNMP queries failing on *,g from trace. Added Features: - CMM and CRM interfaces are now separated. Each can be selected via a tool dropdown. Also included in the tool dropdown is an Administration option. Administration contains functions that are common to both CMM and CRM.

Table 1 ***CMM Releases and Issues***

Release	Upgrade Notes	Platform	Description
CMM 2.3.2 (continued)		All IOS-based routers, including the 6500 and 12000. The CRS and blade servers are not supported.	- Support for polling start/stop times per polling interval.  Note There is now a housekeeping thread that will run every hour to remove old route monitoring reports. By default, any report over 30 days will be removed, or if there are more than 12 reports for a single baseline, only the most recent 12 reports will be kept. These parameters can be modified under Administration, Global Polling Configuration. The housekeeping thread will run immediately upon upgrading the application. - Support for 12.3T, 12.4, and 12.4T. - The route monitor polling interval has been restricted to a minimum of 1 hour. For more frequent checking of routes, the specific route monitoring feature should be used. [CRM] Support for monitoring of specific routes in addition to full routing table monitoring. [CMM] Support for tracing bidir multicast forwarding trees. [CMM] GroupAddress and groupMask added to RP status and RP summary screens.

Table 1 ***CMM Releases and Issues***

Release	Upgrade Notes	Platform	Description
CMM 2.3.2 (continued)		All IOS-based routers, including the 6500 and 12000. The CRS and blade servers are not supported.	• [CMM] Provides MDSP status info for all MSDP enabled devices, not just RPs. • [CMM] Support for Native IOS switches under Layer 2 Diagnostics. • [CMM] Improves forwarding tree graph rendering times. Caveat: • IGMP Diagnostics will not work for IOS 12.0S devices.
CMM 2.3.1	You must be running version 2.3 to install the 2.3(1) upgrade.	All IOS-based routers, including the 6500 and 12000. The CRS and blade servers are not supported.	• TACACS login support added for the application. • If the keys are configured incorrectly, they will have to be manually changed in the /opt/RMSMMT/httpd_perl/conf/httpd.conf file. • Tacacs_Pri_Key tac_plus_key • Tacacs_Sec_Key tac_plus_key

Table 1 ***CMM Releases and Issues***

Release	Upgrade Notes	Platform	Description
CMM 2.3.1 (continued)		All IOS-based routers, including the 6500 and 12000. The CRS and blade servers are not supported.	<pre><Sample AAA Server Config> group = admins { service = connection { priv-lvl=15 } } group = netop { service = connection {} } user = mike { member = netop login = des mRm6KucrBaoHY } user = admin { member = admins login = cleartext "ciscocmm" } </Sample AAA Server Config></pre> • Output filter added for IGMP Diagnostics. • Filtering option added in RP Polling Report. Clicking on a source, will now filter the report, so only that source and group are shown.

Product Documentation



Note

Electronic documentation is sometimes updated after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 2 describes the product documentation available for CMM.

Table 2 **CMM Documentation**

Document Title	Available Formats
<i>Release Notes for Cisco Multicast Manager</i>	• PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/en/US/products/ps6337/tsd_products_support_series_home.html
<i>Quick Start Guide for Cisco Multicast Manager</i>	• PDF on the product CD-ROM. • Printed document that was included with the product.
<i>Installation Guide for Cisco Multicast Manager</i>	• PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/en/US/products/ps6337/tsd_products_support_series_home.html
<i>User Guide for Cisco Multicast Manager</i>	• PDF on the product CD-ROM. • On Cisco.com at http://www.cisco.com/en/US/products/ps6337/tsd_products_support_series_home.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support 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 (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI 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.

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 TAC 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 TAC 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)—Your 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 operation 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 your network is impaired, but 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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>

- *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>

- 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>

This document is to be used in conjunction with the documents listed in the “[Product Documentation](#)” section.

CCVP, the Cisco logo, and Welcome to the Human Network 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, 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, Networkers, 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. (0711R)

Copyright © 2006 Cisco Systems, Inc.
All rights reserved.

