Release Notes for Cisco Route Manager Version 2.3

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

These release notes provide:

CISCO SYSTEMS

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

New Features

Release 2.3 contains the following new features:

- Verification of unicast routing tables —Check on any routing table and if any new, deleted or changes have occurred then a snmp trap is sent and a report generated.

- Verification of multicast routing tables—Check on any routing table and if any new, deleted or changes have occurred then a snmp trap is sent and a report generated.

- Flexible Scheduling—The checks can be run at scheduled periods or on-demand.

- Historical Reports—The number of routes that exist is stored at each polling interval and this information is available

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

Table 1   Product Documentation

Document Title	Available Formats
Release Notes for Cisco Route Manager	• PDF on the product CD-ROM. • On Cisco.com at http://www.cisco.com/en/US/products/sw/netmgtsw/. Navigate to Cisco Route Manager.
Quick Start Guide for Cisco Route Manager	• Printed document that was included with the product. • On Cisco.com at http://www.cisco.com/en/US/products/sw/netmgtsw/. Navigate to Cisco Route Manager.
Installation Guide for Cisco Route Manager	• PDF on the product CD-ROM. • On Cisco.com at http://www.cisco.com/en/US/products/sw/netmgtsw/. Navigate to Cisco Route Manager.
User Guide for Cisco Route Manager	• PDF on the product CD-ROM. • On Cisco.com at http://www.cisco.com/en/US/products/sw/netmgtsw/. Navigate to Cisco Route Manager.

Additions and Updates

Table 2 describes problems known to exist in this 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 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
CMM 2.3	You must be running Version 2.2(2) to install the 2.3 upgrade.		• Adds support for route monitoring reports via email • Changes how S,Gs are polled for exsitence. As of version 2.2(2) sgDeletion traps are now sent by the threshold polling thread. That is, with RMON style traps enabled, threshold polling will now generate the following traps: – hiThresholdExceeded – loThresholdExceeded – sgThresholdNormalized – sgDeletion Therefore, any S,Gs that were configured with thresholds of -1,-1, should be changed to have positive hi/lo thresholds. These changes can be done from the SG Polling Configuration screen. • Adds user description per user id. • Adds DNS lookup of multicast addresses • Adds support for filtering of S,G queries • Adds support for manual entry of S,Gs • Adds support for multiple community strings per domain along with device specific SNMP timeout and retries • Adds support for DR monitoring

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description

CMM 2.2(2)]	You must be running Version 2.1(3) to install the 2.2(2) upgrade.
	
	If you are upgrading from 2.1(3) you must run configure.sh from the application home directory:
		Solaris
		`cd /opt/RMSMMT`
		`./configure.sh`
		
		Linux
		`cd /usr/local/netman`
		`./configure.sh`
			• Fixes CMM0068 - multicast domains with a "." in the name are not displayed correctly.
			
			• Adds support for sending of sgDeletion trap for threshold polling with RMON style thresholds.

CMM 2.2(1)]	You must be running Version 2.1(3) to install the 2.2(1) upgrade.
	
	After upgrading you must run configure.sh from the application home directory:
		Solaris
		`cd /opt/RMSMMT`
		`./configure.sh`
		
		Linux
		cd /usr/local/netman
		./configure.sh
			• Fixes CMM0069 - Missing IP address database causing OK screen.
			
			• Fixes CMM0071 - IP address in events.log may not be consistent with db after srd.
			
			• Fixes CMM0072 - Polling daemon exits abnormally
			
			• Fixes CMM0073 - The polling daemon will not run and produces the following error in the rmspolld.log file: 12/15/2004 14:45:50 Error in config file on line 9. Exiting.
			
			• Adds support for DNS lookups during discovery to determine the management address of a device.

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description

CMM 2.2	You must be running Version 2.1(3) to install the 2.2 upgrade.
	
	You must obtain a license.key file prior to upgrading to 2.2.
	
	Version 2.2 of CMM requires a license file. The license will be valid for (CMM) or (CMM/CRM). The application license is contained in the license.key file. This file must be placed in
		Solaris
		`/opt/RMSMMT/mmtsys/sys`
		
		Linux
		`/usr/local/netman/mmtsys/sys`
			• The file must be owned by mmtuser chown mmtuser:mmtuser license.key and be set read-only chmod 0444 license.key
			
			• The license is tied to the IP address of the server that the application is running on.
			
			• After upgrading you must run configure.sh from the application home directory:
			
			Solaris
			`cd /opt/RMSMMT`
			`./configure.sh`
			
			Linux
			`cd /usr/local/netman`
			`./configure.sh`
			
			• This release includes a new start-up script which can also be used as a watchdog script for the polling daemon. The S98mmtpolld script is called from S98mmt. Therefore the polling daemon will now start when the application is started. The S98mmtpolld script can also be run from cron every 5 minutes as show below to ensure that the polling daemon is always up:

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
			Solaris
			0,5,10,15,20,25,30,35,40,45,50,55 * * * * /opt/RMSMMT/S98mmtpolld
			Linux
			*/5 * * * * /usr/local/netman/S98mmtpolld
			• Adds support for RP Status Monitoring.
			• Adds support for running Single Router Discovery in the background. If a device is being rediscovered by the polling daemon, the database will be locked and the list of routers will display the message "Cannot access database" until the discovery is complete.
			• Adds support for unicast/multicast route monitoring.
			Querying the routing table via SNMP, can in certain cases cause the CPU utilization on the router to become excessively high which can potentially disrupt the network. Once recommendation stated in the link below is turn on CEF and use get-bulk requests.
			http://www.cisco.com/en/US/tech/tk648/ tk362/technologies_tech_note09186a008 00948e6.shtml

Table 2 Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
			• CMM does use get-bulk requests when querying the routing table.
			• Adds support for sorting the S,G polling configuration table.
			• Adds time range support on the Graphs (Trends) interface.
			• Adds MAX EVENTS option to reporting function.
			• Improves text display of forwarding trees.
			• Fixes CMM0061 - Forwarding tree not being drawn accurately in some cases.
			• Fixes CMM0062 - Interfaces not shown on LHRs.
			• The changes made to the rendering of the forwarding trees will cause the current baselines to appear invalid. Any existing baselines should be replaced with baselines created by the current version.

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
			• CMM does use get-bulk requests when querying the routing table. • Adds support for sorting the S,G polling configuration table. • Adds time range support on the Graphs (Trends) interface. • Adds MAX EVENTS option to reporting function. • Improves text display of forwarding trees. • Fixes CMM0061 - Forwarding tree not being drawn accurately in some cases • Fixes CMM0062 - Interfaces not shown on LHRs • The changes made to the rendering of the forwarding trees will cause the current baselines to appear invalid. Any existing baselines should be replaced with baselines created by the current version.
CMM 2.1(3a)	You must be running Version 2.1(3) to install the 2.1(3a) patch/update.		• Adds support for sorting IOS version table. • Adds support for graphing up to 3 devices under Graphs (Trends). • Fixes CMM0059 - Running discovery after adding L2 switches corrupts switch entries. • Fixes CMM0060 - Newly configured domain is not the default on discovery screen.

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
CMM 2.1(3)	You must be running Version 2.1(2) or higher to install the 2.1(3) upgrade.		**Upgrading Only** • After upgrading to 2.1(3) run rrdfix.pl. It may be necessary to set the LD_LIBRARY_PATH prior to running the script as described below. If rrdfix.pl produces the following error message: Can't load '/opt/RMS /perl/lib/site_perl/5.8.0/sun4-solaris/auto/BerkeleyDB/BerkeleyDB.so' for module BerkeleyDB: ld.so.1: Then issue the following command in the shell, and re-run the script. **Solaris:** LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/RMSMMT/mmtsys/lib export LD_LIBRARY_PATH **Linux:** LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/netman/mmtsys/lib export LD_LIBRARY_PATH

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
			• Adds support for IGMP Last Reporter queries. • Adds support for 12.2.*.BC* releases. • Adds support for S,G pps delta checks between routers on a tree. • Adds support for MSDP Peers in health checks. This may require a rediscovery of the network. • Adds support for single router discovery/rediscovery. • Adds support for graphing PPS between more than two routers. • Adds show ip mroute active on diagnostics. • Adds option to delete forwarding tree baselines. • Optimized reporting functions. **Caveats** • Devices should be rediscovered if changes have been made that cause the ifIndex values to change. When possible, devices should have "snmp ifindex persist" configured. • Using the Enter key instead if clicking available buttons can cause unexpected behavior when saving traces. • Time-based thresholds cannot contain blank entries between settings.

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
CMM 2.1(2e)	You must be running Version 2.1(2) to install the 2.1(2e) patch/update.		This patch fixes a problem with detecting tree changes when partial trees are being used as a baseline, i.e., when the FHR and LHR are set to something other than SOURCE and ALL.
CMM 2.1(2d)	You must be running Version 2.1(2) to install the 2.1(2d) patch/update.		This patch fixes the order of the varbinds for the hiThresholdExceeded trap.
CMM 2.1(2c)	You must be running Version 2.1(2) to install the 2.1(2c) patch/update.		This patch fixes a problem observed with the polling daemon when intervals of 1 second are used on threshold and layer 2 polling. The problem may also intermittently occur when small polling intervals are used on very slow systems.
CMM 2.1(2b)	You must be running Version 2.1(2) to install the 2.1(2b) patch/update.		This patch provides an option on the system configuration screen tospecify the tftp server address for the domain. The default will be the IP address of the host as defined in the /etc/hosts file. Fixes source count on Show All Groups.

Table 2 Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
CMM 2.1(2)	You must be running Version 2.1(1) to install the 2.1(2) upgrade. **Upgrading Only** After upgrading to 2.1(2) run httpdconfig.sh.		• Global versus local email and trap receivers now work correctly. • SSG exceptions are now checked per domain. • Health checks are now supported. • Support for BiDir has been added. • S,G cache is now created even if there are no RPs present in a domain. • Time-based thresholds have been increased to 50. • RMON style traps are now available for PPS threshold events. • Support for RP group thresholds has been added. • rpAddition and rpDeletion traps can now be disabled. • Support for the STOP button has been added. Note however, that stopping a discovery before it's completed will most likely result in an unusable database for the domain. If a discovery is stopped for some reason, it should at some point be permitted to run tocompletion.

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
			Caveats • ATM sub-interfaces may not be reported correctly on multicast forwarding trees. • Using the Enter key instead if clicking available buttons can cause unexpected behavior when saving traces. • Time-based thresholds cannot contain blank entries between settings.

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
CMM 2.1(1)	If you are running an rc version of 2.1 you must remove it before installing 2.1(1).		• Adds support for IOS 12.3 • As of version 12.3 MIB support for the IPMROUTE-MIB has been replaced by the IPMROUTE-STD-MIB and the IGMP-MIB has been replaced by IGMP-STD-MIB. **Caveats** • Only the global SNMP trap receivers and email addresses are used at this time. Any domain specific SNMP trap receivers and email addresses will not be used. • Detection of SSG exceptions currently occurs across all domains. For example if the same Group is detected in two different domains with different Sources, an SSG exception will be generated. • Using the Enter key instead if clicking available buttons can cause unexpected behavior when saving traces. • Pressing STOP after starting discovery will not stop the discovery process. • ATM sub-interfaces may not be reported correctly on multicast forwarding trees.

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
CMM 2.1 rc4	You must be running Version 2.1 rc3 to install the 2.1 rc4 update. Be sure the polling daemon is not running while updating.		**IMPORTANT** This should be done before running the update.sh script. **Linux:** If upgrading you must add the following line to the end of the: <INSTALL-DIR>/httpd_perl/conf/httpd.conf file. Alias /db /usr/local/netman/mmtsys/db **On Solaris:** Alias /db /opt/RMSMMT/mmtsys/db • Adds support for multicast tree comparisons. • Fixes problem with discovery depth. • Fixes problem with screen refresh when switching domains. • Fixes problem with SNMP trap format. Also make sure the latest MIB is loaded.

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
CMM 2.1 rc3	You must be running Version 2.1 rc2 to install the 2.1 rc3 update.		• The polling daemon will now update the S,G cache when polling the RPs. • The polling daemon configuration is now separated by domain, i.e., each domain has its own polling configuration file. The global polling configuration file contains the polling times and intervals along with global trap receivers and email recipients. The global trap and email recipients will only be used if none are defined for the domain. Domain specific trap and email recipients are defined on the RP Polling Configuration screen. If upgrading, the polling daemon will have to be reconfigured since the polling daemon is not backward compatible with previous pollingconfiguration files. • Adds option to cache TACACS username/password. Once a username/password is entered to log into a router/switch, it will be cached in the browser, if Cache TACACS Info is checked on the System Configuration screen. • Adds import/export options for the IP Address database #import file format # this line will be skipped 239.1.1.1,test group 192.168.1.1,sourceA • IP Address database export will create /tmp/mmtIPdb.csv

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
CMM 2.1 rc2	You must be running Version 2.1 rc1 to install the 2.1 rc2 update.		• Fixes problem with trace when a router has the same PIM neighbor overmultiple VLANs. • Adds support for filtering of S,Gs. • Displays group descriptions. • Added option to import L2 switch file. The file should be in thefollowing format: # Layer 2 switch import file for CMM. callisto earth 172.16.1.7 # Blank lines or lines beginning with a '#' are skipped. # The file should only contain switches for the domain you're currently # working in.

Table 2   Additions and Problems in Cisco Route Manager, Release Number 2.3

Upgrade	Notes	Platform	Description
CMM 2.1 rc1	You must be running Version 2.0 rc6 or higher to install the 2.1 rc1 update.		• The polling daemon will have to be reconfigured for version 2.1 rc1. • Log files created by CMM should be rotated along with local system log files. The following log files are generated by CMM: \<INSTALLDIR\>/mmtsys/sys/events.log \<INSTALLDIR\>/mmtsys/sys/rmspolld.log \<INSTALLDIR\>/httpd_perl/logs/error_log **New Features** • Polling of L2 switch ports • Time-based thresholds • Detection of multiple sources • Reporting

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_inpck/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.