Release Notes for Cisco Media Gateway Manager, Release 2.0

May 2002

These release notes describe new features and caveats in system Software Release 2.0 for the Cisco Media Gateway Manager (MGM). Use these release notes in conjunction with the documentation listed in the "Related Documentation" section on page 11.

Contents

Introduction

Cisco MGM supports four of the five major OSI system management functional areas—fault, configuration, performance, and security. Cisco MGM also conforms to the Telecommunications Management Network model, operating as an Element Management System (EMS) at the element management layer.

Cisco Systems

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

78-12367-05

Cisco MGM features a graphical user interface (GUI) that displays network information and supports device management. This interface extends the capabilities of the Cisco Element Management Framework (Cisco EMF) to include the management of Cisco PXM1-based MGX 8000 Series Carrier Voice Gateways, as well as supported media gateway controllers (MGCs).

Cisco MGM includes links to two management tools, CiscoView and the Cisco MGX command line interface.

System Requirements

Cisco MGM and MGX 8000 Series hardware and software requirements are listed in the following sections.

Cisco MGM Platform Requirements

The platform requirements you need for Cisco MGM depends on the number of Cisco MGX 8000 Series gateways and associated MGCs that Cisco MGM will manage. Table 1 lists the server and client requirements for small and large Cisco MGM installations.

Table 1 Cisco MGM Platform Requirements

	Cisco MGM Server		
Resource	**Small Installation**	**Large Installation**	**Cisco MGM Client**
Workstation	Sun Netra t1400 or Sun Ultra 60	Sun Netra t1400	Sun Ultra 10
Operating system	Solaris 8	Solaris 8	Solaris 8
Memory	2 GB RAM	4 GB RAM	256 MB RAM
Disk space	Two hard disks, 18 GB or larger	Four hard disks, 18 GB or larger	One hard disk, 9 GB or larger
Processor	2 x 450 MHz	4 x 440MHz	440 MHz
Swap space	4 GB[1]	8 GB[1]	2 GB
Monitor	17-inch color	17-inch color	17-inch color
Graphics card	24-bit	24-bit	24-bit
Power supply	1	2 (second power supply optional for high availability installations)	1
Miscellaneous Resources	Local or remote CD ROM DAT tape backup	Local or remote CD ROM DAT tape backup	Local or remote CD ROM

1. If CiscoView is running on the same system as Cisco MGM, you will need an additional 1 GB swap space.

Cisco MGM Software Requirements

Cisco MGM 2.0 requires the following software components:

- Cisco EMF Release 3.2 Patch 1.4
- Netscape 4.76 for Solaris (included and automatically installed with Cisco EMF 3.2)
- CiscoView 5.4
- WANCV Release 3.60 (included with CMGM 2.0)

Note Solaris patch 108528-14 is required for critical performance improvement. Without installing this patch, Cisco MGM will function. However, installation of 108528-14 will improve Cisco MGM performance by approximately 70 percent.

Cisco MGX 8000 Series Software Requirements

Cisco MGM 2.0 manages Cisco MGX 8000 Series gateways based on the Cisco Processor Switch Module (PXM1). Cisco MGM 2.0 also provides management of VISM, VISM-PR, RPM-PR, SRM, and SRM-E cards. Table 2 shows the matrix of card software requirements for Cisco MGM 2.0.

Table 2 Cisco MGX 8000 Series Software Requirements for CMGM 2.0

PXM1 Release 1.1.40	VISM Release 2.2 RPM-PR Release 1.2.2
PXM1 Release 1.2.00	VISM Release 2.2 RPM-PR Release 1.2.2
PXM1 Release 1.2.10	VISM Release 3.0 VISM-PR Release 3.0 RPM-PR Release 1.2.2

CiscoView Requirements

You need in order to view and configure Cisco MGX 8000 Series Carrier Voice Gateways using Cisco MGM. Table 3 shows the Solaris 8 patches that must be installed in order for CiscoView to properly work.

Table 3 CiscoView Solaris 8 Patch Requirements

Patch	Description	Purpose
Required		
111626-01	X view	CW2k UNIX Clients
111327-02	socket library	
110945-02	syslog patch	CSCOmd
110934-01	pkgtrans, pkgadd, pkgchk and libpkg.a patch	All packages
110898-02	memory leak of csh scripts, cores when trying to echo env var > 1024 chars set in Bourne shell	
110700-01	kernel and /etc/mnttab do not contain reliable info on automounted file systems	
110670-01	RCP patch	Config modules and swim of RME
109742-04	/kernel/drv/icmp patch	kernel
109326-07	libresolv.so.2 and in.named patch	DNS queries being checked by CW2k

Table 3 CiscoView Solaris 8 Patch Requirements (continued)

Patch	Description	Purpose
109322-09	To avoid NIS+ fatal error and other problems in RPC API, say multiple system daemons loop in clnt_dg_call	RPC
109279-18	/kernel/drv/ip patch - Issues related ping, arp and ifconfig, etc	Kernel
108991-18	/usr/lib/libc.so.1 patch	ACE
108827-10	usr/lib/libthread.so.1 patch (To avoid Problem with Sybase Replication Server, non-static recursive mutexes, threaded process grows tired of receiving signals, etc	ACE
108652-35	Xserver related problems	X windows
108528-09	kernel update patch (other problems with kernel)	security
Recommended		
110951-02	/usr/sbin/tar and /usr/sbin/static/tar patch	Tar tool
110662-02	ksh patch (To avoid ksh shell bugs)	ksh
110615-01	sendmail patch	To send mail from cw2k
110286-04	OpenWindows 3.6.2: Tooltalk patch (To avoid problem with CDE, automount maps, and ttsession)	OpenWIndows
109324-02	sh/jsh/rsh/pfsh patch	
111085-02	buffer overflow in login(1) command	security

Media Gateway Controller Software Requirements

Cisco EMF and Cisco MGM provide integrated connection to the management interfaces of the following Media Gateway Controllers (MGCs):

- Cisco BTS 10200 Softswitch
- Tekelec VX*i* Media Gateway Controller (MGC)
- NexVerse ipVerse ControlSwitch

Table 4 shows the software requirements for each supported media gateway controller.

Table 4 Media Gateway Controller Software Requirements

Cisco BTS 10200	Release 3.1
Tekelec Vx*i*	Release 4.0
NexVerse ipVerse	Release 5.1

New Features

This section describes new features in Cisco Media Gateway Manager Release 2.0.

Cisco MGX 8000 Series Carrier Voice Gateway Support

Cisco MGM 2.0 adds the following features to support Cisco MGX 8000 Series network elements.

Auto Discovery

Cisco MGM automatically discovers Cisco MGX 8000 Series Carrier Voice Gateways and associated media gateway controllers. Cisco MGM displays the gateways and media gateway controllers on the MapViewer screen. From this display you can view operational status and navigate to screens that support configuration and software upgrades.

Cisco MGM Release 2.0 supports Cisco MGX 8230, MGX 8250, and MGX 8850 Carrier Voice Gateways.

Cisco MGM Release 2.0 adds support for the following media gateway controllers:

- Cisco BTS 10200 Softswitch
- Tekelec VX*i* Media Gateway Controller (MGC)
- NexVerse ipVerse ControlSwitch

Auto discovery occurs in two phases:

1. Automatic discovery of MGX 8000 Series gateways in a subnet
2. Subchassis synchronization of MGX 8000 Series subcomponents

Chassis State Configuration

Cisco MGM 2.0 reports Cisco MGX 8000 Series gateways as being in one of the following states:

- Error
- Normal
- Maintenance

The default is Normal (commissioned) state. However, in some circumstances, you may need to change the gateway to Maintenance (decommissioned) state.

Cisco MGM 2.0 adds a Chassis Maintenance dialog to the Cisco MGM MapViewer. You can use this dialog to commission or decommission MGX 8000 Series gateways.

CiscoView Integration

The Cisco MGM 2.0 interface enables you to launch CiscoView.

CiscoView is a graphical SNMP-based device management tool that provides powerful real-time views of your networked Cisco Systems devices. These views give you a continuously updated physical picture of device configuration and performance conditions, with simultaneous views available for multiple device sessions.

CiscoView also contains device-specific applications, such as Threshold Manager, StackMaker, and Flash File System, which further enhance your network management, monitoring, and troubleshooting capabilities.

Configuration Save and Restore

Cisco MGM 2.0 enables you to back up and restore MGX 8000 Series network card and chassis configurations. The configuration save function logs on to the selected device, invokes a **saveallcnf** command to generate the configuration file, and sends a **tftp get** command to transfer the device configuration file to your Cisco MGM workstation.The configuration restore function logs on to the selected devices, and sends a **tftp put** command to transfer the configuration file from your Cisco MGM workstation to the selected device.

Backup files are saved one level above your <CEMFROOT> directory with the following file naming convention:

<CEMFROOT>/../ConfigData/<IPADDRESS>_<BACKUPID>/<NODENAME>.ZIP

Note You can change the default directory by editing the CMGMVConfigSaveDir setting in <CEMFROOT>/config/init/cmgmCtlrUserData.ini.

Note The configuration restore action only transfers the configuration file from the Cisco MGM workstation to the selected device's hard disk. To restore the configuration back to the device from the configuration file, telnet to the device and run the CLI **restoreallcnf** command.

Network Card Configuration

Cisco MGM 2.0 adds support for auto discovery and configuration of the following Cisco MGX 8000 series network cards:

- PXM1 Processor Switch Model
- Voice Interworking Service Module (VISM and VISM-PR)
- Route Processor Module (RPM-PR)
- Service Redundancy Module (SRM and SRM-E)

Software Download

The software download feature facilitates downloading of runtime and backup boot image files to selected MGX 8000 Series gateways. Downloading software does not automatically activate it; the selected gateway continues to operate on current software until you perform the upgrade procedure. When you are downloading software images, Cisco MGM accepts a list of nodes and the fully qualified name of the image or configuration file. After download, the system reports successes and failures by node name.

SNMPv1 Community String Configuration

When Cisco MGM communicates with Cisco MGX 8000 Series Carrier Voice Gateways, security is enforced with SNMP community strings. SNMP communities group workstations and servers (or gateways) that can manage the Cisco MGX 8000 Series gateways according to each community's access privileges.

Cisco MGM uses the default community string (public) to read Cisco MGX 8000 Series information during the automatic discovery and subchassis synchronization processes. For Cisco MGM to configure the gateways, both Cisco MGM and the gateways must agree on a community string. Community string configuration is a multistep process, starting with each gateway and ending with the Cisco MGM that manages each gateway.

SNMP Trap Registration

Cisco MGM 2.0 includes a trap registration dialog window. You can use the trap registration window to configure SNMP traps to be forwarded from the Cisco MGX 8000 Series Carrier Voice Gateways to Cisco MGM for alarm management.

Subchassis Synchronization

Subchassis synchronization searches for entities within an Cisco MGX 8000 Series gateway and displays them on the Cisco MGM interface.

Subchassis discovery inspects SNMP MIBs for the following configurable objects:

- Chassis and Status
- Card Configuration and Status, including PXM1, VISM, VISM-PR, RPM-PR, SRM, and SRM-E cards and lines
- Line Configuration and Status, including DS1, DS3, and SONET.

Upon completion of subchassis discovery, Cisco MGM adds the subchassis components to the site hierarchy display.

The subchassis synchronization process is automatically invoked after auto discovery. Cisco MGM also runs periodic subchassis synchronizations, once every 24 hours. The time of day when this task runs depends on the last time the Cisco MGM controller was initialized.

You can also manually invoke the subchassis synchronization process from the Cisco MGM pull-down menu.

Telnet Sessions

With Cisco MGM 2.0, you can launch telnet sessions to Cisco MGX 8000 Series Carrier Voice Gateways from the Cisco MGM MapViewer. Telnet sessions enable you to enter CLI commands to the desired Cisco MGX 8000 Series gateways.

Media Gateway Controller (MGC) Support

Cisco EMF and Cisco MGM provide integrated connection to the management interfaces of the following Media Gateway Controllers (MGCs):

- Cisco BTS 10200 Softswitch
- Tekelec VX*i* Media Gateway Controller (MGC)
- NexVerse ipVerse ControlSwitch

Cisco MGM 2.0 provides the following support for these MGCs:

- Auto-discovery of MGCs from the Cisco MGM auto-discovery window.
- Ability to launch MGCs management systems from the Cisco MGM MapViewer window.
- Integration of MGC traps and alarms into the Cisco MGM Event Browser window.

Limitations and Restrictions

- Cisco MGM 2.0 supports only Solaris 8.
- Cisco MGM 2.0 GUI does not support the Open Windows environment.
- The CiscoView 5.4 server can run on a local or remote machine. If it is running on a remote machine, you must manually run the CiscoView security integration script and WanCV installation by executing the following commands from the Cisco MGM CD on the remote machine:

  ```
  /cdrom/cmgm2.0pkg/ciscoview/cvsecurity/cvsecurityinstall
  /cdrom/cmgm2.0pkg/ciscoview/wancv/wancvinstall
  ```

- Due to a known Cisco MGX 8000 series trap issue, Cisco MGM might display the SRM-E card as SRM.
- The cardInformation attribute in the Object Configuration Tool for the secondary active VISM may show the cardInformation of the primary VISM card being covered.
- Cisco MGX 8000 Series gateways do not send traps to Cisco MGM when you enter **clrallcnf** commands. The **clrallcnf** command erases the gateway configuration in Cisco MGM, but this does not show in the Map Viewer because no trap is sent. You must perform a manual chassis synchronization from Cisco MGM to reset the gateway configuration in the Map Viewer.
- The card switch over commands do not send all the necessary traps for Cisco MGM to update the card inventory in the Cisco MGM database. Map Viewer may not show the correct card and line inventory after these commands are executed. If you run a **softswitch** or **switchcc** command, perform a manual synchronization after this action. The 24-hour periodic resync task will eventually pick up the correct inventory for all the chassis managed by Cisco MGM as well.
- The system reset CLI command may cause the chassis to be out-of-reach from the network, which leads to loss of traps from the device to the Cisco MGM management server. Redundant card failover may not report all the necessary information in the alarm for Cisco MGM to recovery its configuration on the Map Viewer. If the operator executes a **resetsys** command on a chassis or if Cisco MGM receives traps indicating card failover, the Cisco MGM operator should perform a manual sub-chassis synchronization. The 24-hour periodic resync task will eventually pick up the correct inventory for all the chassis managed by Cisco MGM as well.

Installation Notes

- Cisco EMF must be installed and running before Cisco MGM can be installed.
- After Cisco EMF installation is complete, execute **cemf shell** to set up the run-time environment for Cisco EMF before executing **cemf start.**

- If CiscoView is to run on the same server with Cisco MGM, CiscoView must be installed and running before you install Cisco MGM.
- During installation, you may get the following CiscoView installation message that can be ignored:

```
Preparing to install CiscoView Security files...
ERROR: cmd failed. Server reason:
CiscoView Security installation completed successfully.
```

- Before installing the Cisco MGM client, check that the Cisco EMF server name and IP address are listed in the /etc/hosts file of your client system.
- Before installing the Tekelec package in CMGM, the Tekelec EMS Java Client Package must be installed first. For further information, refer to the *Cisco Media Gateway Manager User Guide.*
- Uninstalling Cisco MGM does not uninstall wancv and other CiscoView integration files.
- If you run the cmgmvinstall script from the CDE File Manager GUI, after installation is done and you select "q" to quit from the installation script, the window won't exit. You must use the File > Close menu to close the window.

For detailed Cisco MGM installation instructions, refer to the *Cisco Media Gateway Manager User Guide.*

Important Notes

- Do not interrupt the Cisco MGM installation or uninstallation with **Ctrl-C** or the **kill** command. After such an interruption, the system might not successfully install or uninstall Cisco MGM when you try to perform these actions again, or the system might enter an abnormal state.
- Do not interrupt the cemf backup operation using **Ctrl-C** or the **kill** command.
- In rare cases, installation fails with a pkgadd error. If this occurs, manually set the file permissions for the /tmp directory to rwx.
- Always run **cemf stop** to gracefully shut down Cisco EMF and Cisco MGM processes before rebooting the machine. If the machine is accidentally rebooted (or restarted due to a power failure), the Cisco MGM database integrity can be damaged, and you might need to run **cemf reset** and rediscover the network to restore normal operation. Running low on swap space leads to the same problem. Make sure that a minimum of 2 GB of swap space is allocated on the server machine.
- If the **cemf stop** operation hangs while suspending the participant service, wait for at least 1 hour for the **cemf stop** command to complete. If the **cemf stop** command continues to hang, enter the **/opt/cemf/bin/sysmgrClient -q** command to stop Cisco EMF core processes, and then run **cemf stop** and **cemf reset** to reset the database.
- If the following error messages appear when you are running **cemf session**, run **cemf stop** and **cemf start** to restart the Cisco EMF and Cisco MGM processes.

```
ERROR: "/opt/cemf/config/scripts/session" command failed.
ERROR: Cannot connect to Session
```

- Do not use the Deployment menu on the Cisco MGM GUI to delete site objects. Doing so might cause the MapViewer window to stop working correctly. If this occurs, close the MapViewer window and reopen it from the Cisco EMF LaunchPad. Always delete chassis one at a time.
- Before launching CiscoView from a Cisco MGM session, make sure that you do not have any Netscape process already running. ((If a Netscape process is running before you launch CiscoView for the first time in your Cisco MGM session, Netscape will incorrectly prompt you to install the java plug-in every time CiscoView is launched.)

- The object indicator color on the Cisco MGM GUI represents the highest severity of alarm on the object, but not necessarily the status of the resource on the chassis. To find out the status of the resource that the object represents, use the Object Configuration window.
- The alarm indicator next to the object name on the left side of the Cisco MGM GUI sometimes does not show the correct color of the highest outstanding alarm. If this occurs, close the MapViewer window and open a new one. For information about Cisco MGM alarm colors, refer to the *Cisco MGM User Guide*, Chapter 6, "Fault and Performance Management".
- If you want to use the updCmgmTrapForward script to configure trap forwarding, you must install Cisco EMF 3.2 Patch 2. There is a problem in the Cisco EMF trapManager supporting the wild card format in the trap forwarding configuration file, and the wild card trap forwarding entry will cause the trapManager process to core dump and no alarms will be reported in the Cisco EMF Event Browser.

Caveats

Table 5 describes the known problems in Cisco MGM 2.0.

Table 5 Cisco MGM Release 2.0 Caveats

Identifier	Title	Description	Workaround
CSCdu04192	Card disappears from map viewer when it is reset using WebViewer	When resetting a card to test notification, the card disappears from map viewer and is removed from all object groups. Upon reboot, the object reappears on the map, but it is no longer a member of the object group and is no longer monitored by the thresholding regime.	After the card object is re-created, use the Object Group Editor of Cisco EMF to add the card object back to the object group.
CSCdx60375	Too many traps may cause problem with buffer	When many traps are received by Cisco MGM, it may cause its internal trap cache to get out of synch with the database inventory, and may not handle creation traps correctly.	Run <CEMFROOT>/bin/sysmgrClient -k cmgmvCtlr and then <CEMFROOT>/bin/sysmgrClient -x cmgmvCtlr to restart the Cisco MGM controller to refresh the trap cache.
CSCdx65344	SRM switchover not captured by Map Viewer correctly	When you perform a CLI **switchcc** command on the PXM1 card, the SRM also switches over. Although the traps for the SRM remove and add are received, the Map Viewer does not display the standby SRM card.	Run the subchassis sync up command on the chassis to synchronize the chassis inventory and recover the standby SRM card on the Map Viewer.

Table 5 Cisco MGM Release 2.0 Caveats (continued)

Identifier	Title	Description	Workaround
CSCuk33887	CMGM 2.0 must clarify how to change CMGM_Default_Site name	The Cisco MGM 2.0 User Guide does not describe any procedure to change the name of the Default_CMGM_Site. For customers who want to split the network into subnetworks, the guide should document how to do this.	The Cisco MGM 2.0 User Guide has described how to configure the sysLocation value of a chassis to put the chassis under different site container. An enhancement will be added in CMGM 3.0 to provide a dialog to facilitate the sysLocation configuration.
CSCdx61118	3 Tekelec traps do not show full trap description	The following three Tekelec traps do not display full trap descriptions in the Cisco EMF Event Browser: mgcHotStandbyUnavailiable mgcPrilnvalidQ931Message mgcPriQ931TimerExpired	A Cisco MGM patch is required to fix this issue.

Related Documentation

The following Cisco publications contain additional information related to the operation of Cisco MGM:

- *Cisco Media Gateway Manager User Guide*
- *Cisco Element Management Framework Installation and Administration Guide*
- *Overview for CiscoView*
- *CiscoView Getting Started Guide*
- *Cisco MGX 8230 Command Line Interface Guide*
- *Cisco MGX 8250 Command Line Interface Guide*
- *Cisco MGX 8850 Command Line Interface Guide*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.