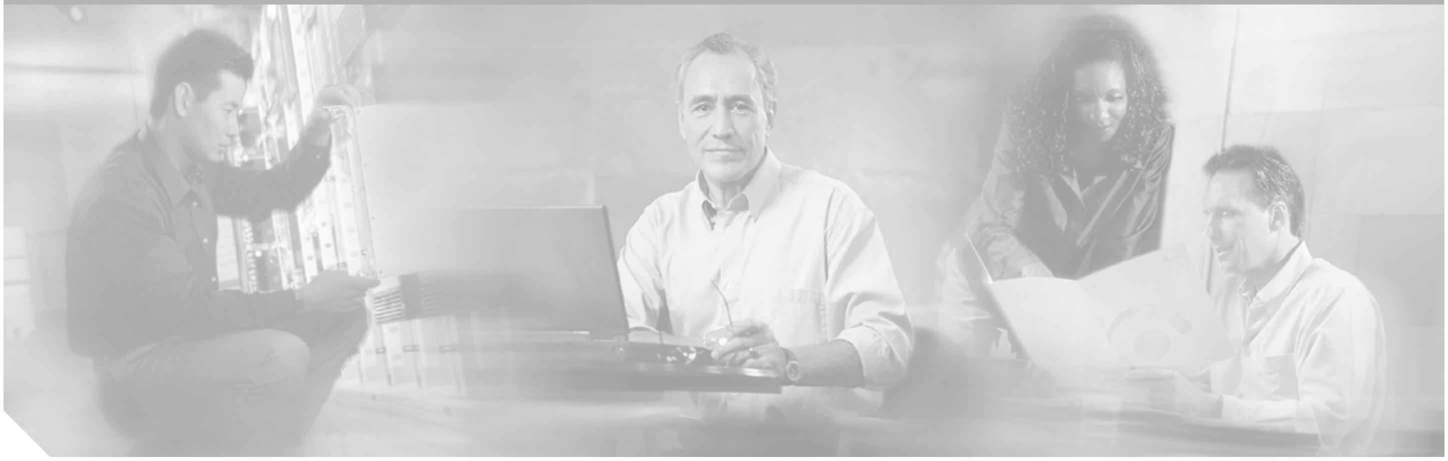


Cisco Media Gateway Manager User Guide

Software Release 3.0

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-3543-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco Media Gateway Manager User Guide

CONTENTS

About This Guide

This guide provides Cisco Media Gateway Manager (Cisco MGM) users with the detailed information they need to configure, manage, and troubleshoot Cisco MGX 8000 Series Carrier Voice Gateway (CVG) networks that employ Cisco's MGX PXM1, PXM1-E, and PXM45 Processor Switch Modules and/or Voice Interworking Service Module (VISM/VISM-PR).

Audience

This guide is meant to be used by network operators and administrators who have experience in telecommunications networks, protocols, and equipment and who are familiar with data communications networks, protocols, and equipment.

Organization

This guide contains instructions for installing the Cisco MGM software and configuring Cisco MGX 8000 Series CVGs.

This guide contains the following chapters:

- Chapter 1, "Overview," provides an overview of the applications and features.
- Chapter 2, "Installation," describes how to install and test the system.
- Chapter 3, "User Interfaces," orients the user to the graphical interfaces.
- Chapter 4, "Configuration," provides procedures for using the automatic discovery and subchassis synchronization for Cisco media gateways.
- Chapter 6, "Fault and Performance Management," provides procedures for monitoring alarms and performance.
- Chapter 7, "Security," introduces Cisco EMF and Cisco MGM user accounts, as well as SNMP community strings.
- Chapter 8, "Media Gateway Controller Integration,"describes how Cisco MGM manages media gateway controllers in the overall Cisco EMF system.
- Chapter 9, "Cisco EMF Coresidency" describes the coresident EMs compatible with Cisco MGM.

Conventions

Warning **Means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.**

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not covered in this manual.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information.

Related Documentation

Related Cisco documentation includes:

- Cisco EMF
  - *Quick Start Guide Cisco EMF Version 3.2 SP4*
    Cisco Element Manager November 2002 Upgrade
  - *Cisco Element Management Framework Installation and Administration Guide Version 3.2 Service Pack 4 (Cisco Element Manager November 2002 Upgrade)*
  - *Cisco Element Management Framework User Guide Version 3.2 Service Pack 4 (Cisco Element Manager November 2002 Upgrade)*
  - *Release Notes for Cisco Element Management Framework v3.2 Service Pack 4*
    Cisco Element Manager November 2002 Upgrade
- Cisco MGM:
  - *Release Notes for Cisco Media Gateway Manager, Release 3.0*
  - *Cisco Media Gateway Manager User Guide, Release 3.0*
- Cisco BTS:
  - *Release Notes for the Cisco BTS 10200, Release 3.3*
  - *Cisco BTS 10200 System Description*
  - *Cisco BTS 10200 Command Line Interface Reference Guide*
  - *Cisco BTS 10200 Application Installation Procedures*
  - *Cisco BTS 10200 Softswitch CORBA Installation and Programmer's Guides*
  - *Cisco BTS 10200 Cabling Procedures*

- CiscoView:
  - *Release Notes for CiscoView 5.4*
  - *Installation and Setup Guide for CiscoView 5.4*
  - *Using CiscoView 5.4*
  - *WAN CiscoView Release 3 for the MGX 8230 Edge Concentrator, Release 1*
  - *WAN CiscoView Release 3 for the MGX 8250 Edge Concentrator, Release 1*
  - *WAN CiscoView Release 3 for the MGX 8850 Edge Switch, Release 1*
  - *WAN CiscoView Release 2 of the MGX 8850*
- Cisco MGX 8000 Series CVGs:
  - *Cisco MGX 8850 and MGX 8950 Switch Software Configuration Guide*
  - *Cisco MGX 8850 (PXM1E) and MGX 8830 Switch Software Configuration Guide*
  - *Cisco MGX 8850 (PXM45) and MGX 8950 Switch Software Configuration Guide*
  - *Cisco MGX 8230 Multiservice Gateway Command Reference*
  - *Cisco MGX 8250 Multiservice Gateway Command Reference*
  - *Cisco MGX 8830, MGX 8850 (PXM45 and PXM1E), and MGX 8950 Command Reference*

For information concerning non-Cisco MGC documentation, refer to the company web sites.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped 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.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

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 Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) 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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

You can submit your comments by mail by using the response card 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.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Web Site

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

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

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

CHAPTER 1

Overview

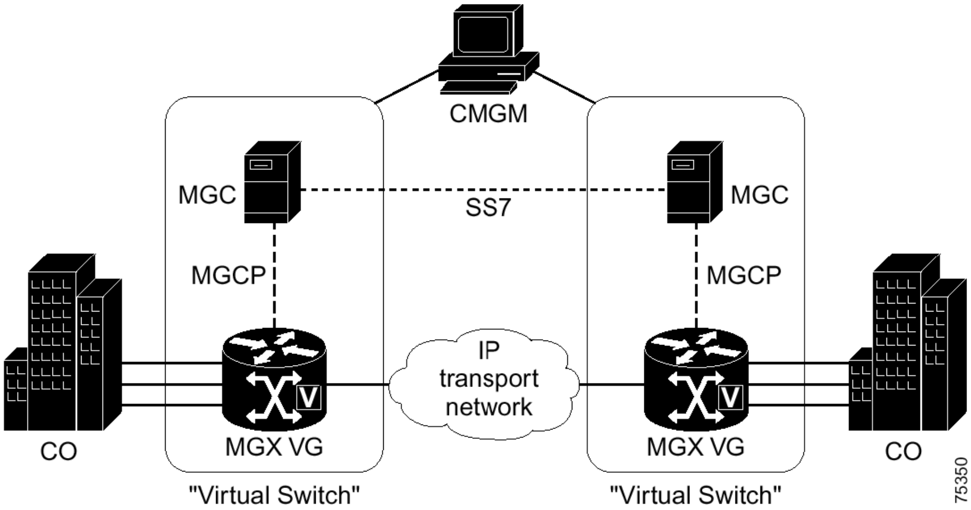
Cisco MGM operates as a component of the Cisco Element Management Framework (Cisco EMF) software. Cisco MGM enables you to deploy, configure, and manage Cisco MGX 8000 Series CVGs that utilize the Cisco PXM1, PXM1-E, and PXM45 Processor Switch Modules.

Cisco MGM provides a graphical user interface (GUI) for the display of network information and device management, including access to media gateway controllers (MGCs) functioning in the network.

Cisco MGM Architecture

Cisco MGM extends the functionality of Cisco EMF to include management of Cisco MGX 8000 Series CVGs, as well as supported media gateway controllers (MGCs). Figure 1-1 provides a simple view of Cisco MGM's location in a voice gateway network.

Figure 1-1 Cisco MGM Architecture



User Interfaces

Cisco MGM provides a graphical user interface (GUI) using UNIX Motif. For device-specific configuration, Cisco MGM also provides access to the CiscoView GUI, as well as to command line interface functions through telnet sessions.

For detailed information on CiscoView installation and operation, refer to *Using CiscoView 5.4*.

For command line interface functions, refer to the following documents:

- *Cisco MGX 8230 Multiservice Gateway Command Reference*
- *Cisco MGX 8250 Multiservice Gateway Command Reference*
- *Cisco MGX 8830, MGX 8850 (PXM45 and PXM1E), and MGX 8950 Command Reference*

Supported Protocols

Cisco MGM supports the following protocols as part of its overall management capabilities:

- CEMF Event Channel
- HTTP
- Telnet
- FTP
- TFTP
- SNMPv1
- SNMPv2c
- CORBA

Features

Cisco MGM provides a powerful range of network management capabilities, including support for network configuration, administration, fault and performance management, and security.

Configuration

Cisco MGM configuration capabilities include the following features:

- Auto discovery and topology views of Cisco MGX 8000 Series CVGs
- Auto discovery of media gateway controllers (MGCs)
- Provisioning and queries of Cisco MGX 8000 Series service modules, lines, and ports. (This function is accessed through CiscoView.)
- Maintenance state support
- Software image downloads
- Configuration save and restore
- Menu-launched telnet sessions for CLI device management

Administration

Cisco MGM administration capabilities provide database support for Cisco MGX 8000 Series components, including:

- Chassis
- PXM1, PXM1-E, and PXM45 cards and lines
- Voice Interworking Service Module (VISM/VISM-PR) cards and lines
- Route Processor Module (RPM-PR and RPM-XF) cards and RPM-XF Ethernet lines
- Service Redundancy Module (SRM and SRM-E) cards and lines
- ATM Switch Service Module (AXSM and AXSM-E) cards and lines

Cisco MGM performs asynchronous database updates in response to network equipment configuration and status changes.

Fault Management

Cisco MGM provides consolidated alarm viewing and filtering through the use of the Cisco EMF event browser interface. Cisco MGM displays alarms and events on a color-coded topology map. Fault management functions include:

- Alarm monitoring
- Alarm filtering
- Assignment/Deletion
- Acknowledgement
- Alarm based performance threshold alerts
- Trap registration and forwarding of traps to remote SNMP managers

Performance Management

Cisco MGM performance management capabilities include threshold and call related statistics using CiscoView and the appropriate MGC element management systems.

CiscoView provides device-specific performance management, including the following information:

- LAPD Statistics
- Session Set Counters
- Session Group Counters
- RUDP Statistics and Counters
- SVC Statistics Counters
- Bearer Statistical Counters
- HDLC Counters
- DSX1 Line Real Time Counters

All statistics data are collected in real-time, no history is stored.

Security

Cisco MGM security uses the mechanisms of Cisco EMF, which authenticates users based on names and passwords. When using CLI management interfaces, the Cisco MGX 8000 Series CVGs also authenticate users based on user accounts. Security profiles define access rights for typical users, from administrators to guests.

SNMP community strings allow access between Cisco MGM and network elements messages to be controlled. Unique community strings known by all network elements should be configured.

Cisco Info Center Support

Cisco EMF provides an interface to the Cisco Info Center (CIC) through use of the Cisco EMF event channel. The Cisco Info Center is purchased as a separate product from Cisco MGM.

CIC provides service-level alarm monitoring and diagnostics tools for network fault and performance monitoring, network trouble isolation, and real-time service-level management for large networks. CIC helps operators focus on important network events, offering a combination of alarm processing rules, filtering, customizable alarm viewing, and partitioning. CIC provides a highly configurable client/server application that can consolidate, duplicate, filter, and correlate fault information from multiple network layers.

CIC is the fault management component of the Cisco Service Management (CSM) infrastructure that provides end-to-end service management solutions for service provider and large enterprise networks. Operating at the service and network levels, CIC interacts with other management tools within the CSM product suite to provide customer-focused, service-level monitoring and network partitioning for Virtual Private Network and Customer Network Management services. CIC works in conjunction with network element management software such as Wide Area Network Manager to provide fault and alarm management across local and wide area networks.

Installation

Cisco MGM is based on Cisco's Element Management Framework (Cisco EMF) software, which operates in a distributed environment using a server and clients. This chapter describes the deployment options, software components, hardware requirements, and installation procedures for Cisco MGM, and identifies the Cisco EMF options that are important when you are installing Cisco MGM.

Deployment Options

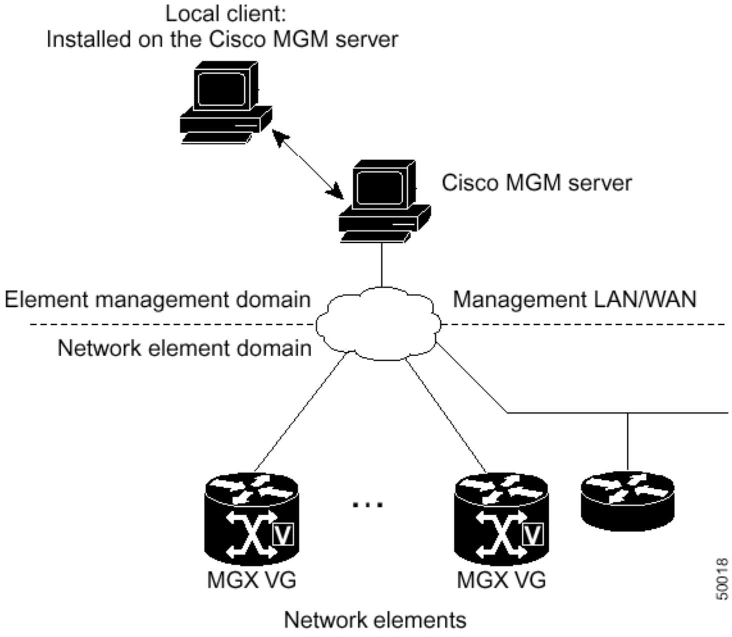
The following types of deployment are available:

- Server with local client. (See Figure 2-1.) A client can be local or remote. A local client is one that is running on the server itself.
- Server with local and remote clients. (See Figure 2-2.) A remote client is running on a Sun workstation separate from the server.

Server with Local Client

Every deployment includes Cisco EMF server and Cisco MGM extensions. Processes on the server keep track of the current state of the network, user access, and events. The Cisco EMF clients provide the user interface to the system. When you install a Cisco EMF server, you automatically add a local client. (See Figure 2-1.)

Figure 2-1 Server With Local Client

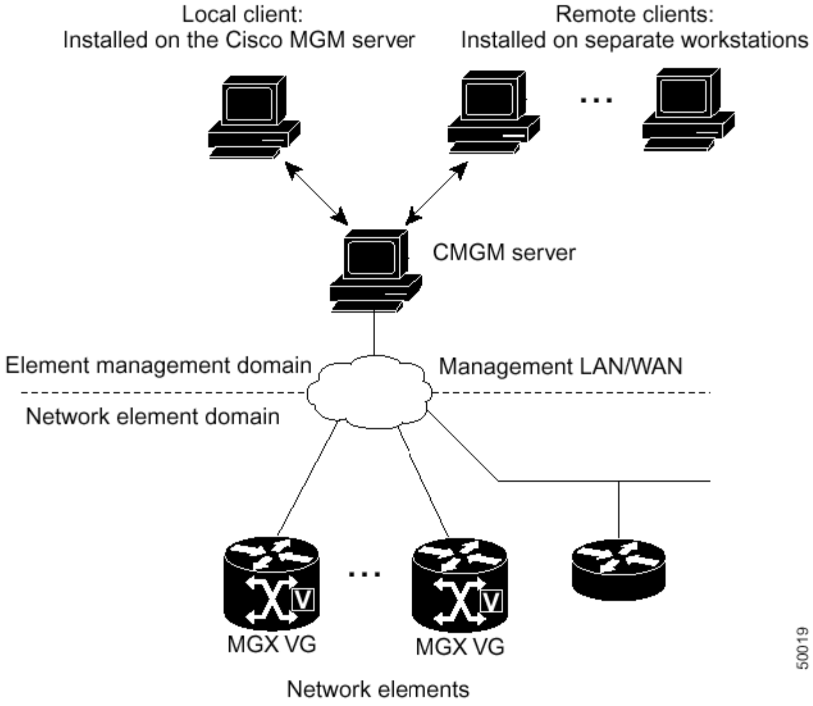


Note You can also log on to the server from a PC running X-window emulation software, such as ReflectionX or Exceed.

Server with Remote Clients

A Cisco EMF deployment can have additional clients installed on separate workstations. (See Figure 2-2.) A client installation retrieves management information from the Cisco EMF server and displays it on the user interface. Using clients that run on separate hosts frees system resources on the server and improves overall performance. You can install client software from a local CD ROM drive; you do not need to mount files across a network.

Figure 2-2 Server with Local and Remote Clients



System Requirements

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

Cisco MGM Hardware Requirements

The hardware resources you need for Cisco MGM depend on the number of Cisco MGX 8000 Series CVGs and associated MGCs that Cisco MGM will manage. Table 2-1 lists the server and client requirements for small and large Cisco MGM installations.

Table 2-1 Cisco MGM Platform Requirements

Resource	Cisco MGM Server Small Installation[1]	 Large Installation[2]	Cisco MGM Client
Workstation	Sun Netra t1400[3]	Sun Netra t1400[3]	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, each one 18 GB or larger	Four hard disks, each one 18 GB or larger	One hard disk, 9 GB or larger
Processor	2 x 440 MHz	4 x 440MHz	440 MHz
Swap space	5 GB[4]	9 GB[4]	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] Up to 10 fully-loaded MGX CVGs

[2] Between 10 to 50 fully-loaded MGX CVGs

[3] Netra platforms are supported, but not required. Alternate platforms that have been tested include: Sun Ultra 60, 220r, 420r, 280r, and Netra 20. Sun UltraSPARC III servers and desktops are also supported by Cisco MGM.

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

Cisco MGM Supported Hardware

Cisco MGM manages Cisco MGX 8000 Series CVGs based on the Cisco processor switch modules (PXM1, PXM1-E, and PXM45). In addition, Cisco MGM provides management of VISM, VISM-PR, RPM-PR, RPM-XF, SRM, SRM-E, AXSM, and AXSM-E cards. The following table lists the processor switch and services modules supported by chassis.

Table 2-2 Cisco MGM Supported Hardware

Modules	Chassis MGX 8230	 MGX 8250	 MGX 8830	 MGX 8850
PXM1	Yes	Yes	N/A	Yes
PXM1-E	N/A	N/A	Yes	Yes
PXM45	N/A	N/A	N/A	Yes
VISM	Yes	Yes	N/A	Yes
VISM-PR	Yes	Yes	Yes	Yes
RPM-PR	Yes	Yes	Yes	Yes
RPM-XF	N/A	N/A	N/A	Yes
SRM/SRM-E	Yes	Yes	Yes	Yes
AXSM/AXSM-E	N/A	N/A	N/A	Yes

In the preceding table, “yes” indicates that the module listed in the left–hand column is supported by the chassis type displayed at the top of the column. An entry of “N/A” indicates that the module listed in the left–hand column is not supported by the chassis type displayed at the top of the column.

For information on card–to–card compatibility, see the appropriate Cisco MGX software release notes.

Cisco MGM Software Requirements

This version of Cisco MGM requires the following software components:

- Cisco EMF Release 3.2 Service Pack 4 or greater
- CiscoView 5.4
- MGX 8230, 8250, 8830, and 8850 package release 4.11 (included with Cisco MGM 3.0 package)

Note To ensure optimal system performance and the inclusion of critical security updates, it is recommended that you install the latest Solaris patches available.

Cisco MGX 8000 Series Software Requirements

The Cisco processor switch and service modules require the installation of specific firmware releases in order to function properly in Cisco MGX 8000 series chassis running Cisco MGM. Depending on the Cisco processor switch module present in the chassis, different service modules may be supported. For each processor module and service module within a particular chassis, the firmware release may vary.

The following table lists Cisco MGM and Cisco MGX 8000 Series CVG compatibility, including the supported firmware release. Other firmware versions may be used; however, some functionality may not be compatible with other firmware releases.

Table 2-3 Cisco MGM and Cisco MGX 8000 Series CVG Compliance Matrix

	Module		
Chassis	**Processor Module**	**Service Module**	**Supported Firmware Release**[1]
MGX 8230 MGX 8250 MGX 8850	PXM1	N/A	MGX 1.2.10
		VISM/VISM-PR	VISM 3.1
		RPM-PR	RPM 1.2.13
		SRM/SRM-E	N/A
MGX 8830 MGX 8850	PXM1-E	N/A	MGX 3.0.20
		VISM-PR	VISM 3.1
		RPM-PR	RPM 1.2.13
		SRM/SRM-E	N/A
MGX 8850	PXM45	N/A	MGX 3.0.20
		VISM-PR	VISM 3.1
		RPM-PR/RPM-XF	RPM 1.2.13
		SRM/SRM-E	N/A
		AXSM/AXSM-E	AXSM 3.0.20

[1] For other Cisco MGX firmware versions, see the corresponding Cisco MGX software release notes to determine the appropriate firmware version supported for the specific service module(s).

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 2-4 shows the software requirements for each supported media gateway controller.

Table 2-4 Media Gateway Controller Software Requirements

Cisco BTS 10200	Release 3.3
Tekelec Vxi	Release 4.0
NexVerse ipVerse	Release 5.1

Configuring /etc/hosts Files

Before installing the Cisco MGM client software, the /etc/hosts file of the server and client machines must be modified.

Configuring the Server /etc/hosts File

Modify the server /etc/hosts file by adding the IP address and name of the client machine. Following is an example of the server hosts file before and after the modification:

Before:

```
# more /etc/hosts
#
# Internet host table
#
127.0.0.1       localhost
172.29.51.179   cmgm-server     loghost
```

After:

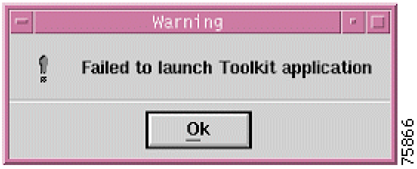
```
# more /etc/hosts
#
# Internet host table
#
127.0.0.1       localhost
172.29.51.179   cmgm-server     loghost
172.29.51.164   cmgm-client
```

Note If the Cisco MGM server does not have DNS or NIS service, you need to also add the following line to your server /etc/hosts file to access the Cisco MGM online user guide:

```
198.133.219.25    www.cisco.com   www.cisco.com
```

If you do not update the server etc/hosts file, the warning dialog box and error message shown in Figure 2-3 will appear when you attempt to login to Cisco MGM from the client machine:

Figure 2-3 Cisco MGM Login Warning Dialog



Failed to launch Toolkit application

After you modify the /etc/hosts file, enter the following commands to restart the Cisco MGM server:

```
cd /opt/cemf/bin
./cemf shell
./cemf stop
./cemf start
```

Note Wait until Cisco EMF stops before executing the cemf start command.

Configuring the Client /etc/hosts File

Modify the client /etc/hosts file by adding the IP address and name of the server machine. Following is an example of the client hosts file before and after the modification:

Before:

```
CEMF Client> more /etc/hosts
#
# Internet host table
#
127.0.0.1       localhost
172.29.51.164   cmgm-client     loghost
```

After:

```
CEMF Client> more /etc/hosts
#
# Internet host table
#
127.0.0.1       localhost
172.29.51.164   cmgm-client     loghost
172.29.51.179   cmgm-server
```

Installing CiscoView Applications

The Cisco MGM server software requires the integration of the CiscoView security package and installation of the WanCV package on the CiscoView server. The CiscoView security integration implements functionality on the CiscoView server so that you will not be required to log into the CiscoView server each time you launch the CiscoView application from the Cisco MGM EM. Essentially, the CiscoView server authenticates the CiscoView launch per the Cisco MGM login. The WanCV installation adds four device packages to the CiscoView server, specifically in support of MGX 8230, MGX 8250, MGX 8830, and MGX 8850.

If the CiscoView server is on the local machine, the CiscoView security and WanCV installation will be automatically performed by the Cisco MGM server installation. If the CiscoView server is on the remote machine, you must manually install the CV security and WanCV applications.

To manually install the CV security integration and WanCV applications on a remote CiscoView server, follow these steps:

Step 1 Log into the remote CiscoView server as the root user.

Step 2 Ensure that CiscoView 5.4 is installed and running on the remote machine. For information about installing CiscoView, refer to the CiscoView product documentation located in the documentation directory of the CiscoView CD ROM.

Step 3 Enter the following commands in a terminal window on the remote machine:

```
/cdrom/cmgm3.0pkg/ciscoview/cvsecurity/cvsecurityinstall
/cdrom/cmgm3.0pkg/ciscoview/wancv/wancvinstall
```

Installing the Cisco MGM Server

Installing the Cisco MGM server software requires the following procedures:

1. Installing the Cisco EMF server software
2. Configuring raw partitions
3. Backing up the Cisco EMF database
4. Installing the Cisco MGM server software

Note Before beginning the installation process, refer to the "Important Notes" section of *Release Notes for Cisco Media Gateway Manager, Release 3.0*.

Installing Cisco EMF Server Software

Install the Cisco EMF server software according to the procedures described in the *Cisco Element Management Framework Installation and Administration Guide*.

Configuring Raw Partitions

In the RAW File System (RAWFS), databases can be placed in a raw partition. If you have a large deployment, the databases should be placed in a raw partition. This improves Cisco EMF performance and allows databases to grow larger than 2 GB.

For more detailed information about configuring raw partitions for the Cisco EMF database, refer to the *Cisco Element Management Framework Installation and Administration Guide*.

Backing up the Cisco EMF Database

Cisco EMF backup and restore functions allow you to recover from hardware or software failures with minimal loss of management data. You can also use the backup and restore functions to move databases from one Cisco EMF installation to another, for example, to facilitate hardware upgrades.

Cisco EMF backups should be performed under the following circumstances:

- Before upgrading Cisco EMF
- Before installing or uninstalling a new element manager, such as Cisco MGM
- Before installing an upgrade or patch for installed Cisco EMF element manager packages
- Before making major changes to the network data model (such as deletion or untested changes)
- Before making major changes to the network hardware
- Before deploying a large number of new network devices
- On a daily basis

For detailed Cisco EMF backup and restore instructions, refer to *Cisco Element Management Framework Installation and Administration Guide*.

Installing Cisco MGM Server Software

The following procedure details how to install Cisco MGM server software. If this software already exists on the workstation, you may upgrade to a new release. For further information on upgrading Cisco MGM server software, see the "Upgrading the Cisco MGM Server" section on page 2-13.

To install the Cisco MGM server, follow these steps:

Step 1 Log in to the Cisco EMF server as the root user.

Step 2 Ensure that CiscoView 5.4 is installed and running on either the local or remote machine. For information about installing CiscoView, refer to the CiscoView product documentation located in the documentation directory of the CiscoView CD ROM.

Step 3 If the CiscoView server is on a remote machine, ensure that the CiscoView security integration and WANCV installation has taken place. For instructions on performing the security and Wan CV installations, see the "Installing CiscoView Applications" section on page 2-8.

Tip To ensure that the WANCV packages have been installed, click **About** on the CiscoView main window. Verify that the package names appear in the Installed Device Packages list at the bottom of the window.

If the CiscoView server is on the local machine, the security and WanCV installation will be automatically performed by the Cisco MGM installation. Proceed to Step 4.

Step 4 Navigate to the appropriate directory on the CD ROM by entering:

```
cd /cdrom/cmgm3.0pkg/cmgmv
```

Step 5 Start the installation script.

```
./cmgmvinstall
```

Tip To get help, enter **cmgmvinstall -h**

Note 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.
```

Step 6 Follow the onscreen instructions. When prompted for the type of installation, select the **cmgmvpkg Server Package** option.

A prompt displays requesting how you want to provide the host on which CiscoView and the required CiscoView applications are installed, by hostname or IP address.

Step 7 Enter the corresponding CiscoView host option at the prompt.

A prompt displays according to the entry provided in Step 7, hostname or IP address.

Step 8 Enter the appropriate CiscoView server hostname or IP address accordingly.

Text displays indicating that the CiscoView Security and WanCV device packages are required by manual installation and lists the basic steps for installing. For additional information, see the "Installing CiscoView Applications" section on page 2-8.

The script continues with the Cisco MGM server package installation. Text displays recommending that you backup the Cisco EMF database before continuing. Should you initiate a backup at this time, all sessions connected to the server will stop. For additional information, see the "Backing Up the Cisco EMF Database" section on page 2-13.

The script checks to see if the Cisco MGM server package has been previously installed. If it determines that the package already exists, installation occurs as the "Upgrading the Cisco MGM Server" section on page 2-13 describes. You are prompted to confirm the installation option displayed.

Step 9 Enter y to proceed with the installation or n to quit the installation accordingly.

If you entered n, the installation of the software aborts. If you entered y, the installation of the software continues and data displays indicating the resulting activities.

Upon completion of the package installation, you may check the installation log for errors. The log file is in the following location:

```
/var/adm/Atlantech/avinstall/Cisco_Element_Management_Framework_-_Server/logfile
```

You may verify that the cmgmCtlr process is running. For example:

```
/opt/cemf/bin/cemf status
```

Installing Cisco MGM Clients

The Cisco EMF clients provide the user interface to the system. When you install a Cisco EMF Server, you automatically add a local client. (See Figure 2-1).

Installing the Cisco MGM clients requires the following procedures:

1. Installing the Cisco EMF client
2. Installing the Cisco MGM client

Note Before beginning the installation process, refer to the Important Notes section of *Release Notes for Cisco Media Gateway Manager, Release 3.0.*

Note For additional information about installing MGC EMS packages, refer to Chapter 8, "Media Gateway Controller Integration".

Installing Cisco EMF Client Software

Install the Cisco EMF client software according to the procedures described in the *Cisco Element Management Framework Installation and Administration Guide*.

Installing Cisco MGM Client Software

The following procedure details how to install the Cisco MGM client software. If Cisco MGM client software already exists on the client workstation, you may upgrade to a more recent release without uninstalling the existing software. For further information on upgrading Cisco MGM client software, see the "Upgrading a Cisco MGM Client" section on page 2-16.

To install Cisco MGM client software, follow these steps:

Step 1 Log in to the Cisco EMF client as the root user.

Step 2 Navigate to the appropriate directory on the CD ROM by entering:

```
cd /cdrom/cmgm3.0pkg/cmgmv
```

Step 3 Start the installation script.

```
./cmgmvinstall
```

Tip To get help, enter **cmgmvinstall -h**

Step 4 Follow the onscreen instructions. When prompted for the type of installation, select the **cmgmvpkg Client Package** option.

A prompt displays requesting how you want to provide the host on which CiscoView and the required CiscoView applications are installed, by hostname or IP address.

Step 5 Enter the corresponding CiscoView host option at the prompt.

A prompt displays according to the entry provided in Step 7, hostname or IP address.

Step 6 Enter the appropriate CiscoView server hostname or IP address accordingly.

Text displays indicating that the CiscoView Security and WanCV device packages are required by manual installation and lists the basic steps for installing. For additional information, see the "Installing CiscoView Applications" section on page 2-8.

The script continues with the Cisco MGM client package installation.

The script checks to see if the Cisco MGM client package has been previously installed. If it determines that the package already exists, installation occurs as the "Upgrading the Cisco MGM Server" section on page 2-13 describes. You are prompted to confirm the installation option displayed.

Step 7 Enter y to proceed with the installation or n to quit the installation accordingly.

If you entered n, the installation of the software aborts. If you entered y, the installation of the software continues and data displays indicating the resulting activities.

Upon completion of the package installation, you may check the installation log for errors. The log file is in the following location:

```
/var/adm/Atlantech/avinstall/Cisco_Element_Management_Framework_-_Server/logfile
```

You may verify that the cmgmCtlr process is running. For example:

```
/opt/cemf/bin/cemf status
```

Installing MGC EMS Packages

For information about media gateway controllers (MGCs) supported in Cisco MGM, refer to Chapter 8, "Media Gateway Controller Integration."

Upgrading Cisco MGM

Cisco MGM servers and clients may be upgraded as necessary.

Upgrading the Cisco MGM Server

When upgrading the Cisco MGM server, the Cisco EMF server must be upgraded as well. By upgrading previously installed versions of the Cisco EMF and Cisco MGM server software packages, you are able to retain existing network data through the use of the Cisco EMF backup and restore feature.

Upgrading the Cisco MGM server involves the following:

1. Backing Up the Cisco EMF Database
2. Saving Backup MGX Configuration Files
3. Upgrading the Cisco EMF Server Software
4. Upgrading Cisco MGM Server Software
5. Restoring the Cisco EMF Database
6. Restoring Cisco MGM Configuration Files
7. Synchronizing Managed Devices

The following sections provide information on the performing the tasks in the preceding list.

Backing Up the Cisco EMF Database

Cisco EMF offers configuration backup capabilities through the Resource Manager Essentials (RME) application. Using the RME application you can archive the network database as necessary. For overview information on the RME tool and instructions specific to using RME with Cisco EMF, see the *Cisco Element Management Framework Installation and Administration Guide* and the *Cisco Element Management Framework User Guide*. For detailed information on the RME tool, see the *User Guide for Resource Manager Essentials*.

Saving Backup MGX Configuration Files

You can back up network card and chassis configurations using the Cisco MGM configuration save feature. The Cisco MGM 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. For further information, see the "Configuration Save" section on page 4-9.

Upgrading the Cisco EMF Server Software

In order to upgrade the Cisco MGM server software, you must ensure that the Cisco EMF server software is upgraded to the required level and that the appropriate service pack is being used. For the current Cisco EMF software requirements, see the "Cisco MGM Software Requirements" section on page 2-5.

Upgrade the Cisco EMF server software according to the procedures described in the *Cisco Element Management Framework Installation and Administration Guide*.

Upgrading Cisco MGM Server Software

The following procedure details how to upgrade Cisco MGM server software which has been previously installed. If Cisco MGM server software has never been installed on the client workstation, you may perform a new installation. For further information on upgrading Cisco MGM server software, see the "Installing the Cisco MGM Server" section on page 2-9.

You can determine whether Cisco MGM server software exists on the workstation and/or the version of previously installed packages. For further information, see the "Viewing Software Version Information" section on page 2-18.

Before loading the software, the installation script automatically checks the system for existing Cisco MGM server packages. If an existing Cisco MGM server package is found, the script compares the existing version to the version on the CD. If the version on the CD is more recent, the previously installed version is upgraded. If the version on the CD is older than the installed version, no system change occurs. If an existing package is not found, the version on the CD is installed.

To upgrade the Cisco MGM server, follow these steps:

Step 1 Log in to the Cisco EMF/Cisco MGM server as the root user.

Step 2 Ensure that CiscoView 5.4 is installed and running on either the local or remote machine. For information about installing CiscoView, refer to the CiscoView product documentation located in the documentation directory of the CiscoView CD ROM.

Step 3 If the CiscoView server is on a remote machine, ensure that the CiscoView security integration and WANCV installation has taken place. For instructions on performing the security and Wan CV installations, see the "Installing CiscoView Applications" section on page 2-8.

Tip To ensure that the CiscoView security integration and WANCV packages have been installed, click **About** on the CiscoView main window. Verify that the package names appear in the Installed Device Packages list at the bottom of the window.

If the CiscoView server is on the local machine, the security and WanCV installation will be automatically performed by the Cisco MGM installation. Proceed to Step 4.

Step 4 Navigate to the appropriate package directory on the CD ROM by entering:

```
cd /cdrom/cmgm3.0pkg/cmgmv
```

Step 5 Start the installation script.

```
./cmgmvinstall
```

Tip To get help, enter **cmgmvinstall -h**

Note During installation, you may see 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.
```

Step 6 Follow the onscreen instructions. When prompted for the type of installation, select the **cmgmvpkg Server Package Upgrade** option.

A prompt displays requesting how you want to provide the host on which CiscoView and the required CiscoView applications are installed, by hostname or IP address.

Step 7 Enter the corresponding CiscoView host option at the prompt.

A prompt displays according to the entry provided in Step 7, hostname or IP address.

Step 8 Enter the appropriate CiscoView server hostname or IP address accordingly.

Text displays indicating that the CiscoView Security and WanCV device packages must be installed before upgrading the Cisco MGM server package and basic steps for installing. For additional information, see the "Installing CiscoView Applications" section on page 2-8.

The script continues with the Cisco MGM server package installation. Text displays recommending that you backup the Cisco EMF database before continuing. Should you initiate a backup at this time, all sessions connected to the server will stop. For additional information, see the "Backing Up the Cisco EMF Database" section on page 2-13.

The script checks to see if the Cisco MGM server package has been previously installed. If it determines that it has not, installation occurs as the "Installing Cisco EMF Server Software" section on page 2-9 describes. If a version of the Cisco MGM server package has been previously installed, the timestamp of the installed package displays. If this time stamp is newer or the same as the version on the CD, the installation script aborts. If the time stamp is older than the version on the CD, the time stamp displays and you are prompted to confirm the upgrade.

Step 9 Enter y to proceed with the upgrade or n to quit the upgrade accordingly.

The script removes the existing Cisco MGM server package and, again, prompts you to confirm the upgrade.

Step 10 Enter y to proceed with the upgrade or n to quit the upgrade accordingly.

Note that if you did not proceed with the upgrade at this point, you must install the Cisco MGM server package as a new installation. For further information, see the "Installing Cisco EMF Server Software" section on page 2-9.

The installation of the current software continues and data displays indicating the resulting activities.

Upon completion of the package installation, you may check the installation log for errors. The log file is in the following location:

```
/var/adm/Atlantech/avinstall/Cisco_Element_Management_Framework_-_Server/logfile
```

You may verify that the cmgmCtlr process is running. For example:

```
/opt/cemf/bin/cemf status
```

Restoring the Cisco EMF Database

If the Cisco EMF database was backed up as identified by the "Backing Up the Cisco EMF Database" section on page 2-13, restoration is possible via the RME application.

For overview information on the RME tool and instructions specific to using RME with Cisco EMF, see the *Cisco Element Management Framework Installation and Administration Guide* and the *Cisco Element Management Framework User Guide.* For detailed information on the RME tool, see the *User Guide for Resource Manager Essentials.*

Restoring Cisco MGM Configuration Files

You restore network card and chassis configurations using the Cisco MGM configuration restore feature. The Cisco MGM configuration restore function logs on to the selected device, and sends a **tftp put** command to transfer the configuration file from your Cisco MGM workstation to the selected device. For further information, see the "Configuration Restore" section on page 4-11.

Synchronizing Managed Devices

After upgrading the server package, manually invoking subchassis synchronization initiates the subchassis discovery process to resync the system with the managed devices. Subchassis component information from each Cisco MGX 8000 Series CVG is retrieved to display corresponding objects on the Cisco MGM user interface.

The subchassis synchronization process inspects SNMP MIBs for the following configurable objects:

- Chassis and status
- Card configuration and status, including PXM1, PXM1-E, PXM45, VISM, VISM-PR, RPM-PR, RPM-XF, SRM, SRM-E, AXSM, and AXSM-E cards and lines
- Line configuration and status, including DS1, DS3, and SONET

For additional information, see the "Manual Initiation of Subchassis Synchronization" section on page 4-5.

Upgrading a Cisco MGM Client

In order to upgrade the Cisco MGM client software, you must first ensure that the Cisco EMF client software is upgraded to the required level. For the current Cisco EMF software requirements, see the "Cisco MGM Software Requirements" section on page 2-5. Upgrade the Cisco EMF client software according to the procedures described in the *Cisco Element Management Framework Installation and Administration Guide*.

The following procedure details how to upgrade Cisco MGM client software which has been previously installed. If Cisco MGM client software has never been installed on the client workstation, you may perform a new installation. For further information on upgrading Cisco MGM client software, see the "Installing Cisco MGM Clients" section on page 2-11.

Before loading the software, the installation script automatically checks the system for existing Cisco MGM client packages. If an existing Cisco MGM client package is found, the script compares the existing version to the version on the CD. If the version on the CD is more recent, the previously installed version is upgraded. If the version on the CD is older than the installed version, no system change occurs. If an existing package is not found, the version on the CD is installed.

To upgrade Cisco MGM client software, follow these steps:

Step 1 Log in to Cisco EMF as the root user.

Step 2 Ensure that the CiscoView Security and WanCV device packages are installed on the CiscoView server.

For further details, see the "Installing CiscoView Applications" section on page 2-8.

Step 3 Navigate to the appropriate package directory on the CD ROM by entering:

```
cd /cdrom/cmgm3.0pkg/cmgmv
```

Step 4 Start the installation script.

```
./cmgmvinstall
```

Tip To get help, enter **cmgmvinstall -h**

Step 5 Follow the onscreen instructions. When prompted for the type of installation, select the **cmgmvpkg Client Package Upgrade** option.

A prompt displays requesting how you want to provide the host on which CiscoView and the required CiscoView applications are installed, by hostname or IP address.

Step 6 Enter the corresponding CiscoView host option at the prompt.

A prompt displays according to the entry provided in Step 6, hostname or IP address.

Step 7 Enter the appropriate CiscoView server hostname or IP address accordingly.

Text displays indicating that the CiscoView Security and WanCV device packages must be installed before upgrading the Cisco MGM client package and basic steps for installing. For additional information, see the "Installing CiscoView Applications" section on page 2-8.

The script continues with the Cisco MGM client package installation. The script checks to see if the Cisco MGM client package has been previously installed. If it determines that it has not, installation occurs as the "Installing Cisco MGM Client Software" section on page 2-12 describes. If a version of the Cisco MGM client package has been previously installed, the timestamp of the installed package displays. If this time stamp is newer or the same as the version on the CD, the installation script aborts. If the time stamp is older than the version on the CD, the time stamp displays and you are prompted to confirm the upgrade.

Step 8 Enter y to proceed with the upgrade or n to quit the upgrade accordingly.

The script removes the existing Cisco MGM client package and prompts you to confirm the upgrade.

Step 9 Enter y to proceed with the upgrade or n to quit the upgrade accordingly.

Note that if you did not proceed with the upgrade at this point, you must install the Cisco MGM client package as a new installation. For further information, see the "Installing Cisco MGM Client Software" section on page 2-12.

The installation of the current software continues and data displays indicating the resulting activities.

Upon completion of the package installation, you may check the installation log for errors. The log file is in the following location:

```
/var/adm/Atlantech/avinstall/Cisco_Element_Management_Framework_-_Server/logfile
```

You may verify that the cmgmCtlr process is running. For example:

```
/opt/cemf/bin/cemf status
```

Changing the Installation

Cisco MGM includes scripts and options for viewing software information and uninstalling software.

Viewing Software Version Information

To view software version information, follow these steps:

Step 1 Log in as the root user.

Step 2 Change to the directory for the installation script.

```
cd <CEMFROOT>/config/scripts/cmgmv
```

Step 3 Run the installation script with the -s option.

```
./cmgmvinstall -s
```

The script displays software information

Uninstalling Cisco MGM Server or Client

The uninstall script can be run on the server and/or client machines. When you uninstall the Cisco MGM server, you also remove the Cisco MGM client from the same host. On a client machine, the script just removes the client software.

Note Before uninstalling the Cisco MGM server or client, backup your Cisco EMF database according to the procedures described in the *Cisco Element Management Framework Installation and Administration Guide,* Chapter, 10, “Cisco EMF Database Backup and Restore”.

To remove Cisco MGM, follow these steps:

Step 1 Log in as the root user.

Step 2 Change to the script directory.

```
cd <CEMFROOT>/config/scripts/cmgmv
```

Step 3 Run the uninstallation script.

```
./cmgmvinstall -r
```

Step 4 If you receive a “port not ready” message, repeat Step 3. If the problem persists, contact technical support.

Step 5 Check the installation log for errors. The server log file is in the following location:

```
/var/adm/Atlantech/avinstall/Cisco_Element_Management_Framework_-_Server/logfile
```

The client log file is in the following location:

```
/var/adm/Atlantech/avinstall/Cisco_Element_Management_Framework_-_Client/logfile
```

Note Uninstalling Cisco MGM does not uninstall WanCV and other CiscoView integration files that were installed in Step 2 of the installation procedures. The following directory and files remain in your CiscoView installation:

```
<CiscoView Root>/www/classpath/ems
<CiscoView Root>/www/classpath/cvpars.properties
<CiscoViewRoot>/www/classpath/com/cisco/nm/cvw/devpkgs/MGX8*.zip
<CiscoView Root>/htdocs/CmgmSessionTimeOut.html
```

Configuring Cisco MGX 8000 Series CVGs

For the Cisco MGM to communicate with Cisco MGX 8000 Series CVGs, you must initialize the following parameters for each chassis:

- Management IP address
- System location
- Read and read-write community strings
- Telnet/FTP login and password

For more information about configuring Cisco MGX nodes, refer to the following documents:

- *Cisco MGX 8230 Multiservice Gateway Command Reference*
- *Cisco MGX 8250 Multiservice Gateway Command Reference*
- *Cisco MGX 8830, MGX 8850 (PXM45 and PXM1E), and MGX 8950 Command Reference*

For detailed information about managing Cisco MGX 8000 Series CVGs using CiscoView, refer to CiscoView Documents on CCO, or refer to the following individual documents:

- *WAN CiscoView Release 3 for the MGX 8230 Edge Concentrator, Release 1*
- *WAN CiscoView Release 3 for the MGX 8250 Edge Concentrator, Release 1*
- *WAN CiscoView Release 3 for the MGX 8850 Edge Switch, Release 1*
- *WAN CiscoView Release 2 of the MGX 8850*

User Interfaces

Cisco MGM provides a graphical user interface using Unix Motif. For device specific configuration functions, Cisco MGM also provides access to the CiscoView GUI, as well as to command line interface functions through telnet sessions.

For detailed information on CiscoView installation and operation, refer to *Using CiscoView 5.4*.

For command line interface functions, refer to the following documents:

- *Cisco MGX 8230 Multiservice Gateway Command Reference*
- *Cisco MGX 8250 Multiservice Gateway Command Reference*
- *Cisco MGX 8830, MGX 8850 (PXM45 and PXM1E), and MGX 8950 Command Reference*

Cisco EMF User Sessions

Cisco MGM uses the Cisco EMF user interface and security features. In order to gain access to Cisco MGM features, start a Cisco EMF user session.

Starting a Cisco EMF User Session

Note The Cisco EMF server should already be running. When you start your system, if you receive a message that Cisco EMF is not running, contact your system administrator.

To start a Cisco EMF user session, follow these steps:

Step 1 From the command line on the terminal window, type:

```
host# <CEMFROOT>/bin/cemf session
```

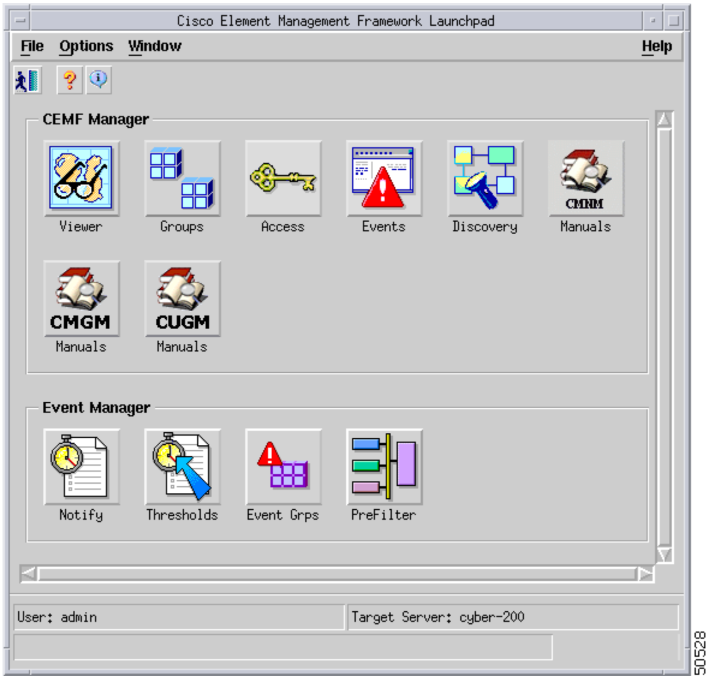
where <*CEMFROOT*> is the root directory for Cisco EMF installation (for example, **/opt/cemf**).

The Cisco EMF Login window opens.

Step 2 Enter your user name and password, and click **OK**.

The Cisco EMF Launchpad window opens. (See Figure 3-1.)

Figure 3-1 Cisco EMF Launchpad



User: admin
Target Server: cyber-200

The icons on the Launchpad represent applications provided by this Cisco EMF installation.

The area at the bottom of most windows displays status information. When you double-click in this area, the Status Dialog window opens. This window lists previous status messages.

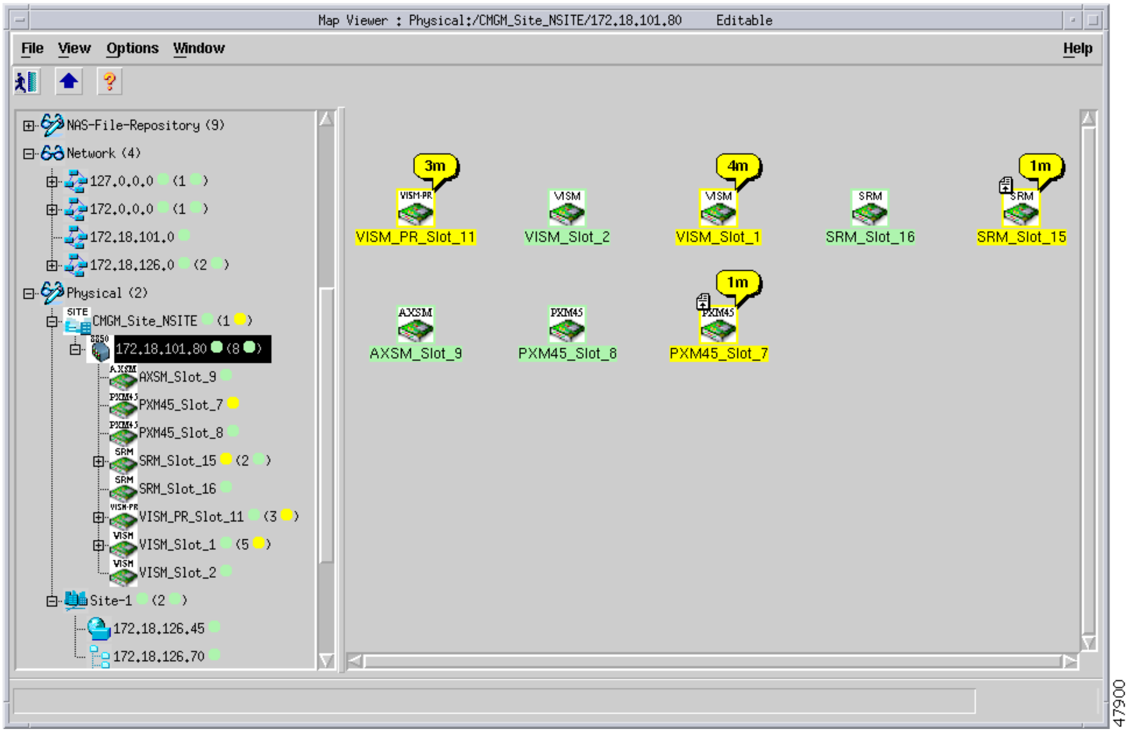
Launching an Application

To launch an application, click on the desired application icon in the Cisco EMF Launchpad. A “busy” icon and a message in the status bar are displayed during launch. You can open more than one instance of an application simultaneously.

Note If an application is already open, it appears in the Windows list. Click **Window** and choose the application from the drop down menu.

For Cisco MGM, the Viewer application displays information about the Cisco MGX 8000 Series network cards and other equipment. (See Figure 3-2.)

Figure 3-2 Cisco MGM Topology View



Cisco MGM displays Cisco MGX 8000 Series CVGs and media gateway controllers as icons.

Quitting a Cisco EMF User Session

To quit a Cisco EMF user session, follow these steps:

Step 1 From the File menu, select **Close** or press **Ctrl-W**.

Step 2 A dialog box is displayed.

```
Do you wish to quit the CEMF Manager System?
```

Click **Yes** to quit the session.

All active applications are closed, and the session terminates.

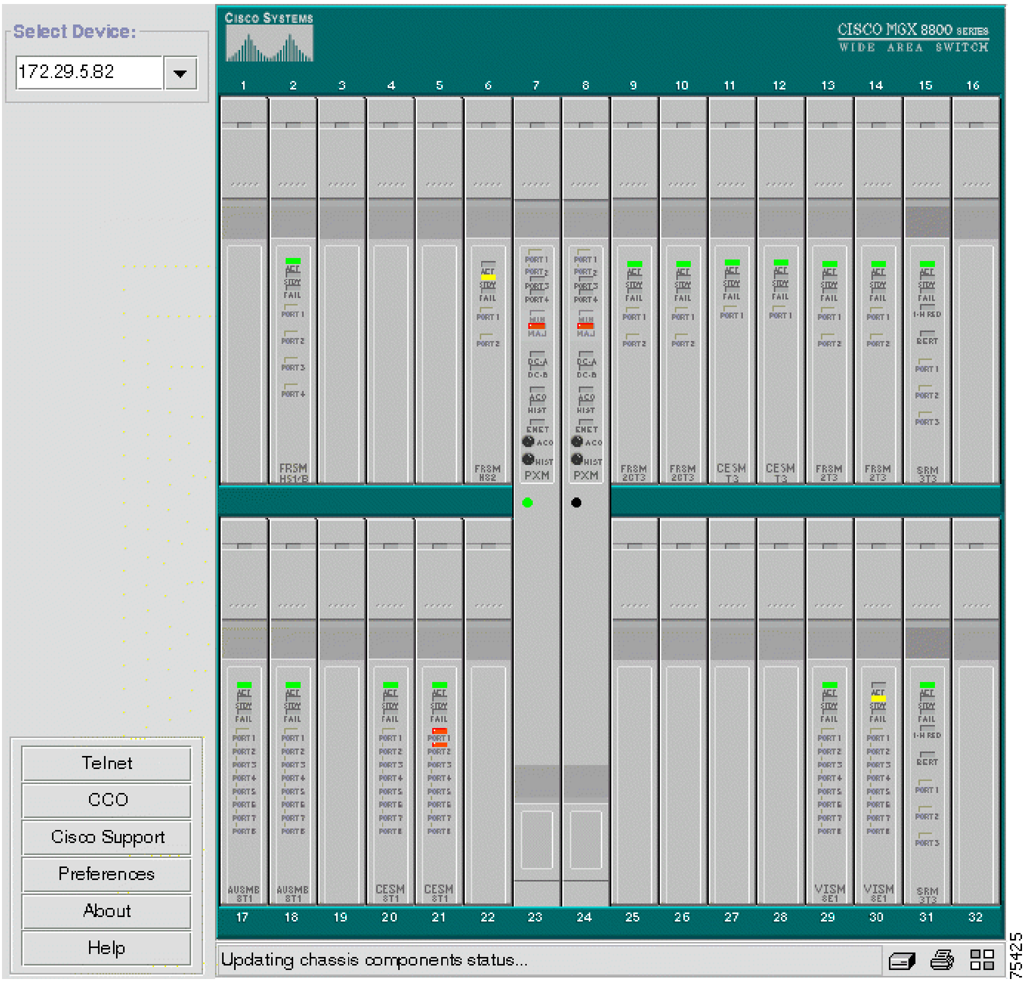
CiscoView

CiscoView is a graphical SNMP-based device management tool that provides powerful real-time views of your networked Cisco Systems devices. These views deliver a continuously updated 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.

Figure 3-3 shows an example view of the CiscoView interface.

Figure 3-3 CiscoView Interface



Select Device: 172.29.5.82

Updating chassis components status...

CiscoView device software is installed as a device package; for example, the MGX 8850 software is installed as the MGX8850.*pkg*. CiscoView uses the device package to display a dynamic view of the physical device and all its components.

If you are installing CiscoView and Cisco MGM on the same server, the device package is automatically installed as part of the Cisco MGM installation. For more information about Cisco MGM installation, refer to Chapter 2, “Installation.”

If you are installing CiscoView and Cisco MGM on different servers, use Cisco MGM CD to install the device package on the remote CiscoView server. For detailed information on CiscoView installation and operation, refer to *Using CiscoView 5.4*.

Starting a CiscoView Session

To launch CiscoView and configure a Cisco MGX 8000 Series CVG from Cisco MGM, follow these steps:

Step 1 Make sure you do not have any Netscape processes 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.)

Step 2 On the MapViewer, right-click the desired MGX 8000 Series node; then click **Tools**; then click **Launch CiscoView (Read Only)** for CiscoView read access or **Launch CiscoView (Read-Write)** for full CiscoView configuration access.

Step 3 A graphical view of the opened device is displayed in the CiscoView window. Use this view to configure and monitor the device and its components.

For detailed information about managing Cisco MGX 8000 Series CVGs using CiscoView, refer to CiscoView Documents on CCO, or refer to the following individual documents:

- *WAN CiscoView Release 3 for the MGX 8230 Edge Concentrator, Release 1*
- *WAN CiscoView Release 3 for the MGX 8250 Edge Concentrator, Release 1*
- *WAN CiscoView Release 3 for the MGX 8850 Edge Switch, Release 1*
- *WAN CiscoView Release 2 of the MGX 8850*

Initiating a Telnet Session

To initiate a telnet session, follow these steps:

Step 1 On the MapViewer, right-click the desired MGX 8000 Series node; click **Tools**; click **Launch Telnet**.

The telnet screen opens.

Step 2 At the User prompt, enter the name of a valid MGX 8000 Series account name. For a new system, enter **SuperUser**.

Step 3 At the Password prompt, type the account password. On a new system, use **cisco** or the new password you assigned to this account.

CHAPTER 4

Configuration

Cisco MGM automatically discovers network elements and displays them on the Map Viewer screen. From this screen you can view operational status and navigate to screens that support Cisco MGX 8000 Series CVG configuration and software upgrades.

Cisco MGM Site Organization

Cisco MGM organizes MGX 8000 Series CVGs by site. A site contains all gateways that have the same value for the standard SNMP sysLocation object. If a gateway does not have a value set for sysLocation, Cisco MGM includes the gateway under CMGM_Site_default. If a gateway does have a value set for sysLocation, Cisco MGM includes the gateway under the site titled CMGM_Site_<sysLocation value>.

Note A Cisco MGM site remains in the system even if you delete all its gateways. Use Deployment > Delete Objects to remove an empty site.

To change the system location of a selected object, follow these steps:

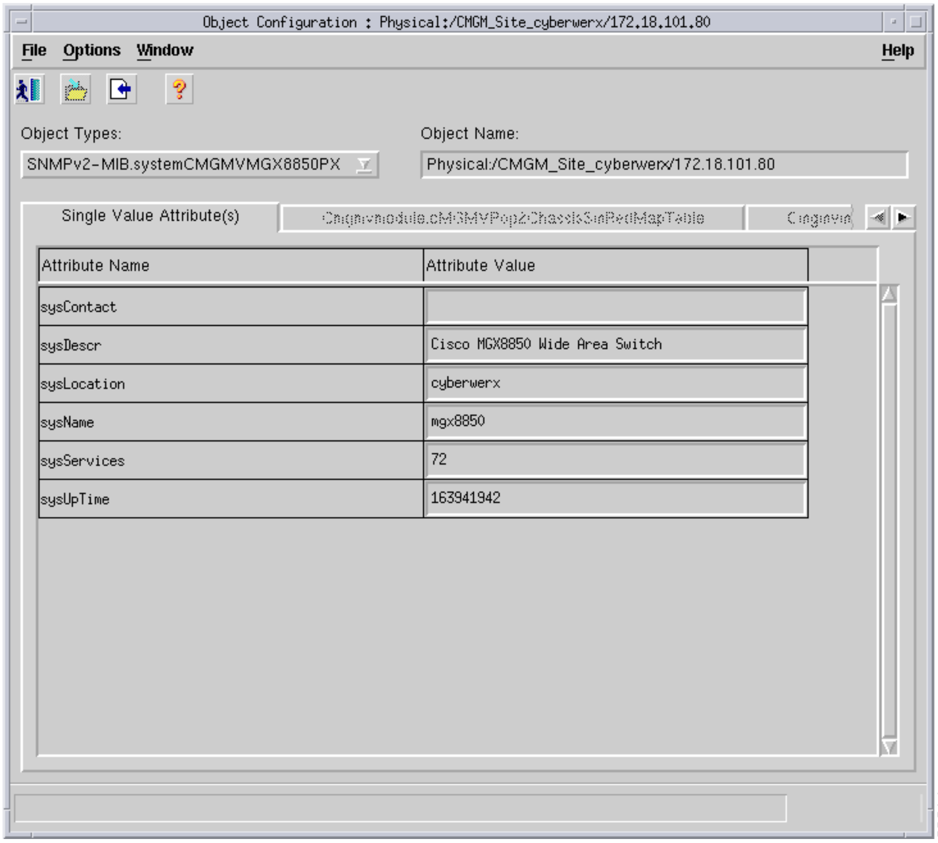
Step 1 Log on to Cisco EMF. The Cisco Element Manager Framework Launchpad screen opens.

Step 2 Click the **Viewer** button. The MapViewer screen opens.

Step 3 Click the tree of objects to display the list of sites and nodes.

Step 4 Right-click the desired site or node and select **Open Object Configuration**. The Object Configuration window opens. (See Figure 4-1.)

Figure 4-1 Object Configuration


Object Configuration : Physical:/CMGM_Site_cyberwerx/172.18.101.80
File Options Window Help
Single Value Attribute(s)
Cmgmvmodule.cMGMVPop2ChassisSnRedMapTable
Cmgmvm
89014

Object Types: SNMPv2-MIB.systemCMGMVMGX8850PX

Object Name: Physical:/CMGM_Site_cyberwerx/172.18.101.80

Attribute Name	Attribute Value
sysContact	
sysDescr	Cisco MGX8850 Wide Area Switch
sysLocation	cyberwerx
sysName	mgx8850
sysServices	72
sysUpTime	163941942

Step 5 Select the desired object from the **Object Types** list. The associated object parameters display in the **Single Value Attributes** tab.

Step 6 Enter the new system location in the **sysLocation** field, then choose **File > Save**. The system updates the location for the selected object.

Node Discovery

Automatic discovery occurs in two phases:

1. Automatic discovery of Cisco MGX 8000 Series CVGs and associated media gateway controllers in a subnet.
2. Subchassis synchronization of MGX 8000 Series subcomponents.

You initiate automatic discovery from the Cisco MGM GUI by specifying the desired IP address range. Cisco MGM automatically discovers MGX 8000 Series CVGs and media gateway controllers with IP addresses that fall within this range. For more information, see the "Cisco MGM Community String and Security Configuration" section on page 7-2.

Invoking Automatic Discovery

When you initiate automatic discovery, Cisco EMF pings each IP address in the given range. If a response is received, Cisco EMF initiates an SNMP GET request for the enterprise object id (OID). If the OID matches any of the predefined Cisco EMF class mappings, an object of that class is created and displayed. If no match is found, the process creates a generic SNMP device under the physical level of the hierarchy. You can't manage these generic devices.

To discover network elements, follow these steps:

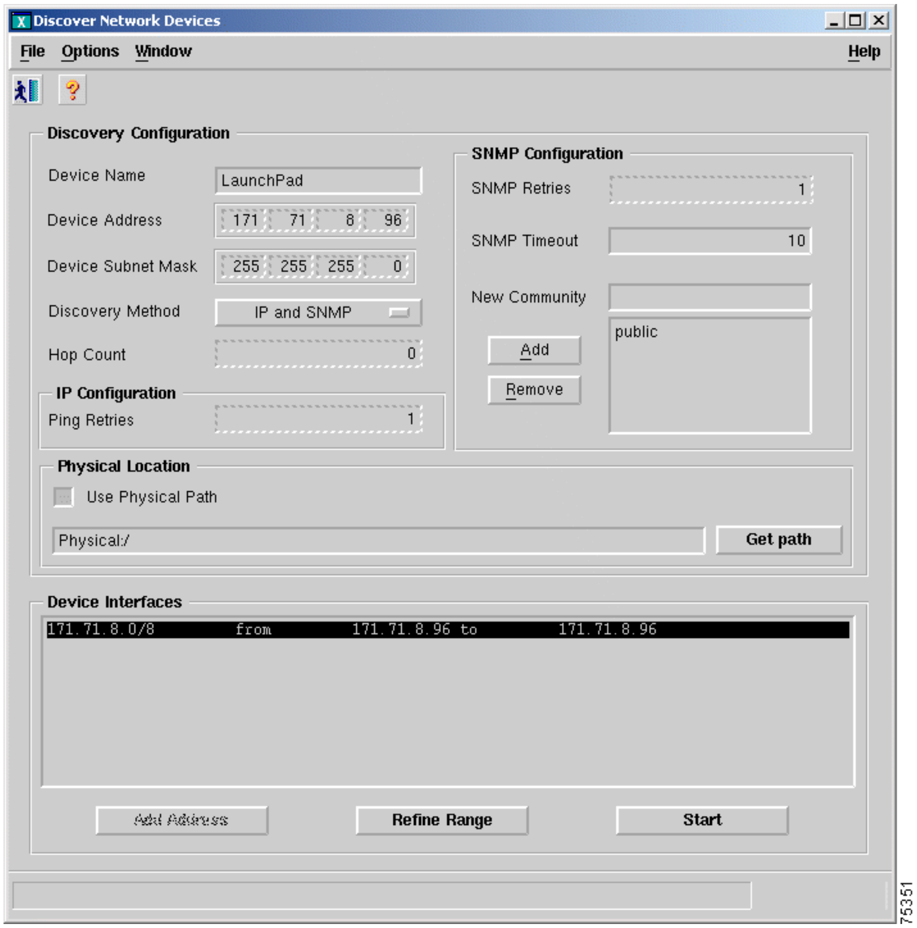
Step 1 Start Cisco EMF.

```
<CEMFROOT>/cemf/bin/cemf session
```

Step 2 Log on to Cisco EMF. The Launchpad screen opens.

Step 3 Click the **Discovery** button. The Discover Network Devices screen opens. (See Figure 4-2.)

Figure 4-2 Discover Network Devices



Device Name: LaunchPad

Device Address: 171 . 71 . 8 . 96

Device Subnet Mask: 255 . 255 . 255 . 0

Discovery Method: IP and SNMP

Hop Count: 0

Ping Retries: 1

SNMP Retries: 1

SNMP Timeout: 10

New Community:

public

□ Use Physical Path

Physical:/

```
171.71.8.0/8        from          171.71.8.96 to          171.71.8.96
```

Step 4 Configure the discovery parameters:

Parameter	Description
Device Name	Fixed as LaunchPad.
Device Address	The IP address from which to start the discovery process, expressed in standard dot notation.
Discovery Method	The method of discovery, IP, SNMP, or IP and SNMP. Specify SNMP to discover all components.
Hop Count	The number of routing hops to allow. Default: 0.
Ping Retries	The number of times to ping each address in the range. Default: 1.
SNMP Retries	The number of SNMP retries to allow. Default: 1.
SNMP Timeout	The timeout of SNMP tries. Default: 10.
New Community	Add or remove SNMP communities.
Physical Location	The physical path in the Cisco EMF hierarchy. Click Use Physical Path to use an existing path.
Interface Attributes	The subnet and range of IP addresses to search. Double click to specify or change the range.

Step 5 Click **Start**.

Step 6 At the end of the discovery process, click **Close**.

Inventory Discovery

Subchassis synchronization searches for entities within a Cisco MGX 8000 Series CVG and displays them on the Cisco MGM user interface. The subchassis synchronization process is automatically invoked after auto discovery. The subchassis synchronization process inspects SNMP MIBs for the following configurable objects:

- Chassis and Status
- Card Configuration and Status, including PXM1, PXM1-E, PXM45, VISM, VISM-PR, RPM-PR, RPM-XF, SRM, SRM-E, AXSM, and AXSM-E cards and lines
- Line Configuration and Status, including DS1, DS3, and SONET.

Cisco MGM uses the read-write community string for subchassis synchronization. You can change the default read-write community string in the cmgmvCtrlUserData.ini file. For more information about the cmgmvCtlrUserData.ini file, refer to Appendix A, “Cisco MGM Server Configuration Files.”

When the subchassis synchronization process is complete, Cisco MGM adds the subchassis components to the site hierarchy display. You can expand the hierarchy to display cards and profiles by clicking the + sign next to the Cisco MGX 8000 Series icons. Similarly, you can expand the hierarchy to display lines by clicking the + sign next to each card. A number next to the object indicates the number of contained cards or lines.

Manual Initiation of Subchassis Synchronization

You can manually invoke the subchassis synchronization process from the Cisco EMF menu bar. The subchassis discovery process retrieves subchassis component information from each Cisco MGX 8000 Series CVG and displays corresponding objects on the Cisco MGM user interface.

To synchronize subchassis components, follow these steps:

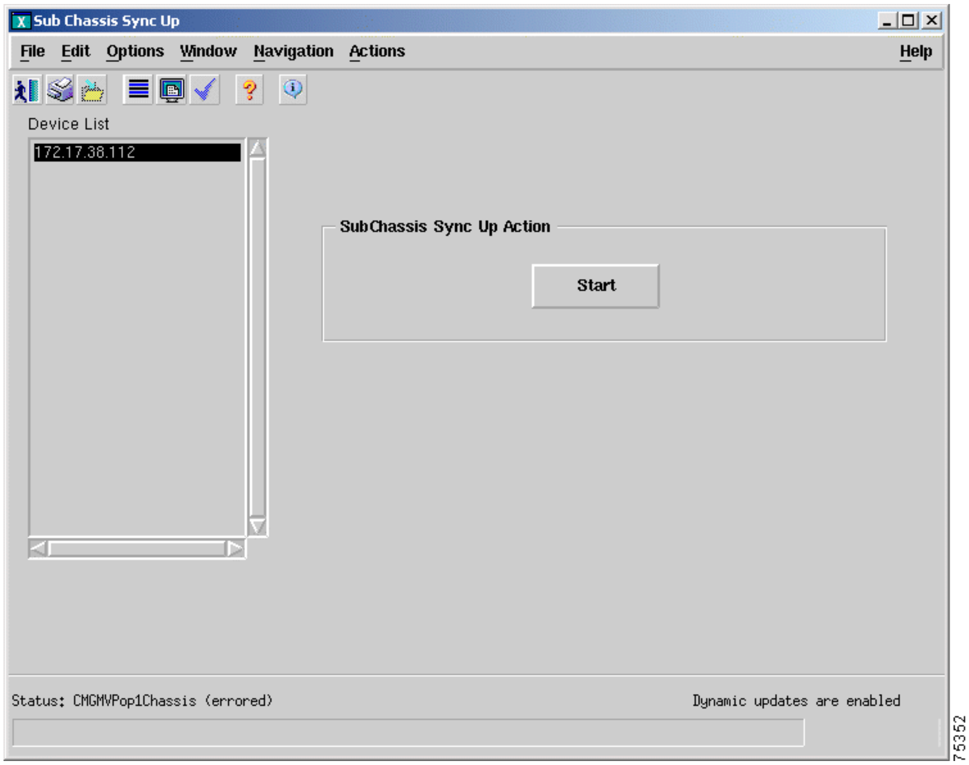
Step 1 Log on to Cisco EMF. The Cisco Element Manager Framework Launchpad screen opens.

Step 2 Click the **Viewer** button. The MapViewer screen opens.

Step 3 Click the tree of objects to display the list of sites and nodes.

Step 4 Right-click the desired site or node and select **SubChassis Sync Up**. The Subchassis Sync Up window opens. (See Figure 4-3.)

Figure 4-3 Subchassis Sync Up



Device List

172.17.38.112

Status: CMGMVPop1Chassis (errored)

Dynamic updates are enabled

Step 5 Select the desired nodes from the list.

Step 6 Click **Start**.

The system synchronizes the user display with subchassis components.

Periodic Subchassis Synchronization

Periodic subchassis synchronization discovers the subchassis components of each node without user intervention. This background task runs on a fixed interval, once every 24 hours, rather than at a fixed time. Therefore, the time of day when this task runs depends on the last time the Cisco MGM controller was initialized.

Object Configuration

Object configuration data for Cisco MGM supported objects are available through the Cisco EMF Object Configuration window. By selecting an object and launching the Object Configuration window, data specific to the selected object is available. Choose the appropriate option from the Object Type list to view the applicable data in the lower portion of the window. Because each type of object is modeled differently in the software, data is available through different object type selections for each type of object. For example, the available object type selections for a VISM card differ from those supporting a AXSM card.

Although the data presented in the Object Configuration window is modifiable, it is not recommended to save changes.

For further information on launching and using the Object Configuration window, see the *Cisco Element Management Framework User Guide*.

Downloading and Activating Software Images

The software download feature facilitates the downloading of runtime and backup boot image files from a Cisco MGM workstation to a device. Depending upon the device type, the image is downloaded either via TFTP (PXM1-based card) or FTP (PXM1-E or PXM45-based cards.) The system reports whether the download was a success or failure; in the case of a failure, detailed information is provided about the failed TFTP or FTP commands. Downloading a software image does not automatically activate it; the selected gateway continues to operate on current software until you perform the upgrade procedure.

Note Runtime software image files are saved using the extension ".fw" and boot images are saved using the extension ".bt".

Downloading Software Images

To download software image files, follow these steps:

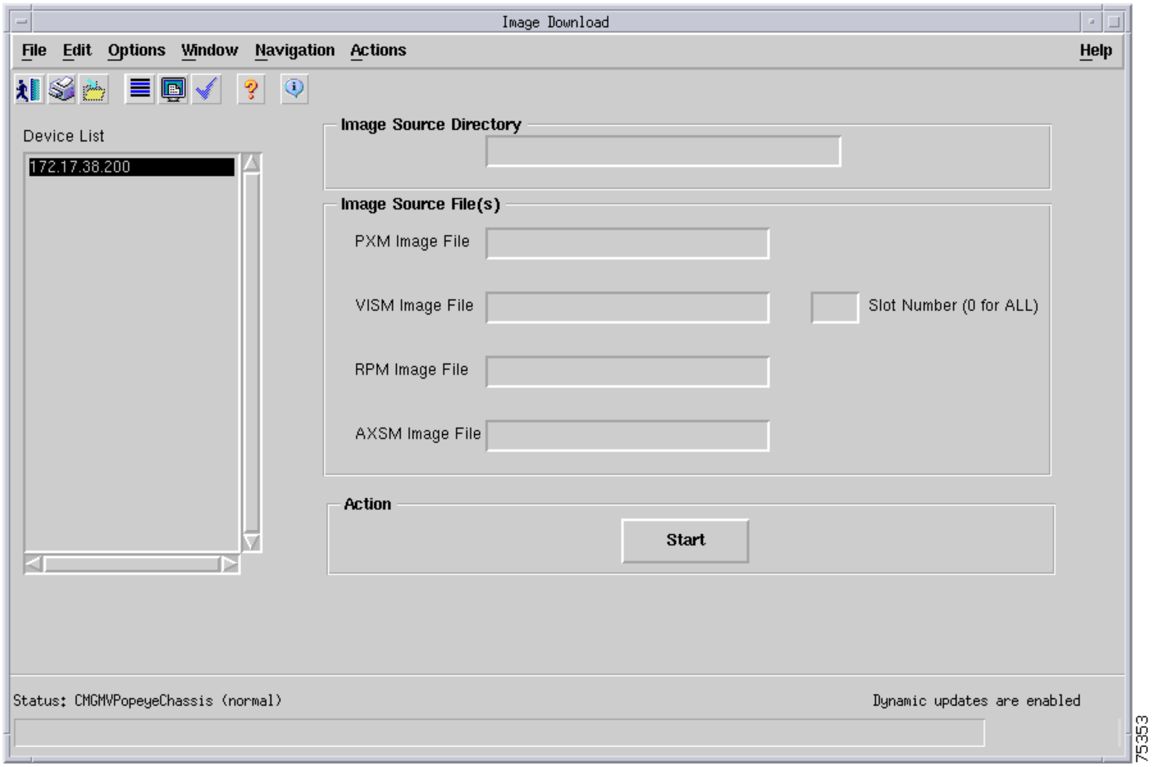
Step 1 Log on to Cisco EMF. The Launchpad screen opens.

Step 2 Click the **Viewer** button. The Map Viewer screen opens.

Step 3 Click the tree of objects to display the list of sites and nodes.

Step 4 Right-click the icon for the desired site or chassis and select **Image Download**. The Image Download screen opens. (See Figure 4-4.)

Figure 4-4 Image Download



172.17.38.200

Status: CMGMVPopeyeChassis (normal)

Step 5 Enter the file information shown in Table 4-1.

Caution Cisco MGM does not check for a match between the device and the image file entered. If you select an incorrect type of image for the device, the device does not function properly. Before installing images on your managed devices, check their compatibility by contacting the Cisco Technical Assistance Center.

Table 4-1 Software Image Download

Field	Description	Usage
Device	List of devices	Select the device objects for software download.
Image Source Directory	Text field for entering the directory from which the image files are to be downloaded	Enter the source directory for the image file(s).
Image Source File(s)	Boot or runtime image files for PXM, VISM, RPM, and AXSM cards	Enter the full boot or runtime image filename(s) for the corresponding card types to download to the device. The detailed description of each text field in the Image Source File(s) frame is listed below:
	PXM Image File	Enter the PXM image file name. **Note** PXM1, PXM1-E, and PXM45 images can be entered in this field.
	VISM Image File	Enter the VISM image file name. **Note** VISM and VISM-PR images can be entered in this field.

Table 4-1 Software Image Download (continued)

Field	Description	Usage
	RPM Image File	Enter the RPM image file name. **Note** RPM, RPM-PR, and RPM-XF images can be entered in this field.
	AXSM Image File	Enter the AXSM image file name. **Note** AXSM and AXSM-E images can be entered in this field.
Slot Number	Integer field to enter slot number for VISM image file	Specify the card slot number of the VISM image file you want to download. If you enter 0 in the Slot Number field or the Slot Number field is empty, the image is downloaded to all cards on the device.

Step 6 Click **Start.** An action result dialog appears with status of the image download action for the selected devices. If successful, the software image files are sent via either TFTP or FTP (depending upon the device type) to the appropriate device directory.

Note Upon successful download of a PXM image file, another supporting file named ComMat.dat is automatically downloaded to the device as well.

Step 7 Repeat steps 5 to 6 for other card images.

Step 8 Click **Close** when finished downloading the desired software images to close the Image Download window.

Activating Software Images

Once the desired software image files have been downloaded, you must telnet to the device and execute the necessary commands to fully activate the image. For more information on how to activate software image files that have been downloaded to the system, refer to the following documents:

- *Cisco MGX 8850 and MGX 8950 Switch Software Configuration Guide*
- *Cisco MGX 8850 (PXM1E) and MGX 8830 Switch Software Configuration Guide*
- *Cisco MGX 8850 (PXM45) and MGX 8950 Switch Software Configuration Guide*

Configuration Save and Restore

You can back up and restore network card and chassis configurations using the Cisco MGM configuration save and restore feature. 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.

Configuration Save

The Cisco MGM 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.

To save a device configuration file, follow these steps:

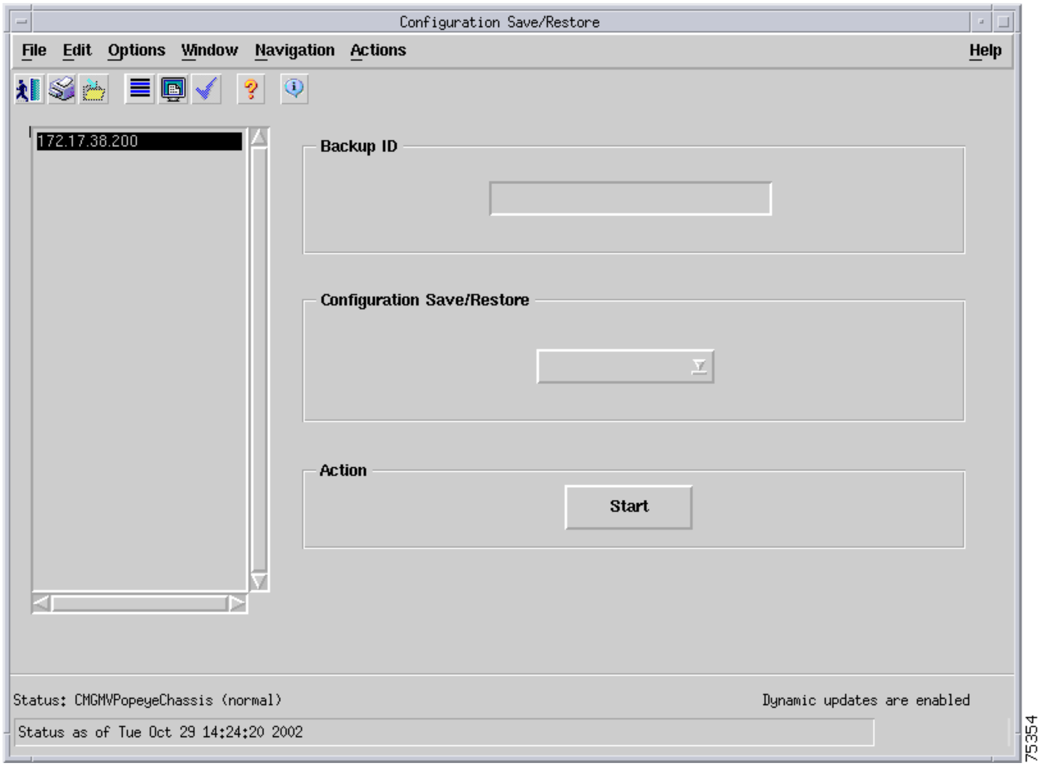
Step 1 Log on to Cisco EMF. The Launchpad screen opens.

Step 2 Click the **Viewer** button. The Map Viewer screen opens.

Step 3 Click the tree of objects to display the list of sites and nodes.

Step 4 Right-click the icon for the desired site and click **Configuration Save/Restore**. The Configuration Save/Restore Dialog window opens. (See Figure 4-5.)

Figure 4-5 Configuration Save/Restore Dialog


Configuration Save/Restore
File Edit Options Window Navigation Actions Help
172.17.38.200
Backup ID
Configuration Save/Restore
Action
Start
75354

Status: CMGMVPopeyeChassis (normal)

Dynamic updates are enabled

Status as of Tue Oct 29 14:24:20 2002

Step 5 Enter the required information. (See Table 4-2.)

Note The default pull-down menus are blank. You must click on each pull-down menu to reveal the available options.

Table 4-2 Configuration Save/Restore Information

Field	Description	Usage
Device List	List of devices	Select the device objects you want to save/restore. You can select multiple devices at the same time.
Backup ID	Alphanumeric text field to enter the backup ID.	You can save multiple versions of the configuration files in different directories if a different backup ID is used each time.
Configuration Save/Restore	Drop down menu to select the save or restore action.	—

Step 6 Click **Start.**

Step 7 An Action Result Dialog appears with the status of the Configuration Save/Restore action on the selected devices.

Configuration Restore

Note The Configuration Restore action transfers only the configuration file from the Cisco MGM workstation to the device hard disk. To restore all the configuration files, telnet to the device and use the CLI **restoreallcnf** command.

The Cisco MGM configuration restore function logs on to the selected device, and sends a **tftp put** command to transfer the configuration file from your Cisco MGM workstation to the selected device.

To restore a device configuration file, follow these steps:

Step 1 Log on to Cisco EMF. The Launchpad screen opens.

Step 2 Click the **Viewer** button. The Map Viewer screen opens.

Step 3 Click the tree of objects to display the list of sites and nodes.

Step 4 Right-click the icon for the desired site and click **Configuration Save/Restore**. The Configuration Save/Restore window opens. (See Figure 4-5.)

Step 5 Enter the required information. (See Table 4-2.)

Note The default pull-down menus are blank. You must click on each pull-down menu to reveal the available options.

Step 6 Click **Start.**

Step 7 An Action Result Dialog appears with the status of the Configuration Save/Restore action on the selected devices.

CHAPTER 5

Administration

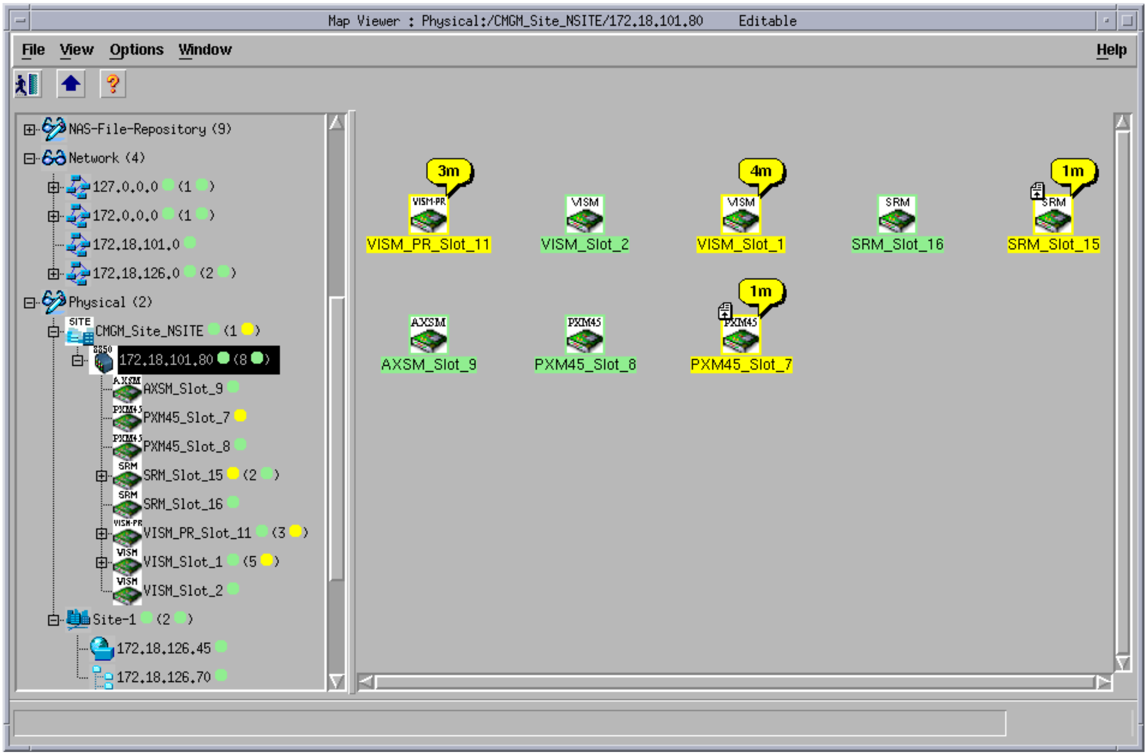
MapViewer

Cisco MGM MapViewer displays information about Cisco MGX 8000 Series CVGs, MGX 8000 Series components, and media gateway controllers (MGCs).

Each object shown in the right window provides graphical cues about the network element that it represents. The information can be structural (for example, a network element name), or it can be state and event information (for example, “out of service”). If an object becomes unreachable, it is represented by a bomb icon.

Figure 5-1 shows an example of a typical MapViewer display.

Figure 5-1 Cisco MGM MapViewer



Changing Node States

Cisco MGM 3.0 reports Cisco MGX 8000 Series CVGs as being in one of the following states:

- Error
- Normal (commissioned)
- Maintenance (decommissioned)

The default is Normal state. However, in some circumstances, you may need to change the node to Maintenance state.

To change the default state of a Cisco MGX 8000 Series CVG, perform the following steps:

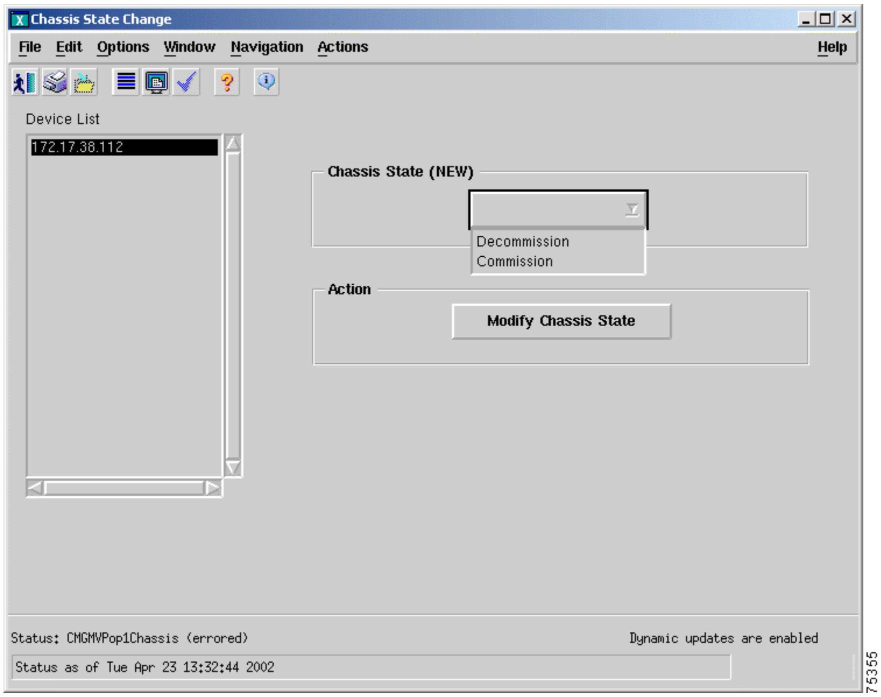
Step 1 Log on to Cisco EMF. The Launchpad screen opens.

Step 2 Click the **Viewer** button. The Map Viewer screen opens.

Step 3 Click the tree of objects to display the list of sites and nodes.

Step 4 Right-click the icon for the desired site or chassis and select **Chassis State Change**. The Chassis State Change Dialog window opens. (See Figure 5-2.)

Figure 5-2 Chassis State Change Dialog



Status: CMGMVPop1Chassis (errored)

Dynamic updates are enabled

Status as of Tue Apr 23 13:32:44 2002

Step 5 Select **Decommission** or **Commission** from the Chassis State pull-down menu.

Note The default pull-down menu is blank. You must click on the pull-down menu to reveal the available options.

Step 6 Click **Modify Chassis State**.

Fault and Performance Management

The Cisco MGM Alarm component, which is a customized component of the Cisco EMF platform, handles Cisco MGX 8000 Series CVG alarms and events. Cisco MGM receives alarm and event messages from managed objects and displays them in the MapViewer and Event Browser screens. MapViewer displays alarms on the topology view, and the event browser displays events in tabular form. The tabular data includes severity, date, source, and other information.

Cisco MGM implements alarm features using SNMP trap messages. A configuration file maps SNMP traps to Cisco MGM alarms. For more information, see the *Cisco Element Management Framework User Guide*.

Before Cisco MGM can process alarm information, you need to register the traps you want the Cisco MGX 8000 Series CVG to forward.

Monitoring Alarms and Events

You can monitor alarms and events from two screens:

- Map Viewer—Shows icons that indicate the most severe alarm
- Event Browser—Shows a table of alarms and events

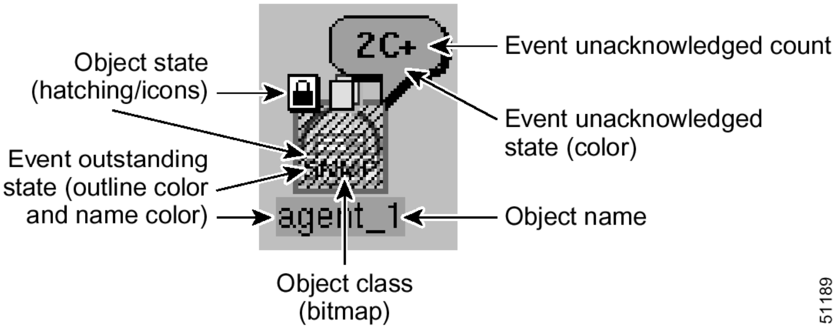
In addition, you can configure notification groups and channels. These notifications provide audible and visual alerts when significant events occur. For usage details, refer to the *Cisco Element Management Framework User Guide*; the following sections are provided only as an orientation.

Using MapViewer to Display Alarms

Each MapViewer object can display the following information about its associated network element:

- Object name
- Object class
- Object state
- Event unacknowledged count
- Event unacknowledged state
- Event outstanding state

Figure 6-1 Information Displayed on an Object



Note The icon displays the most severe event only.

- The icon for the object shows the following information:
  - An event counter is displayed in the balloon.
  - A number indicates the number of the most severe events in the category.
  - A letter indicates the highest unacknowledged event severity in the category.
  - A plus sign appears if there are other less severe, unacknowledged events in the category.
- The object has a colored outline which shows the event status color.

The colors and codes of severities used in Cisco EMF are shown in Table 6-1.

Table 6-1 Alarm Severity Colors and Codes

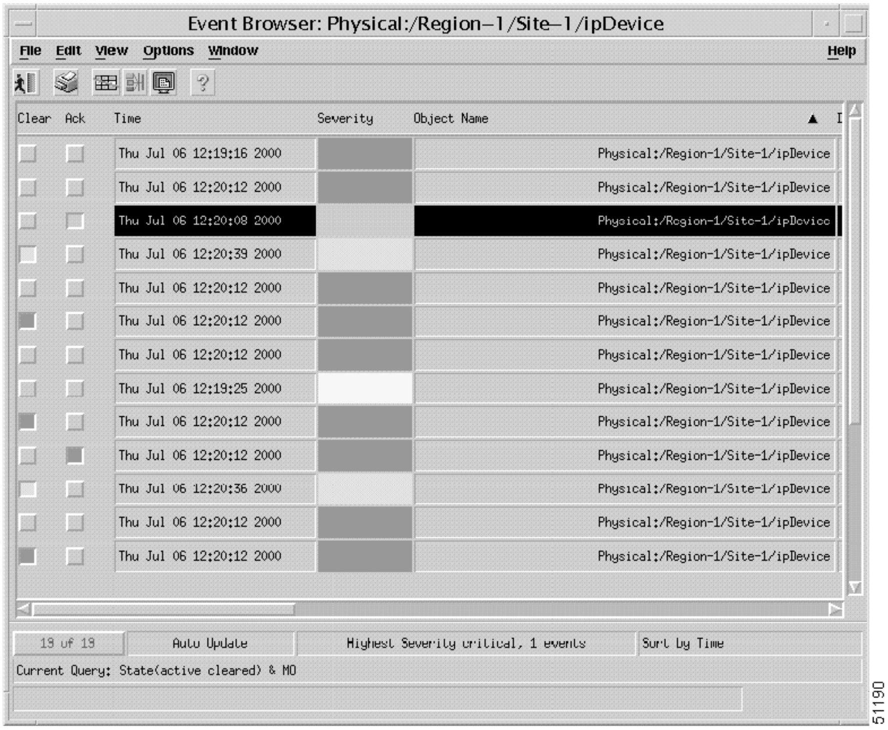
Icon Color	Balloon Code	Severity of Event
Red	C	Critical
Orange	M	Major
Yellow	m	Minor
Cyan	W	Warning
Green	(none)	Normal
White	i	Informational

Event Browser Display

The event status of objects contained in a map can affect the event status of the parent icon. If the event status changes on a map object, the change is propagated to the parent icon. The event status for a parent icon is changed to reflect the most severe event of its children.

In Cisco EMF, when a condition (fault) occurs on a managed object, the system is notified immediately. This notification is shown as an event and can be viewed with the Cisco EMF Event Browser. The Event Browser is opened from the Cisco EMF launchpad. A window similar to the one shown in Figure 6-2 is displayed.

Figure 6-2 Cisco EMF Event Browser



Clear	Ack	Time	Severity	Object Name
☐	☐	Thu Jul 06 12:19:16 2000	▨	Physical:/Region-1/Site-1/ipDevice
☐	☐	Thu Jul 06 12:20:12 2000	▨	Physical:/Region-1/Site-1/ipDevice
☐	☐	Thu Jul 06 12:20:08 2000	░	Physical:/Region-1/Site-1/ipDevice
☐	☐	Thu Jul 06 12:20:39 2000	░	Physical:/Region-1/Site-1/ipDevice
☐	☐	Thu Jul 06 12:20:12 2000	▨	Physical:/Region-1/Site-1/ipDevice
■	☐	Thu Jul 06 12:20:12 2000	▨	Physical:/Region-1/Site-1/ipDevice
☐	☐	Thu Jul 06 12:20:12 2000	▨	Physical:/Region-1/Site-1/ipDevice
☐	☐	Thu Jul 06 12:19:25 2000	□	Physical:/Region-1/Site-1/ipDevice
■	☐	Thu Jul 06 12:20:12 2000	▨	Physical:/Region-1/Site-1/ipDevice
☐	■	Thu Jul 06 12:20:12 2000	▨	Physical:/Region-1/Site-1/ipDevice
☐	☐	Thu Jul 06 12:20:36 2000	░	Physical:/Region-1/Site-1/ipDevice
☐	☐	Thu Jul 06 12:20:12 2000	▨	Physical:/Region-1/Site-1/ipDevice
■	☐	Thu Jul 06 12:20:12 2000	▨	Physical:/Region-1/Site-1/ipDevice

19 of 19 | Auto Update | Highest Severity critical, 1 events | Sort by Time

Current Query: State(active cleared) & MO

The Event Browser enables you to manage the network efficiently; you can list, query, and sort all or some events according to how you want to manage the network.

Note You can view events on Cisco EMF maps; however, only the most severe fault on a managed object is shown on the map icon for that object.

The main panel in the Event Browser window displays a list of events including:

- Object name (the managed resource name associated with the event).
- Time the event was raised.
- Severity of the event (color-coded). Refer to the Table 6-1 for more information.
- Description of the event.

Two indicators, color coded to match the severity of the event, are available to the left of the object name:

- Clear (shows whether an event is active or cleared)
- Ack (shows whether an event is acknowledged or unacknowledged)

Click the **Ack** button to indicate to other users that the fault is being worked on. The button changes to the color of the severity. If for any reason you cannot clear the problem, you can deselect this button so that the event can be reassigned. The **Clear** button is highlighted when the fault has been rectified. Highlighting indicates that the event requires no further attention.

Launching the Event Browser

You launch the Event Browser application using an icon on the Cisco EMF Launchpad. This icon opens the Query Editor window, from which you can specify the type of events to view.

Alternatively, you can right-click on one or more objects in the Map Viewer and then click **Tools > Event Browser**. The Event Browser displays only the events associated with the selected objects.

Viewing Cisco MGM Logs

You can check the log files for significant Cisco MGM and Cisco EMF events. Table 6-2 describes the important logs:

Table 6-2 Log Files

File	Description
<CEMFROOT>/logs/cmgmvCtlr.log	Controller event log
<CEMFROOT>/logs/LoggercmgmvCtlr.log	Cisco MGM-specific log

For more information about Cisco MGM log files, refer to the "Cisco MGM Log Files" section on page A-2.

Trap Management

Cisco MGM recognizes all traps sent from Cisco MGX 8000 Series CVGs. All traps are reported in the Cisco MGM Event Browser. Chassis, card, and line traps are reported in MapViewer.

Registering Traps

Before Cisco MGM can process alarm information, you need to register the traps you want the Cisco MGX 8000 Series CVG or media gateway controller (MGC) to forward to Cisco MGM.

Note Before registering traps, verify that the proper read/write community string is listed for the selected chassis you want to register.

To register traps, perform the following steps:

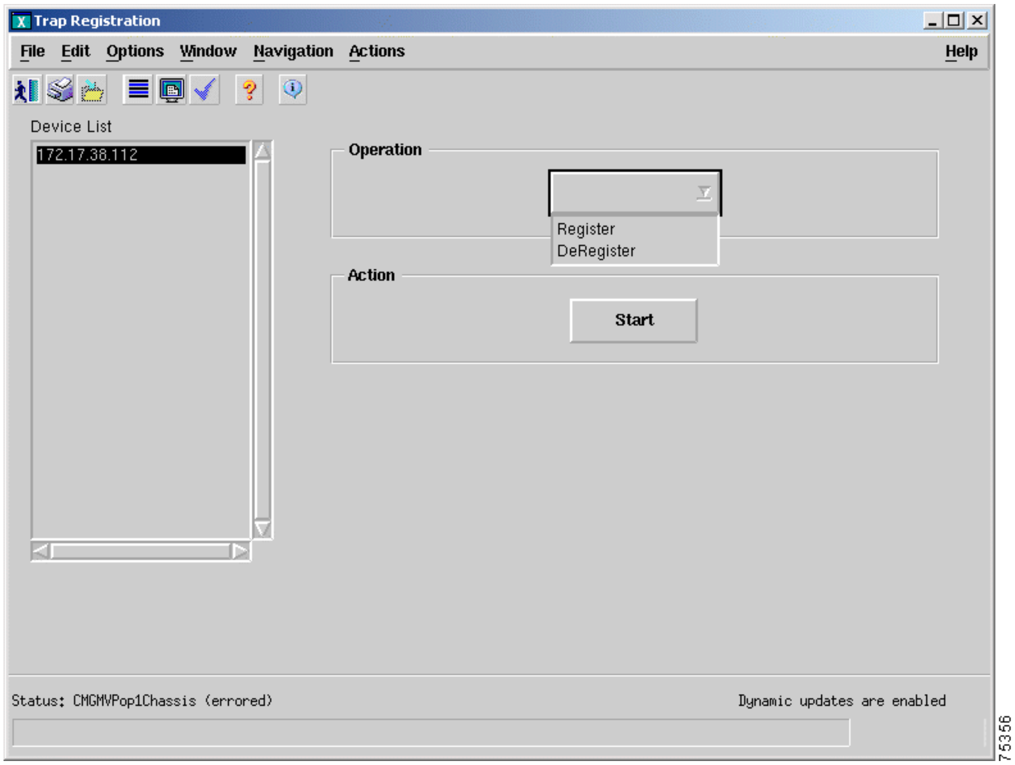
Step 1 Log on to Cisco EMF. The Cisco Element Manager Framework Launchpad screen opens.

Step 2 Click the **Viewer** button. The MapViewer screen opens.

Step 3 Click the tree of objects to display the list of sites and nodes.

Step 4 Right-click the desired site or node and click **Trap Registration**. The Trap Registration window opens. (See Figure 6-3.)

Figure 6-3 Trap Registration



Status: CMGMVPop1Chassis (errored)

Dynamic updates are enabled

Step 5 Select your desired chassis objects from the chassis list.

Step 6 Select **Register** from the Operation pull-down menu.

Note The default pull-down menu is blank. You must click on the pull-down menu to reveal the available options.

Step 7 Click **Start** to execute the operation. A pop-up dialog box indicates the success or failure of the request.

Note For PXM1-based chassis, trap manager aging is set to ENABLE by default. This parameter (set during trap registration) will eventually timeout and MGX will cease to send traps to Cisco MGM. However, Cisco MGM reregisters for traps periodically. Use the CLI command **agetrapmgr** to disable trap manager aging.

Deregistering Traps

To deregister traps using Cisco MGM MapViewer, perform the following steps:

Step 1 Log on to Cisco EMF. The Cisco Element Manager Framework Launchpad screen opens.

Step 2 Click the **Viewer** button. The MapViewer screen opens.

Step 3 Click the tree of objects to display the list of sites and nodes.

Step 4 Right-click the desired site or node and click **Trap Registration**. The Trap Registration window opens. (See Figure 6-3.)

Step 5 Select your desired chassis objects from the chassis list.

Step 6 Click **Deregister** from the Operation pull-down menu.

Note The default pull-down menu is blank. You must click on the pull-down menu to reveal the available options.

Step 7 Click **Start** to execute the operation. A pop-up dialog box indicates the success or failure of the request.

Updating Trap Forwarding

To update forwarding from Cisco MGM to other hosts, follow these steps:

Step 1 Log in as the root user.

Step 2 Change to the directory for scripts.

```
cd <CEMFROOT>/config/scripts/cmgmv
```

Step 3 Run the configuration script.

```
./updCmgmTrapForward
```

Tip To get help, enter **updCmgmTrapForward -h**

The script automatically restarts the trap manager, and the system begins forwarding traps.

Performance Management

Cisco MGX 8000 Series CVGs report performance information for DS1, E1, DS3, and SONET lines. In addition, you can set performance thresholds and assign alarm severities for the reporting gateways.

In addition to Cisco MGM performance management, CiscoView also provides device-specific performance management, including the following information:

- LAPD statistics
- Session set counters
- Session group counters
- RUDP statistics and counters
- SVC statistics counters
- Bearer statistical counters
- HDLC counters
- DSX1 line real time counters

All statistics data is collected in real-time, no historical data is stored.

For detailed information on CiscoView installation and operation, refer to *Using CiscoView 5.4*.

CHAPTER 7

Security

Cisco MGM enforces security with user names and passwords, and manages user accounts individually and in groups. The use of access groups simplifies the process of assigning privileges to individual users because such groups enable you to define a set of privileges for each type of user.

Cisco EMF User Accounts

Cisco EMF enforces security with the following types of accounts.

Table 7-1 Cisco EMF Accounts

Access Level	Account Type	Number of Users	Access Type	Command Groups
1	Administrator	1	Read/Write	All categories
2	User defined	As many as needed	Read/Write	User can only invoke the categories of service defined by the access spec of its user group

From Cisco EMF’s Access application, an administrator can arrange Cisco EMF user accounts in groups. These groups can be used to model user roles; for example, administrators typically set up a user group for administrative users and system operators.

To add, change, or delete user accounts or groups, refer to the *Cisco Element Management Framework User Guide*.

Changing Passwords

You can change your own password. System administrators can change any password.

To make administrative password changes, follow these steps:

Step 1 Open the Access Manager window and select the name of the user whose password is to be changed.

Step 2 From the Edit menu, select **Change Password**. For instance, to change the admin password, select **Change Admin Password**.

Note The **Change Admin Password** option is available only to system administrators.

The Change User Password window opens.

Step 3 Enter the existing password in the Old Password field.

Step 4 Enter a new password in the **New Password** field, and reenter the new password to verify your choice.

Step 5 Click **OK**.

Step 6 If an invalid password is entered or the new password is not verified correctly, an error message is displayed. Click **OK** to try again.

Cisco MGM Community String and Security Configuration

When Cisco MGM communicates with Cisco MGX 8000 Series CVGs, security is enforced with community strings. SNMP communities group workstations and servers that can manage the Cisco MGX 8000 Series CVGs according to their access privileges. A read-only community string is required to perform an SNMP “get” function. A read-write community string is required to perform an SNMP “set” function (can also be used to perform a “get” function.)

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 them.

The following notes pertain to the configuring of community strings for Cisco MGM:

- You need to know the Cisco MGX 8000 Series CVG community strings when configuring Cisco MGM. The read community string you specified for auto discovery is the default read community for all of the managed objects on the Cisco MGX 8000 Series CVG and its children. The default read community for Cisco MGM is public.
- Always use the **SNMP and Security Configuration Dialog** option from the chassis or site level to modify the read/write community string.
- The connection between Cisco MGM and each Cisco MGX 8000 Series CVG has its own community string. You may use identical community strings for each gateway, or you may have different community string values for each managed gateway. The dialog box displays only the last value stored locally.

To configure community strings and security, follow these steps:

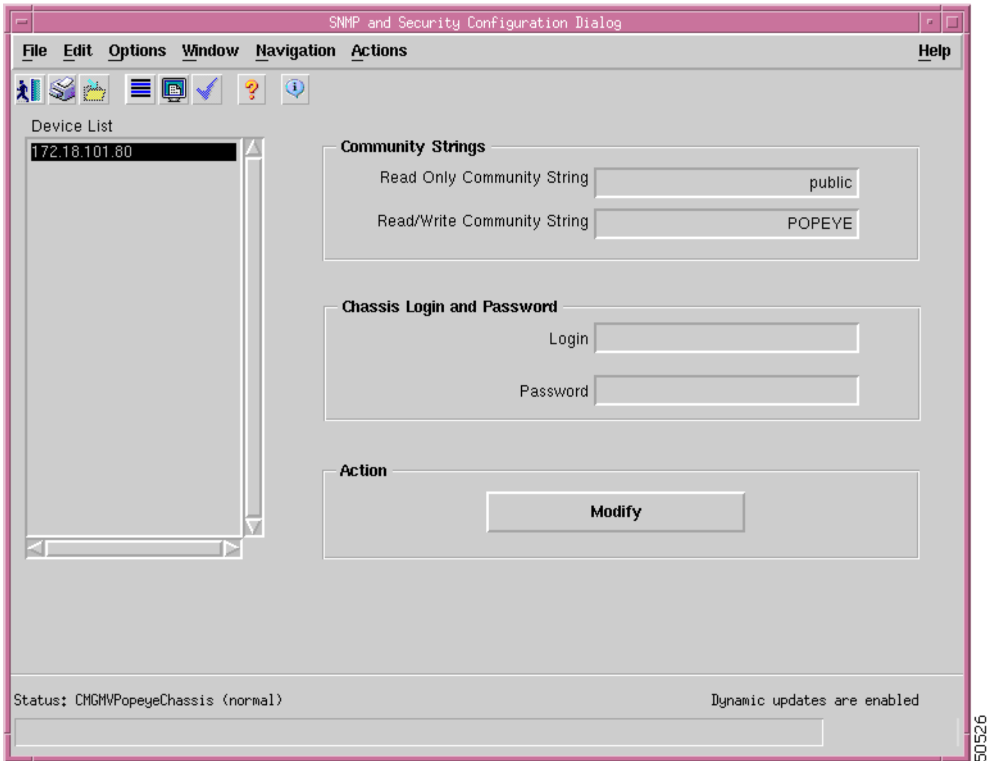
Step 1 Log on to Cisco MGM.

Step 2 On the Cisco EMF Launchpad, click **Viewer**. The Cisco EMF MapViewer opens.

Step 3 Click the object tree, right-click on the desired site or object, and click **SNMP and Security Configuration Dialog**.

The SNMP and Security Configuration window opens. (See Figure 7-1.)

Figure 7-1 SNMP and Security Configuration Dialog



Device List
172.18.101.80

Community Strings
Read Only Community String: public
Read/Write Community String: POPEYE

Chassis Login and Password
Login:
Password:

Action

Status: CMGMVPopeyeChassis (normal)
Dynamic updates are enabled

Note For security reasons, the current chassis password is not displayed.

Step 4 Select one or more IP addresses from the list, using the **Shift** key to select multiple addresses.

Step 5 Modify the default read-only and read-write community strings in the corresponding fields as required.

Note The SNMP read–only community string parameter for PXM1 based chassis is always public on the device, therefore there is no need to change this value on the SNMP and Security Configuration window.

Step 6 Enter the desired chassis login and password values to be used to telnet to the device to issue CLI commands and to transfer data (via FTP or TFTP.)

Note The TFTP function is used when a PXM1-based card is in the chassis while the FTP function is used when a PXM1E or PXM45-based card is in the chassis.

Step 7 Click **Modify**.

A confirmation screen opens that reports successful and unsuccessful configuration attempts.

Step 8 Click **Close**.

Note When subchassis synchronization is first invoked after auto-discovery, Cisco MGM uses the default read-write community string as specified in the UserData.ini file. If the device community string is different from the default read-write community string, objects under cards (lines and sessions) won't be found. In this case, configure the read-write community string of the device in Cisco MGM to match the actual read-write community string of the device, then perform a subchassis synchronization. For information about changing the default read-write community string, refer to the "Inventory Discovery" section on page 4-4.

CHAPTER 8

Media Gateway Controller Integration

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

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

Cisco BTS 10200 Softswitch

Cisco MGM provides the following integration with the Cisco BTS 10200 Softswitch:

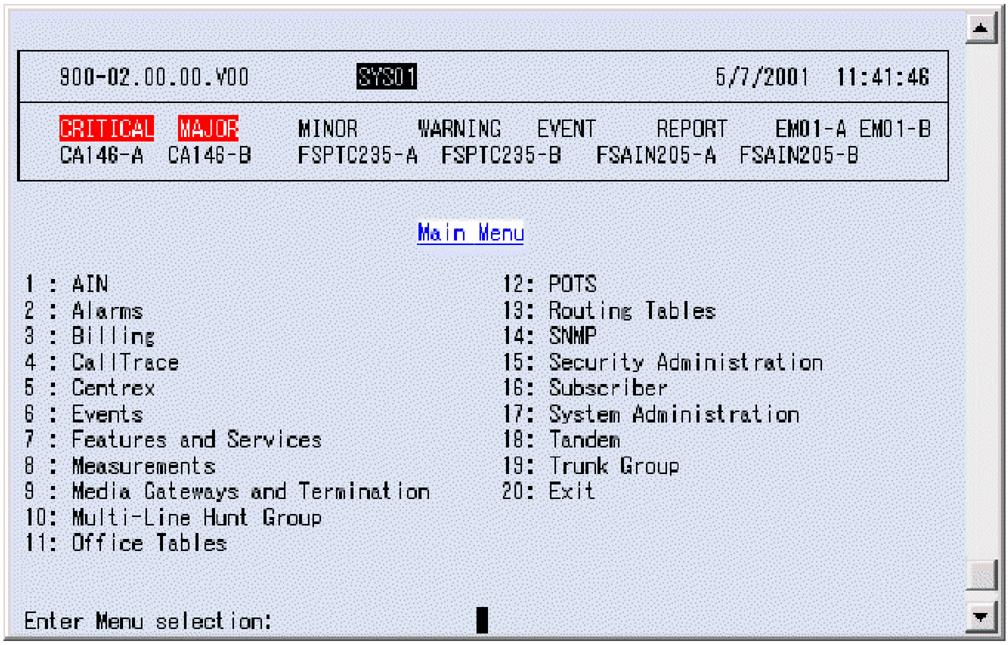
- Auto discovery of Cisco BTS 10200 Softswitch from Cisco MGM auto-discovery window. The BTS MGC is represented as a color-coded icon that can change color to represent the real-time status. The communication link status between Cisco MGM and the BTS 10200 is also reflected by the color-coded icon.
- Ability to launch the BTS 10200 EMS from the BTS icon that is displayed in the MapViewer window.
- Integration of BTS 10200 traps/alarms into the Cisco MGM Event Browser window.
- Ability to launch the BTS document site window from the BTS icon that is displayed on the MapViewer window.

Figure 8-1 shows the main menu of the BTS EMS.

For detailed information about Cisco's BTS 10200 Softswitch, refer to the following Cisco documents:

- *Release Notes for the Cisco BTS 10200, Release 3.3*
- *Cisco BTS 10200 System Description*
- *Cisco BTS 10200 Command Line Interface Reference Guide*
- *Cisco BTS 10200 Application Installation Procedures*
- *Cisco BTS 10200 Softswitch CORBA Installation and Programmer's Guides*
- *Cisco BTS 10200 Cabling Procedures*

Figure 8-1 Cisco BTS 10200 Softswitch EMS



```
 900-02.00.00.V00          SYS01                     5/7/2001   11:41:46

 CRITICAL  MAJOR     MINOR     WARNING   EVENT     REPORT    EM01-A EM01-B
 CA146-A   CA146-B   FSPTC235-A  FSPTC235-B  FSAIN205-A  FSAIN205-B

                                Main Menu

1 : AIN                                 12: POTS
2 : Alarms                              13: Routing Tables
3 : Billing                             14: SNMP
4 : CallTrace                           15: Security Administration
5 : Centrex                             16: Subscriber
6 : Events                              17: System Administration
7 : Features and Services               18: Tandem
8 : Measurements                          19: Trunk Group
9 : Media Gateways and Termination        20: Exit
10: Multi-Line Hunt Group
11: Office Tables

Enter Menu selection:
```

Configuring Cisco BTS Integration

To provide Cisco MGM with access to the Cisco BTS EMS, you need to install the Cisco MGM BTS server. If you are using a remote Cisco MGM client to connect to the Cisco MGM server, you also need to install the Cisco MGM BTS client to the remote workstation.

Installing the Cisco MGM BTS Server Package

To install the Cisco MGM BTS server package, perform the following steps:

Step 1 Log in to the Cisco EMF server as the root user.

Step 2 Change to the appropriate package directory on the CD ROM.

```
cd /cdrom/cmgm3.0pkg/cmgmv
```

Step 3 Start the installation script.

```
./cmgmvinstall
```

Step 4 Follow the onscreen instructions, considering the following guidelines:

When prompted for the type of installation, select the **bts server package** option.

The Cisco MGM BTS plugin automatically starts on Cisco EMF.

Step 5 Check the installation log for errors. The log file is in the following location:

```
/var/adm/Atlantech/avinstall/btspkg_Server_Package/logfile
```

Installing the Cisco MGM BTS Client Package

To install the Cisco MGM BTS client package, perform the following steps:

Step 1 Log in to Cisco EMF as the root user.

Step 2 Change to the appropriate package directory on the CD ROM.

```
cd /cdrom/cmgm3.0pkg/cmgmv
```

Step 3 Start the installation script.

```
./cmgmvinstall
```

Step 4 Follow the onscreen instructions, considering the following guidelines:

When prompted for the type of installation, select the **bts client package** option.

The Cisco MGM BTS plugin automatically starts on Cisco EMF.

Step 5 Check the installation log for errors. The log file is in the following location:

```
/var/adm/Atlantech/avinstall/btspkg_Client_Package/logfile
```

Launching the Cisco BTS EMS

To launch the Cisco BTS EMS package, perform the following steps:

Step 1 Log on to Cisco EMF.

Step 2 Click the Viewer button. The Cisco MGM MapViewer screen opens.

Step 3 Expand the tree of objects to display the list of sites and nodes.

Step 4 Right click on the Cisco BTS icon, then select **Tools > Launch BTS EMS.**

Launching Cisco BTS Documentation

To launch the Cisco BTS documentation, perform the following steps:

Step 1 Log on to Cisco EMF.

Step 2 Click the Viewer button. The Cisco MGM MapViewer screen opens.

Step 3 Expand the tree of objects to display the list of sites and nodes.

Step 4 Right click on the Cisco BTS icon, then select **Tools > Launch BTS DOC.**

Monitoring Cisco BTS Traps and Alarms

You can use the Cisco EMF Event Browser to monitor Cisco BTS traps and alarms. For more information about the Event Browser, refer to Chapter 6, “Fault and Performance Management.”

Uninstalling Cisco MGM BTS Server or Client Packages

When you uninstall a server package, you also remove the client from the same host. On a client machine, the script just removes the client software.

Note Before uninstalling a server or client package, backup your Cisco EMF database according to the procedures described in the *Cisco Element Management Framework Installation and Administration Guide,* Chapter, 10, “Cisco EMF Database Backup and Restore”.

To remove the Cisco MGM BTS packages, follow these steps:

Step 1 Log in as the root user.

Step 2 Change to the script directory.

```
cd <CEMFROOT>/config/scripts/cmgmv
```

Step 3 Run the uninstallation script.

```
./cmgmvinstall -r
```

Select the BTS EMS option.

Step 4 If you receive a “port not ready” message, repeat step 3. If the problem persists, contact technical support.

Step 5 Check the installation log for errors. The server log file is in the following location:

```
/var/adm/Atlantech/avinstall/btspkg_Server_Package/logfile
```

The client log file is in the following location:

```
/var/adm/Atlantech/avinstall/btspkg_Client_Package/logfile
```

Tekelec VX*i* Media Gateway Controller

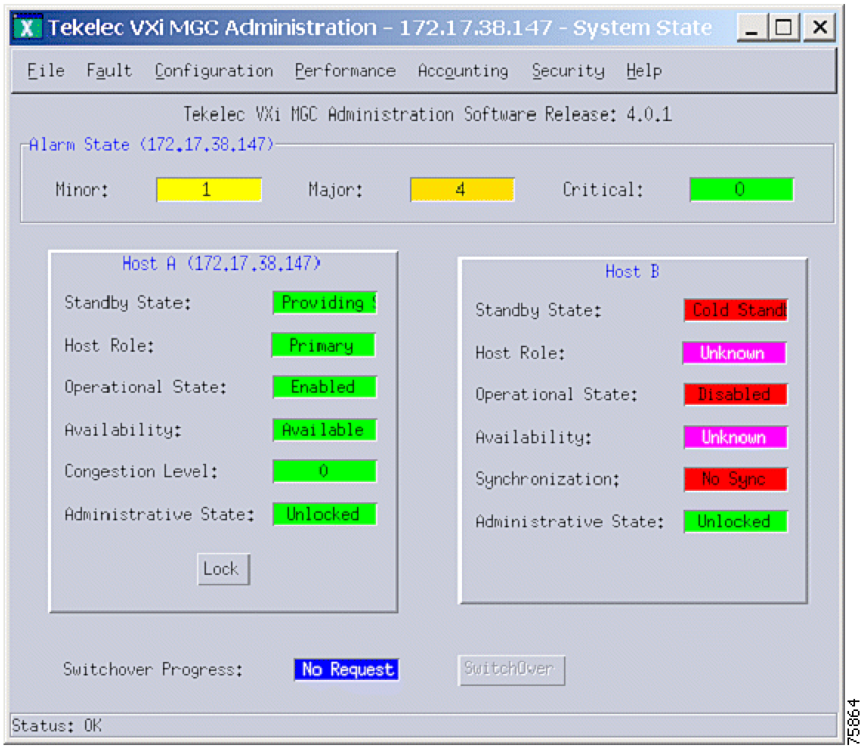
Cisco MGM provides the following integration with the Tekelec VX*i* Media Gateway Controller (MGC):

- Auto discovery of VX*i* MGCs from Cisco MGM auto discovery window
- Ability to launch the VX*i* MGC EMS from the TEKELEC icon that is displayed in the MapViewer window. The Tekelec VX*i* MGC is represented as a color-coded icon that can change color to represent the real-time status of the Tekelec VX*i* MGC. The communication link status between Cisco MGM and the Tekelec VX*i* MGC is also reflected by the color-coded icon.
- Inclusion of Tekelec VX*i* traps/alarms into the Cisco MGM Event Browser window.

Figure 8-2 shows the main menu of the Tekelec VX*i* MGC EMS.

For detailed information about the Tekelec VX*i* Media Gateway Controller, refer to the Tekelec web site at http://www.tekelec.com/

Figure 8-2 Tekelec VXi Media Gateway Controller (MGC) EMS



Tekelec VXi MGC Administration Software Release: 4.0.1

Alarm State (172.17.38.147)

Minor: 1 Major: 4 Critical: 0

Host A (172.17.38.147)

Standby State: Providing S
Host Role: Primary
Operational State: Enabled
Availability: Available
Congestion Level: 0
Administrative State: Unlocked

Host B

Standby State: Cold Standb
Host Role: Unknown
Operational State: Disabled
Availability: Unknown
Synchronization: No Sync
Administrative State: Unlocked

Switchover Progress: No Request

Status: OK

Configuring Tekelec VX*i* MGC Integration

To provide Cisco MGM with access to the Tekelec VX*i* EMS, you need to install the Cisco MGM Tekelec VX*i* server. If you are using a remote Cisco MGM client to connect to the Cisco MGM server, you also need to install the Cisco MGM Tekelec VX*i* client to the remote workstation.

Installing the Cisco MGM Tekelec VX*i* Server Package

Note Before installing the Tekelec package in Cisco MGM, the Tekelec EMS Java Client Package must be installed. For more information about installing the java client package, refer to the Tekelec web site at http://www.tekelec.com/

To install the Cisco MGM Tekelec VX*i* server package, perform the following steps:

Step 1 Log in to the Cisco EMF server as the root user.

Step 2 Change to the appropriate package directory on the CD ROM.

```
cd /cdrom/cmgm3.0pkg/cmgmv
```

Step 3 Start the installation script.

```
./cmgmvinstall
```

Step 4 Follow the onscreen instructions, considering the following guidelines:

When prompted for the type of installation, select the **tekelec server package** option.

The Cisco MGM Tekelec VX*i* plugin automatically starts on Cisco EMF.

Step 5 Check the installation log for errors. The log file is in the following location:

```
/var/adm/Atlantech/avinstall/tekpkg_Server_Package/logfile
```

Installing the Cisco MGM Tekelec VX*i* Client Package

To install the Cisco MGM Tekelec VX*i* client package, perform the following steps:

Step 1 Log in to Cisco EMF as the root user.

Step 2 Change to the appropriate package directory on the CD ROM.

```
cd /cdrom/cmgm3.0pkg/cmgmv
```

Step 3 Start the installation script.

```
./cmgmvinstall
```

Step 4 Follow the onscreen instructions, considering the following guidelines:

When prompted for the type of installation, select the **tekelec client package** option.

The Cisco MGM Tekelec VX*i* plugin automatically starts on Cisco EMF.

Step 5 Check the installation log for errors. The log file is in the following location:

```
/var/adm/Atlantech/avinstall/tekpkg_Client_Package/logfile
```

Launching the Tekelec VX*i* EMS

To launch the Tekelec VXi EMS package, perform the following steps:

Step 1 Log on to Cisco EMF.

Step 2 Click the Viewer button. The Cisco MGM MapViewer screen opens.

Step 3 Expand the tree of objects to display the list of sites and nodes.

Step 4 Right click on the Tekelec icon, then select **Tools > Launch TEKELEC EMS (startVXi).**

Monitoring Tekelec VX*i* Traps and Alarms

You can use the Cisco EMF Event Browser to monitor Tekelec VX*i* traps and alarms. For more information about the Event Browser, refer to Chapter 6, “Fault and Performance Management.”

Uninstalling Cisco MGM Tekelec VX*i* Server or Client Packages

When you uninstall a server package, you also remove the client from the same host. On a client machine, the script just removes the client software.

Note Before uninstalling a server or client package, backup your Cisco EMF database according to the procedures described in the *Cisco Element Management Framework Installation and Administration Guide,* Chapter, 10, "Cisco EMF Database Backup and Restore".

To remove the Cisco MGM Tekelec VX*i* packages, follow these steps:

Step 1 Log in as the root user.

Step 2 Change to the script directory.

```
cd <CEMFROOT>/config/scripts/cmgmv
```

Step 3 Run the uninstallation script.

```
./cmgmvinstall -r
```

Select the Tekelec EMS option.

Step 4 If you receive a "port not ready" message, repeat step 3. If the problem persists, contact technical support.

Step 5 Check the installation log for errors. The server log file is in the following location:

```
/var/adm/Atlantech/avinstall/tekpkg_Server_Package/logfile
```

The client log file is in the following location:

```
/var/adm/Atlantech/avinstall/tekpkg_Client_Package/logfile
```

NexVerse ipVerse ControlSwitch

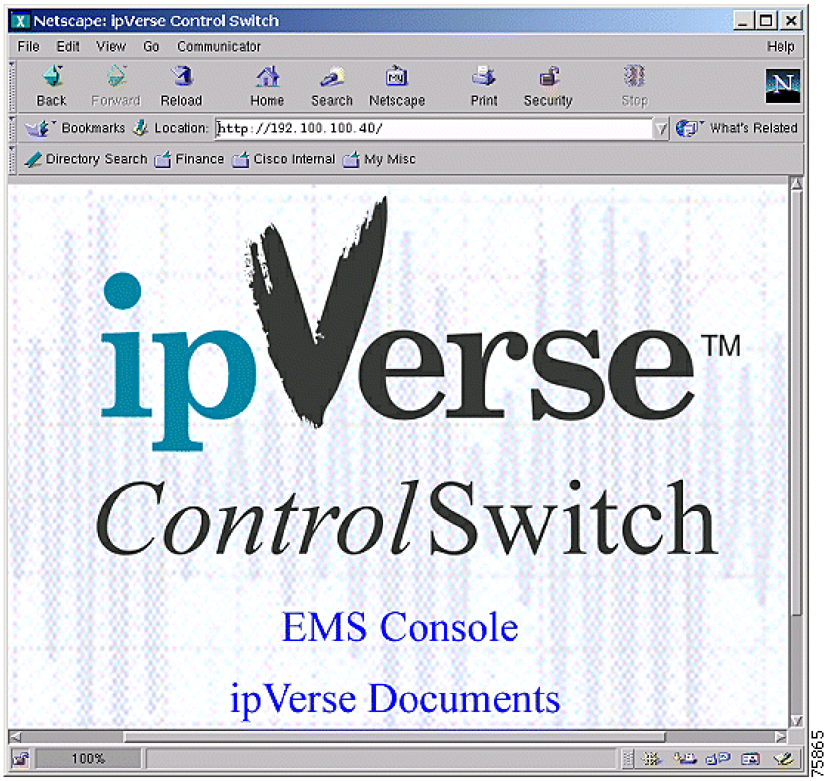
Cisco MGM provides the following integration with the NexVerse ipVerse ControlSwitch EMS:

- Auto discovery of NexVerse ipVerse MGC nodes
- Ability to launch the NexVerse ipVerse EMS from the NexVerse icon that is displayed in the MapViewer window
- Integration of NexVerse ipVerse traps and alarms into the Cisco MGM Event Browser window

Figure 8-3 shows the main menu of the NexVerse ipVerse EMS.

For detailed information about the NexVerse ipVerse ControlSwitch, refer to the NexVerse web site at http://www.nexverse.com/

Figure 8-3 NexVerse ipVerse ControlSwitch EMS


Netscape: ipVerse Control Switch
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://192.100.100.40/
What's Related
Directory Search Finance Cisco Internal My Misc
ipVerse™
ControlSwitch
EMS Console
ipVerse Documents
100%
75865

Configuring NexVerse ipVerse Integration

To provide Cisco MGM with access to the NexVerse ipVerse EMS, you need to install the Cisco MGM NexVerse ipVerse server. If you are using a remote Cisco MGM client to connect to the Cisco MGM server, you also need to install the Cisco MGM NexVerse ipVerse client to the remote workstation.

Installing the Cisco MGM NexVerse ipVerse Server Package

To install the Cisco MGM NexVerse ipVerse server package, perform the following steps:

Step 1 Log in to the Cisco EMF server as the root user.

Step 2 Change to the appropriate package directory on the CD ROM.

```
cd /cdrom/cmgm3.0pkg/cmgmv
```

Step 3 Start the installation script.

```
./cmgmvinstall
```

Step 4 Follow the onscreen instructions, considering the following guidelines:

When prompted for the type of installation, select the **ipverse server package** option.

The Cisco MGM NexVerse ipVerse plugin automatically starts on Cisco EMF.

Step 5 Check the installation log for errors. The log file is in the following location:

```
/var/adm/Atlantech/avinstall/ipvrspkg_Server_Package/logfile
```

Installing the Cisco MGM NexVerse ipVerse Client Package

To install the Cisco MGM NexVerse ipVerse client package, perform the following steps:

Step 1 Log in to Cisco EMF as the root user.

Step 2 Change to the appropriate package directory on the CD ROM.

```
cd /cdrom/cmgm3.0pkg/cmgmv
```

Step 3 Start the installation script.

```
./cmgmvinstall
```

Step 4 Follow the onscreen instructions, considering the following guidelines:

When prompted for the type of installation, select the **ipverse client package** option.

The Cisco MGM NexVerse ipVerse plugin automatically starts on Cisco EMF.

Step 5 Check the installation log for errors. The log file is in the following location:

```
/var/adm/Atlantech/avinstall/ipvrspkg_Client_Package/logfile
```

Launching the NexVerse ipVerse EMS

To launch the NexVerse ipVerse EMS package, perform the following steps:

Step 1 Log on to Cisco EMF.

Step 2 Click the Viewer button. The Cisco MGM MapViewer screen opens.

Step 3 Expand the tree of objects to display the list of sites and nodes.

Step 4 Right click on the NexVerse icon, then select **Launch NexVerse EMS.**

Monitoring NexVerse ipVerse Traps and Alarms

You can use the Cisco EMF Event Browser to monitor NexVerse ipVerse traps and alarms. For more information about the Event Browser, refer to Chapter 6, “Fault and Performance Management.”

Uninstalling Cisco MGM NexVerse ipVerse Server or Client Packages

When you uninstall a server package, you also remove the client from the same host. On a client machine, the script just removes the client software.

Note Before uninstalling a server or client package, backup your Cisco EMF database according to the procedures described in the *Cisco Element Management Framework Installation and Administration Guide,* Chapter, 10, "Cisco EMF Database Backup and Restore".

To remove the Cisco MGM NexVerse ipVerse packages, follow these steps:

Step 1 Log in as the root user.

Step 2 Change to the script directory.

```
cd <CEMFROOT>/config/scripts/cmgmv
```

Step 3 Run the uninstallation script.

```
./cmgmvinstall -r
```

Select the NexVerse EMS option.

Step 4 If you receive a "port not ready" message, repeat step 3. If the problem persists, contact technical support.

Step 5 Check the installation log for errors. The server log file is in the following location:

```
/var/adm/Atlantech/avinstall/ipvrspkg_Server_Package/logfile
```

The client log file is in the following location:

```
/var/adm/Atlantech/avinstall/ipvrspkg_Client_Package/logfile
```

Cisco EMF Coresidency

Multiple EMs can be installed onto a single Cisco EMF server, thereby allowing multi–device and multi–vendor management from a single system. The following packages are compatible to create a coresident network management system:

- Cisco Element Management Framework (Cisco EMF), Release 3.2 Service Pack 4 or greater
- Cisco Media Gateway Manager (Cisco MGM), version 3.0
- Cisco Media Gateway Controller (MCG) Node Manager (Cisco MNM), version 2.3
- Cisco Universal Gateway Manager (Cisco UGM), version 2.1

The following sections provide specific coresidency details for the Cisco MGM application:

- Coresidence Hardware Requirements
- Coresidence Software Requirements
- Preparing the System for Coresident Applications
- Installing Coresident EM Applications
- Working with Coresident EM Applications

Coresidence Hardware Requirements

The following table details the hardware requirements for Cisco MGM coresidence. All coresident systems must meet these requirements in order to support coresidency with Cisco MGM.

Table 9-1 Coresidence Hardware Requirements

	Cisco MGM Server		
Resource	**Small Installation**[1]	**Large Installation**[2]	**Cisco MGM Client**
Workstation	Sun Netra t1400[3]	Sun Netra t1400[3]	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, each one 18 GB or larger	Four hard disks, each one 18 GB or larger	One hard disk, 9 GB or larger
Processor	2 x 440 MHz	4 x 440MHz	440 MHz
Swap space	5 GB[4]	9 GB[4]	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] Up to 10 fully-loaded MGX CVGs

[2] Between 10 to 50 fully-loaded MGX CVGs

[3] Netra platforms are supported, but not required. Alternate platforms that have been tested include: Sun Ultra 60, 220r, 420r, 280r, and Netra 20. Sun UltraSPARC III servers and desktops are also supported by Cisco MGM.

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

Coresidence Software Requirements

The following table details the software requirements for Cisco MGM coresidence. All coresident systems must meet these requirements in order to support coresidency with Cisco MGM. Note that all of the following software packages use the Solaris 8 operating system.

Table 9-2 Coresidence Software Requirements

Software Package	Version
Cisco EMF	3.2, Service Pack 4 or greater
Cisco MGM	3.0
Cisco MNM	2.3
Cisco UGM	2.1
CiscoView	5.4

Preparing the System for Coresident Applications

Prior to installing coresident EM applications, it is recommended that you perform the following tasks:

- Installing Cisco EMF
- Initializing the Cisco EMF System
- Starting a Cisco EMF User Session
- Partitioning the Hard Disk
- Initializing the Cisco EMF System

Installing Cisco EMF

In order to install coresident EM applications such as Cisco MGM, Cisco MNM, and Cisco UGM, the framework application must be installed. Once the base Cisco EMF application is installed, the applicable Cisco EMF patches must be installed.

To install Cisco EMF, follow these steps:

Step 1 Install the Cisco EMF v3.2 software.

For further information on installing the Cisco EMF v3.2 software, see the *Cisco Element Management Framework Installation and Administration Guide* and related release notes.

Step 2 Install the Cisco EMF v3.2, Service Pack 4 software.

For details on installing the Cisco EMF v3.2, Service Pack 4 software, see the *Cisco Element Management Framework Installation and Administration Guide* and related release notes.

Initializing the Cisco EMF System

Before logging into and using the Cisco EMF system, the associated processes must be initialized. Starting the Cisco EMF application also initiates the installed EM application processes.

To start the Cisco EMF system, follow these steps.

Step 1 Log into the workstation as the root user.

Step 2 Start the Cisco EMF system by entering the following command in a terminal window:

```
CEMF_ROOT/bin/cemf start
```

(Replace *CEMF_ROOT* with the name of the directory where Cisco EMF is installed.)

The Cisco EMF and the available EM processes initiate.

Starting a Cisco EMF User Session

Starting a Cisco EMF user session automatically begins a user session for the available EM(s) as well.

To start a Cisco EMF user session, follow these steps:

Step 1 Log into the workstation.

Step 2 Ensure that the Cisco EMF process is running.

For further information, see the preceding section.

Step 3 To start a Cisco EMF user session, enter the following in a terminal window:

```
CEMF_ROOT/bin/cemf session
```

(Replace *CEMF_ROOT* with the name of the directory where Cisco EMF is installed.)

Step 4 Enter the appropriate Cisco EMF user name and password. (The default user name and password are required for the initial login by the system administrator.)

The Cisco EMF application launches. For information on using the Cisco EMF application, see the *Cisco Element Management Framework Administration and Installation Guide*, *Cisco Element Management Framework User Guide*, and related release notes.

Partitioning the Hard Disk

A large amount of data can be expected with the addition of coresident network management systems. In anticipation of the expected Cisco EMF database growth, it is recommended that you perform raw file system (RAWFS) hard disk partitioning before installing the coresident EM packages.

For detailed steps on partitioning the hard disk, see the *Cisco Element Management Framework Installation and Administration Guide*.

Installing CiscoView Applications

The CiscoView application is an installation prerequisite for the Cisco MGM and the Cisco UGM packages. The CiscoView application may be installed on the local Cisco EMF server or a remote server. Following the CiscoView installation, integration of security parameters and installation of device–specific packages are required. If the CiscoView server is the local Cisco EMF server, security parameter integration and device package installation occurs automatically through the EM installation. If the CiscoView server is a remote server, manual execution of available script files is required.

To install CiscoView, follow these steps:

Step 1 Install the CiscoView 5.4 software on the local Cisco EMF server or a remote server.

For further information on installing the CiscoView 5.4 application, see the *Installation and Setup Guide for CiscoView 5.4*.

Step 2 If the CiscoView server is installed on a remote workstation, execute the required CiscoView scripts on the CiscoView server.

For details on running CiscoView scripts, see the "Installing CiscoView Applications" section on page 2-8 of this guide.

Installing Coresident EM Applications

Once the appropriate version of Cisco EMF software is installed, installation of the coresident applications may take place. Note that the EM installation type, server or client, must match that of the installed Cisco EMF application on the particular machine. The installation process is automated to ensure that the compatible EM package is installed.

To establish a coresident network management system, perform the following tasks as applicable:

- Installing Cisco Media Gateway Manager
- Installing Cisco MGC Node Manager
- Installing Cisco Universal Gateway Manager

Installing Cisco Media Gateway Manager

Before installing Cisco MGM server or client software, configuration of the /etc/hosts files must occur. Once configuration of the /etc/hosts files has taken place, the appropriate Cisco MGM software package may be installed.

The Cisco MGM package provides an integrated connection to management interfaces through supported media gateway controllers (MGCs). Following successful installation of Cisco MGM, installation of supported MGCs may occur.

The following procedure provides a summary of the installation process. For complete details regarding Cisco MGM installation, see Chapter 2, "Installation," of this guide.

To install Cisco MGM, follow these steps:

Step 1 Ensure that the appropriate Cisco EMF software package, version, and patches have been installed on the workstation where the EM software is to be installed by entering the following command in a terminal window:

```
cemf install -show
```

Step 2 Configure the /etc/hosts files on the server or client workstation.

Details regarding configuring /etc/hosts files are available in the"Configuring /etc/hosts Files" section on page 2-6.

Step 3 Install the Cisco MGM v3.0 server or client package on the workstation.

For detailed instructions on installing the Cisco MGM server package, see the "Installing the Cisco MGM Server" section on page 2-9.

For detailed instructions on installing the Cisco MGM client package, see the "Installing Cisco MGM Clients" section on page 2-11.

Step 4 Install the following supported MGCs:

- Cisco BTS 10200 Softswitch
- Tekelec VX*i* Media Gateway Controller
- NexVerse ipVerse Control Switch

For further information on MGCs and detailed instructions on installing the Cisco MGM supported MGCs, see Chapter 8, "Media Gateway Controller Integration," of this guide.

Step 5 Upon completion of the installation process, verify the success of the installation and status of the running processes by entering the following in a terminal window:

- To verify the success of the installation, enter the following in a terminal window:

  ```
  cemf install -show cmgmvpkg_Server_Package
  ```

- To view the status of the running processes, enter the following in a terminal window:

  ```
  CEMF_ROOT/cemf/bin/cemf query
  ```

  (Replace *CEMF_ROOT* with the name of the directory where Cisco EMF is installed.)

  Ensure that the cmgmvCtlr controller is listed in the results which display.

Installing Cisco MGC Node Manager

Installing the Cisco MNM package requires that the installation of a Cisco MGC host provisioning tool has occurred. The host provisioning tool implemented depends on the installed PSTN Gateway software version. If the installed PSTN Gateway software version is 7.4.11, 7.4.12, or 9 (or higher), the Cisco Voice Services Provisioning Tool (VSPT) is available. If the installed PSTN Gateway software version is 7.4.11 or 7.4.12, the Cisco MGC Manager (CMM) host provisioning tool is available.

Once a host provisioning tool is installed, the appropriate Cisco MNM package, server or client, may be installed.

The following procedure provides a summary of the installation process. For complete details regarding Cisco MNM installation, see the *Cisco Media Gateway Controller Node Manager User's Guide*.

To install Cisco MNM, follow these steps:

Step 1 Ensure that the appropriate Cisco EMF software package, version, and patches have been installed on the workstation where the EM software is to be installed by entering the following command in a terminal window:

```
cemf install -show
```

Step 2 Install the appropriate Cisco MGC host provisioning tool as follows:

- If running PSTN Gateway software version 7.4.11, 7.4.12, or 9 (or higher), install the Cisco VSPT.
- If running PSTN Gateway software version 7.4.11 or 7.4.12, install the CMM and use the provisioning window.

  Note that the CMM provisioning feature is not available to PSTN Gateway software version 9 or higher.

For detailed instructions on installing an available Cisco MGC host provisioning tools, see the *Cisco Media Gateway Controller Node Manager 2.3 User Guide* and related release notes.

Step 3 Install the Cisco MNM v2.3 server or client package on the workstation.

For further information on installing the Cisco MNM server or client package, see the *Cisco Media Gateway Controller Node Manager 2.3 User Guide* and related release notes.

Step 4 Upon completion of the installation process, verify the success of the installation and status of the running processes by entering the following in a terminal window:

- To verify the success of the installation, enter the following in a terminal window:

  ```
  cemf install -show mgcEM
  cemf install -show hostEM
  ```

- To view the status of the running processes, enter the following in a terminal window:

  ```
  CEMF_ROOT/cemf/bin/cemf query
  ```

  (Replace *CEMF_ROOT* with the name of the directory where Cisco EMF is installed.)

  Ensure that the following controllers are listed in the results which display:

  - hostController
  - mgcController
  - mgcTrapProcessor

Installing Cisco Universal Gateway Manager

The following procedure provides a summary of the installation process. For complete details regarding Cisco UGM installation, see the *Cisco UGM Installation, Upgrade, and Troubleshooting Guide*.

To install Cisco UGM, follow these steps:

Step 1 Ensure that the appropriate Cisco EMF software package, version, and patches have been installed on the workstation where the EM software is to be installed by entering the following command in a terminal window:

```
cemf install -show
```

Step 2 Download the Java plug-in and install.

To determine the specific Java plug-in required, see the *Using CiscoView 5.4* documentation.

For additional information on installing the Java plug-in, see the *Cisco Universal Gateway Manager Installation, Upgrade, and Troubleshooting Guide, Version 2.1* and related release notes.

Step 3 Install the Cisco UGM v2.1 server or client package on the workstation.

For further information on installing the Cisco UGM server or client package, see the *Cisco Universal Gateway Manager Installation, Upgrade, and Troubleshooting Guide, Version 2.1*and related release notes.

Step 4 Upon completion of the installation process, verify the success of the installation and status of the running processes by entering the following in a terminal window:

- To verify the success of the installation, enter the following in a terminal window:

  ```
  cemf install -show mgcEM
  cemf install -show hostEM
  ```

- To view the status of the running processes, enter the following in a terminal window:

  ```
  CEMF_ROOT/cemf/bin/cemf query
  ```

  (Replace *CEMF_ROOT* with the name of the directory where Cisco EMF is installed.)

  Ensure that the following controllers are listed in the results which display:

  - ASMainCtrl
  - IOSConfigCtrl
  - ASFaultStandAlone

Working with Coresident EM Applications

Similar to getting started using independent (i.e., non–coresident) EM applications, essential tasks must take place in order to begin managing the network through coresident EM applications including:

- Enabling the privileged password (as necessary)
- Configuring the Ethernet port on the device (as necessary)
- Configuring SNMP on the network devices (as necessary)
- Ensuring that the devices accept Telnet sessions (as necessary)
- Enabling traps
- Setting up a TFTP Server

Network objects may now be deployed. Again, as with independent EM applications, community strings and device passwords must be set within the EM to enable communication with each device to be managed. Once communication parameters are set, objects may be discovered and Fault, Configuration (Accounting), Performance, and Security (FC[A]PS) management may begin.

For details on performing these tasks, see the appropriate installation, administration, and/or user documentation for the applicable EM application. For a full listing of the related documentation, see the "Coresidence Related Documentation" section on the following page.

Limitations

When using a Cisco MGM, Cisco MNM, and Cisco UGM coresident system, the following limitations exist:

- Object Discovery—Different patterns of discovery are implemented for each application. Discovered Cisco MGM objects display under the Physical view. The Physical view name cannot be customized.
- Viewing Device Properties:
  - Cisco MGM—Select the chassis object, then right–click and choose **Tools > Object Configuration**
  - Cisco MNM—Select the chassis object, then right–click and choose **Properties**
- Monitored Performance Attribute Names:
  - Cisco MGM—Attributes reflect the MIB object title
  - Cisco MNM—Attributes are represented in English
  - Cisco UGM—Attributes reflect the MIB object title
- Modifying the level of debugging:
  - Cisco MNM—Enter the following changes:

    In the hostController.ini file, add **loggingLevelMask=15**

    In the mgcTrapProcessor.ini file, add **loggingLevelMask=15**
  - Cisco UGM—From the Map Viewer window, select **LoggingConfiguration**
- Exporting Inventory, Alarm, and Performance data—
  - Cisco MNM—Not supported
  - Cisco UGM—May export either all data or no data

Coresidence Related Documentation

- Cisco Element Management Framework
  - *Quick Start Guide Cisco EMF Version 3.2 SP4*
    Cisco Element Manager November 2002 Upgrade
  - *Cisco Element Management Framework Installation and Administration Guide Version 3.2 Service Pack 4 (Cisco Element Manager November 2002 Upgrade)*
  - *Cisco Element Management Framework User Guide Version 3.2 Service Pack 4 (Cisco Element Manager November 2002 Upgrade)*
  - *Release Notes for Cisco Element Management Framework v3.2 Service Pack 4*
    Cisco Element Manager November 2002 Upgrade

- Cisco Media Gateway Manager
  - *Release Notes for Cisco Media Gateway Manager, Release 3.0*
  - *Cisco Media Gateway Manager User Guide, Release 3.0*

- Cisco MGC Node Manager
  - *Release Notes for Cisco Media Gateway Controller Node Manager Release 2.3*
  - *Cisco Media Gateway Controller Node Manager User's Guide Release 2.3(1)*

- Cisco Universal Gateway Manager
  - *Release Note for Cisco Universal Gateway Manager, Version 2.1*
  - *Cisco UGM Installation, Upgrade, and Troubleshooting Guide*, Version 2.1
  - *Cisco UGM User Guide*, Version 2.1

- CiscoView 5.4
  - *Release Notes for CiscoView 5.4*
  - *Installation and Setup Guide for CiscoView 5.4*
  - *Using CiscoView 5.4*

APPENDIX A

Cisco MGM Server Configuration Files

The Cisco MGM server software stores a number of configuration files that you can use to select properties and change default values used in Cisco MGM operation. You can edit the files listed in this appendix using a standard UNIX text editor.

cmgmvCtlrUserData.ini

The cmgmvCtlrUserData.ini file is located at:

<CEMFROOT>/config/init/cmgmvCtlrUserData.ini

Configuration Save and Restore

You can change Configuration Save and Restore defaults in the cmgmvCtrlUserData.ini file. The following values can be changed:

CMGMVConfigSaveDir—Root directory location; default value is <CEMFROOT>/..

CMGMVConfigSaveTimeout—tftp or telnet timeout in seconds; default value is 1800 seconds

CMGMConfigSaveMaxnum—Maximum number of concurrent tftp sessions; default value is 2

Software Download

You can change Software Download defaults in the cmgmvCtrlUserData.ini file. The following values can be changed:

CMGMVImageDownloadTimeout—tftp timeout in seconds; default value is 1800 seconds

CMGMVImageDownloadMaxnum—Maximum number of concurrent tftp sessions; default value is 2

CMGMVImageDownloadTftpDelay—Duration between tftp retries in seconds; default value is 60

CMGMVImageDownloadTftpRetry—tftp retries; default value is 2

SNMP Community Strings

You can change the following SNMP Community String default in the cmgmvCtrlUserData.ini file:

MgxRWCommunityString1—Read-Write MGX chassis community for PXM1-based devices; default value is POPEYE.

MgxRWCommunityString2 — Read-Write MGX chassis community for PXM45 and PXM1E-based devices; default value is private.

Cisco MGM Log Files

Cisco MGM log files are located at:

<CEMFROOT>/logs/LoggercmgmvCtlr.log

Cisco MGM automatically moves log files to LoggercmgmCtlr.old after 30000 lines of information are logged. At that point, a new LoggercmgmvCtlr.log file is created.

Changing Logging Levels

To set logging levels for Cisco MGM files, perform the following steps:

Step 1 Access the following file:

```
<CEMFROOT>/init/loggercommon.include
```

Step 2 Change the loggingLevelMask value to your desired logging level. The loggingLevelMask value is a decimal number based on a 4-bit mask. The following levels are valid:

1 (0001): information

2 (0010): warning

4 (0100): debug

8 (1000): error

15 (1111): all

Step 3 For Cisco EMF logging, you must shut down and restart the Cisco EMF system for logging level changes to take effect.

Step 4 For Cisco MGM logging, you do not need to shutdown and restart the system for changes to take effect. Enter the following command to dynamically reset the Cisco MGM logging level:

```
kill -USR1 <process_id>
```

where <process_id> is the id of the cmgmvCtlr process in your Unix system.

INDEX