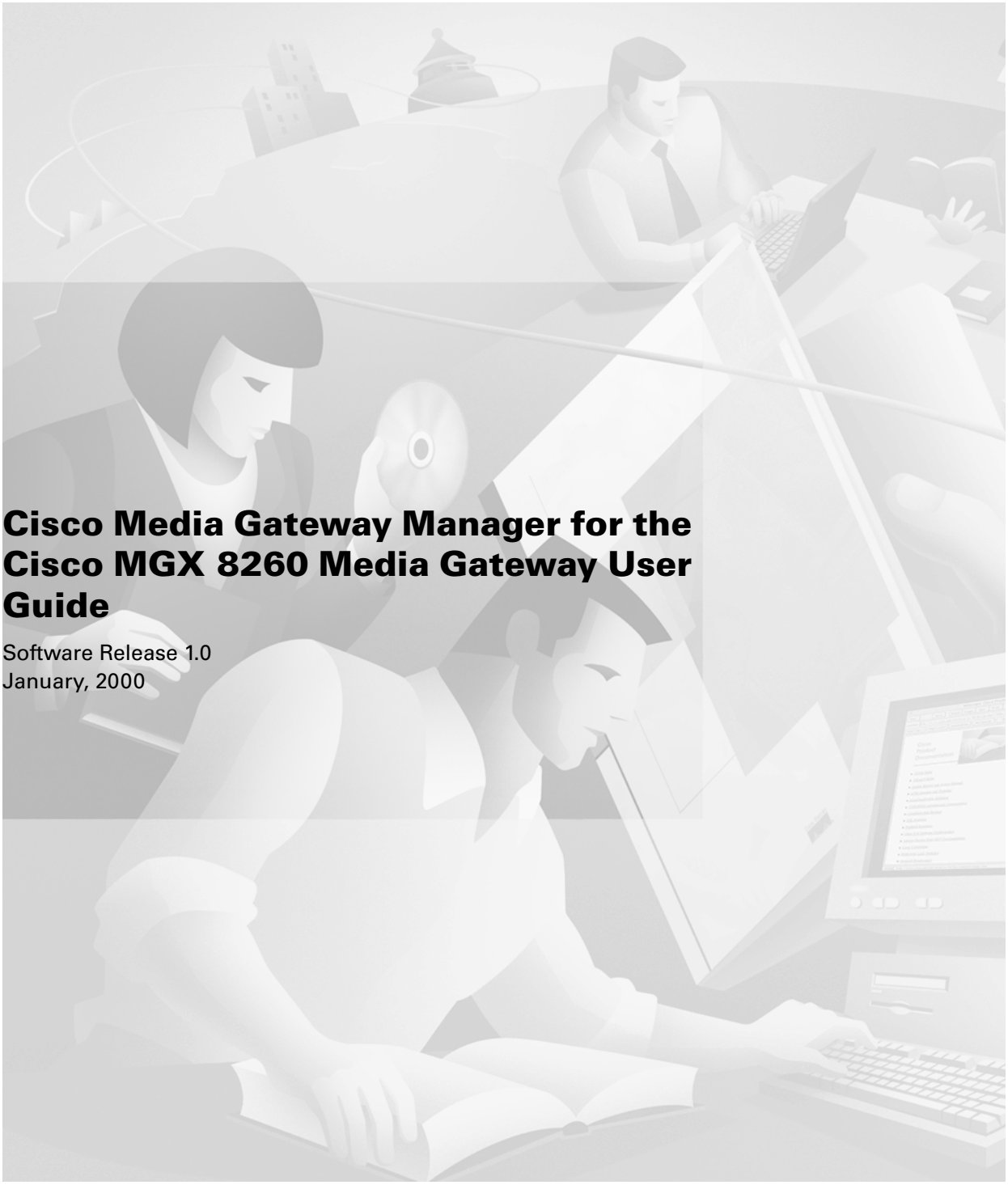


Cisco Media Gateway Manager for the Cisco MGX 8260 Media Gateway User Guide

Software Release 1.0
January, 2000

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

Customer Order Number: DOC-7811705=
Text Part Number: 78-11705-01

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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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.

AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco Net*Works* logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare,FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0011R)

Cisco Media Gateway Manager for the Cisco MGX 8260 Media Gateway User Guide
Copyright © 2000, Cisco Systems, Inc.
All rights reserved.

CONTENTS

Preface xi

Audience xi

Organization xi

Related Documentation xii

Conventions xii

Obtaining Documentation xiii

World Wide Web xiii

Documentation CD-ROM xiii

Ordering Documentation xiv

Documentation Feedback xiv

Obtaining Technical Assistance xiv

Cisco.com xiv

Technical Assistance Center xv

Contacting TAC by Using the Cisco TAC Website xv

Contacting TAC by Telephone xv

CHAPTER 1 **Cisco MGM Orientation** 1-1

Overview 1-1

Management Features 1-2

Fault Management 1-2

Configuration Management 1-2

Performance Management 1-2

Security Management 1-3

Cisco MGM Architecture 1-3

Management Tasks by Interface 1-4

Cisco WebViewer Features 1-5

Cisco Voice CORBA Gateway Features 1-5

CHAPTER 2 **Cisco MGM Installation** 2-1

Deployment Options 2-1

Server with Local Client 2-2

Server with Remote Clients 2-3

System Requirements **2-3**
Platform Requirements **2-4**
Software Requirements **2-4**
Installing the Cisco MGM Server **2-5**
Installing a Netscape Browser **2-5**
Installing Cisco EMF Server Software **2-5**
Configuring Raw Partitions **2-5**
Installing Cisco MGM Server Software **2-6**
Installing Cisco MGM Clients **2-7**
Installing a Netscape Browser **2-7**
Installing Cisco EMF Client Software **2-7**
Changing the Installation **2-8**
Updating Trap Forwarding **2-8**
Viewing Software Version Information **2-9**
Uninstalling Cisco MGM Server or Client **2-9**
Initializing Cisco MGX 8260 Media Gateway Nodes **2-10**

CHAPTER 3 **Using the Management Interfaces** **3-1**
Cisco EMF User Sessions **3-1**
Starting a Cisco EMF User Session **3-1**
Launching an Application **3-2**
Quitting a Cisco EMF User Session **3-4**
Cisco WebViewer Sessions **3-4**
Starting a Cisco WebViewer Session **3-4**
Understanding Cisco WebViewer Panes **3-5**
Common Display and Control Screens **3-6**
Chassis View **3-6**
Status Screens **3-6**
Configuration Forms **3-7**
Quitting a Cisco WebViewer Session **3-8**
Telnet Sessions **3-8**

CHAPTER 4 **Security Management** **4-1**
Cisco EMF User Accounts **4-1**
Changing Passwords **4-2**
Cisco MGX 8260 Media Gateway User Accounts **4-3**

Setting Up Accounts **4-3**
Cisco MGM Community String Configuration **4-4**
Initializing Cisco MGX 8260 Community Strings **4-5**
Initializing Cisco MGM Community Strings **4-5**

CHAPTER 5 **Network Management 5-1**
Cisco MGM Sites **5-1**
Site Discovery **5-1**
Invoking Automatic Discovery **5-2**
Inventory Discovery **5-2**
Manual Initiation of Subchassis Synchronization **5-3**
Periodic Subchassis Synchronization **5-3**
Downloading Software Images and Configuration Files **5-4**
Upgrading Card Software **5-5**

CHAPTER 6 **Fault and Performance Management 6-1**
Alarm Management **6-1**
Performance Management **6-1**
Monitoring Alarms and Events **6-2**
Map Viewer Display **6-2**
Event Browser Display **6-4**
Launching the Event Browser **6-5**
Viewing Cisco MGM Logs **6-5**
Registering Cisco MGX 8260 Traps **6-5**
Monitoring Alarms from the Cisco WebViewer **6-7**
Monitoring Performance from the Cisco WebViewer **6-8**

CHAPTER 7 **Cisco MGX 8260 Node Management 7-1**
Configuring System Parameters **7-1**
Configuring the Management Interfaces **7-2**
Synchronizing the System Clock **7-2**
Configuring Lines **7-3**
Configuring Voice Ports **7-4**
Viewing Active Calls **7-4**
Understanding MGCP **7-5**
Configuring MGCP **7-5**

Understanding Sessions **7-6**
Configuring Sessions **7-7**
Understanding ISDN D Channels Usage **7-7**
Configuring D Channels **7-8**
Configuring IPDC **7-9**
Managing Announcement Files **7-10**

INDEX

FIGURES

Figure 1-1 Cisco MGM Architecture **1-3**
Figure 2-1 Server With Local Client **2-2**
Figure 2-2 Server with Remote Clients **2-3**
Figure 3-1 Cisco EMF Launchpad **3-2**
Figure 3-2 Cisco MGM Topology View **3-3**
Figure 3-3 MGX 8260 Icons **3-3**
Figure 3-4 MGX 8260 Chassis View **3-5**
Figure 3-5 Card Configuration and Status Screen **3-6**
Figure 3-6 Card Configuration Screen **3-7**
Figure 4-1 Cisco EMF Launchpad **4-2**
Figure 4-2 User Profile Screen **4-4**
Figure 4-3 Community String Screen **4-5**
Figure 4-4 SNMP Community String Dialog Box **4-6**
Figure 4-5 Action Report Dialog Box **4-7**
Figure 6-1 Cisco MGM Topology View **6-2**
Figure 6-2 Information Displayed on an Object **6-3**
Figure 6-3 Cisco EMF Event Browser Window **6-4**
Figure 6-4 Chassis View with Alarms **6-7**
Figure 7-1 MGCP Addresses and Ports **7-5**
Figure 7-2 Organization of Sessions **7-6**
Figure 7-3 Logical Session Model **7-7**
Figure 7-4 D Channel to Media Gateway Controller **7-8**

Table 1 Cisco Voice CORBA Gateway Release 1.0 Related Documentation **xii**
Table 1-1 Management Tasks by Cisco MGM Interface **1-4**
Table 2-1 Minimum Platform Requirements **2-4**
Table 3-1 Icons Used On Line Configuration Screens **3-7**
Table 4-1 Cisco EMF Accounts **4-1**
Table 4-2 User Accounts and Access Privileges **4-3**
Table 4-3 System Configuration Map **4-4**
Table 4-4 MGX 8260 Community String Configuration Map **4-5**
Table 6-1 Alarm Severity Colors and Codes **6-3**
Table 6-2 Log Files **6-5**
Table 6-3 Trap Registration Map **6-6**
Table 6-4 Trap Categories **6-6**
Table 6-5 Alarm Surveillance Map **6-8**
Table 6-6 Performance Surveillance Map **6-8**
Table 7-1 System Configuration Map **7-2**
Table 7-2 Management Interface Configuration Map **7-2**
Table 7-3 Clock Source Configuration Map **7-3**
Table 7-4 Line Configuration Map **7-3**
Table 7-5 Voice Port Configuration Map **7-4**
Table 7-6 Active Call Status Map **7-5**
Table 7-7 MGCP Configuration Map **7-6**
Table 7-8 Session Configuration Map **7-7**
Table 7-9 D Channel Configuration Map **7-9**
Table 7-10 IPDC Configuration Map **7-9**
Table 7-11 Announcement File Configuration Map **7-10**

Preface

This chapter describes the objectives, audience, organization, and conventions of the *Cisco Media Gateway Manager for the Cisco MGX 8260 Media Gateway User Guide*, and contains the following sections:

- Audience, page xi
- Organization, page xi
- Related Documentation, page xii
- Conventions, page xii
- Obtaining Documentation, page xiii
- Obtaining Technical Assistance, page xiv

Audience

This guide is meant to be used by the following network experts:

- Network operators and administrators, who have experience in telecommunications networks, protocols, and equipment and who are familiar with data communications networks, protocols, and equipment.
- Network designers, who have experience with telecommunications networks, protocols, and equipment and with data communications networks, protocols, and equipment.

Organization

This guide contains instructions for installing the software and configuring the Cisco MGX 8260 Media Gateway nodes.

This guide contains the following chapters:

Chapter 1, “Cisco MGM Orientation”, provides an overview of the applications and features.

Chapter 2, “Cisco MGM Installation”, describes how to install and test the product.

Chapter 3, “Using the Management Interfaces”, orients the user to the graphical interfaces.

Chapter 4, “Security Management”, introduces Cisco EMF and Cisco MGM user accounts, as well as SNMP community strings.

Chapter 5, “Network Management”, provides procedures for using the automatic discovery and sub-chassis synchronization for Cisco MGX 8260 Media Gateways.

Chapter 6, “Fault and Performance Management”, provides procedures for monitoring alarms and performance.

Chapter 7, “Cisco MGX 8260 Node Management”, summarizes the Cisco WebViewer configuration procedures.

Related Documentation

The following Cisco publications contain additional information related to the operation of the *Cisco Media Gateway Manager for the Cisco MGX 8260 Media Gateway User Guide*.

Table 1 Cisco Voice CORBA Gateway Release 1.0 Related Documentation

Documentation	Description
Cisco Element Manager Framework User Guide DOC-7810791=	This book describes the element management framework on which the Cisco Media Gateway Manager is based.
Cisco Voice CORBA Gateway for the MGX 8260 Media Gateway Developer Reference Guide DOC-7811706=	This book describes the CORBA/IDL interface for the Cisco Media Gateway Manager.
Cisco MGX 8260 Command Line Interface Guide DOC-7810987=	This book describes how to configure MGX 8260 Media Gateways from the command line interface.
Cisco WebViewer Guide *DOC-7811012=*	This book describes how to use the Cisco WebViewer tool.

Conventions

This publication uses the following conventions to convey instructions and information.

Command descriptions use these conventions:

- Commands and keywords are in **boldface**.
- Arguments for which you supply values are in *italics*.
- Required command arguments are inside angle brackets (< >).
- Optional command arguments are in square brackets ([ ]).
- Alternative keywords are separated by vertical bars (|).

Examples use these conventions:

- Terminal sessions and information the system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords, are in angle brackets (< >).

Default responses to system prompts are in square brackets ([ ]).

Notes, tips, cautions, and warnings use the following conventions and symbols:

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. You are capable of doing something that might result in equipment damage or loss of data.

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

Timesaver Means the described action saves time. You can save time by performing the action described in the paragraph.

Tips Means the following information might help you solve a problem.

Obtaining Documentation

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

World Wide Web

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

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

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

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

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

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

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

Documentation Feedback

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

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

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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

CHAPTER 1

Cisco MGM Orientation

The Cisco Media Gateway Manager (Cisco MGM) can deploy, configure, and manage a group of Release 1.2 Cisco MGX 8260 Media Gateways in one or more Points of Presence (POP). This chapter contains the following sections:

- Overview, page 1-1
- Management Features, page 1-2
- Cisco MGM Architecture, page 1-3
- Management Tasks by Interface, page 1-4
- Cisco WebViewer Features, page 1-5

Overview

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

Cisco MGM includes a graphical user interface that displays network information and supports device management. This interface extends the capabilities of the Cisco Element Management Framework (Cisco EMF) to include managing Cisco MGX 8260 Media Gateways. Cisco MGM includes links to two management tools, the Cisco WebViewer and the Cisco MGX 8260 command line interface, from which you configure individual nodes.

Network management layer applications can communicate with Cisco MGM through an optional CORBA/IDL interface provided by the Cisco Voice CORBA Gateway (Cisco VCG). This gateway is a separate product that extends the capabilities of the Cisco MGM product.

Management Features

Cisco MGM implements fault, configuration, performance, and security features.

Fault Management

Using Cisco MGM, you can monitor the network for faults and clear alarms. The system handles alarms and events as follows:

- Displays alarm and events on a color-coded topology map.
- Forwards traps to remote SNMP managers.
- Optionally, propagates alarms to higher-level managers. This feature requires the Cisco Voice CORBA Gateway option.

Using the Cisco WebViewer tool, you can view threshold-based alarms, gather performance statistics, perform line diagnostic tests, and configure email or pager alerts for alarms. You launch the Cisco WebViewer application directly from Cisco MGM.

Configuration Management

Cisco MGM provides the following configuration management features:

- Topology views of network elements
- Automatic discovery of Cisco MGX 8260 Media Gateways
- Synchronization of Cisco MGM objects with subchassis components
- Multichassis download of software images
- Configuration of SNMPv1 community strings
- Menu-launched WebViewer or telnet sessions for web-based or CLI device management

An optional extension, the Cisco Voice CORBA Gateway, provides a programmatic interface from which higher-level managers can fully configure and monitor the Cisco MGX 8260 Media Gateways.

Performance Management

Cisco MGM supports performance management as follows:

- Menu-launched WebViewer tool

  This tool displays performance statistics and real-time counters for all DS1, DS3, and SONET lines. Also, you can adjust the counter thresholds to refine performance collection criteria.

- Cisco Voice CORBA Gateway (optional)

  This interface propagates performance statistics to higher-level managers. On request, Cisco MGM retrieves performance statistics from the Cisco MGX 8260 Media Gateways, packages the statistics in a bulk file, and forwards it to the manager.

Security Management

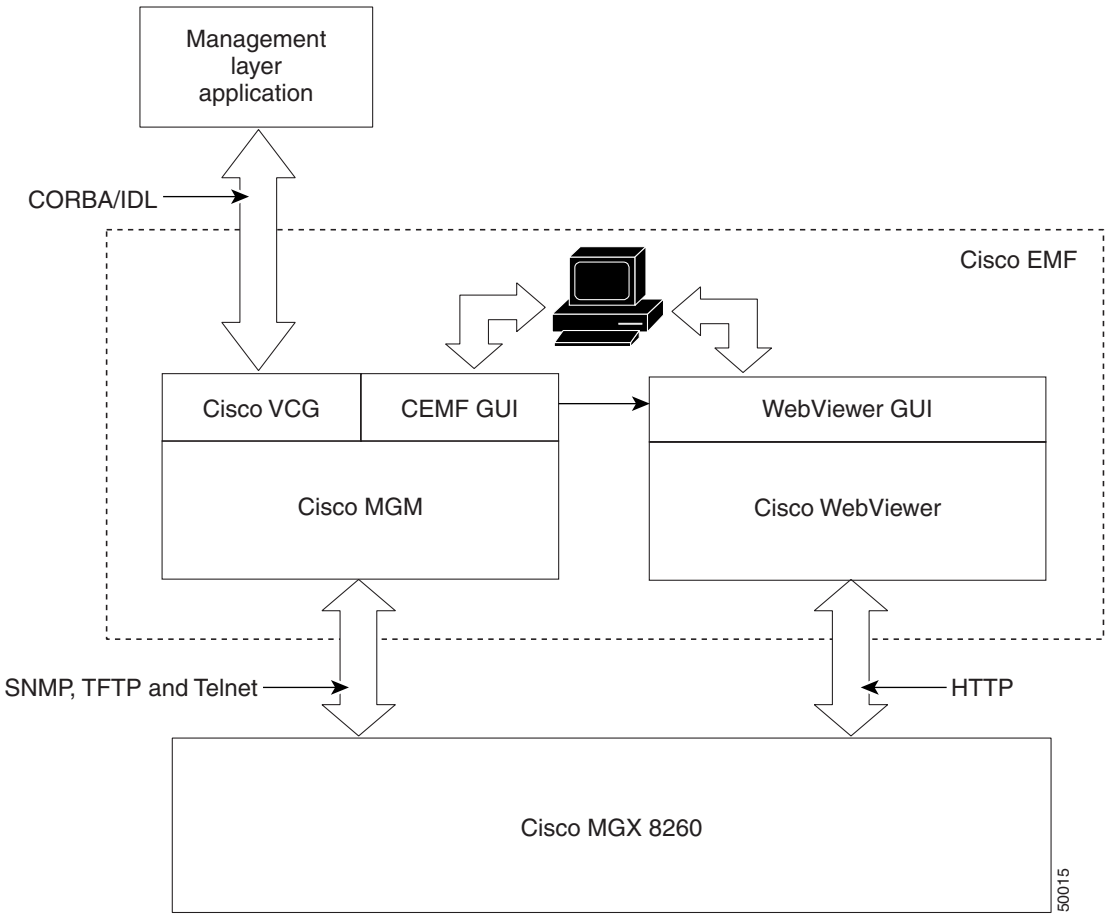
Cisco MGM security uses the mechanisms of Cisco EMF, which authenticates users based on names and passwords. When using the Cisco WebViewer or CLI management interfaces, the Cisco MGX 8260 Media Gateway also authenticates users based on Cisco MGX 8260 user accounts. Both systems support security profiles that define access rights for typical users, from administrators to guests.

Messages between Cisco MGM and network elements is secured using SNMP community strings. You configure unique community strings known by all network elements to limit and control access.

Cisco MGM Architecture

Cisco MGM extends the functionality of Cisco EMF to include management of Cisco MGX 8260 Media Gateways (see Figure 1-1).

Figure 1-1 Cisco MGM Architecture



Cisco MGM is an element manager that adds custom GUI windows and network modeling to the standard Cisco EMF product. Users manage Cisco MGX 8260 Media Gateway nodes from the Cisco EMF GUI, which includes a link to the Cisco WebViewer configuration tool. Cisco MGM communicates

with Cisco MGX 8260 nodes using SNMPv1 and TFTP protocols; the Cisco WebViewer uses a standard web browser, such as Netscape for Solaris, that communicates with the HTTP server in each Cisco MGX 8260 Media Gateway. In addition, you can launch a telnet session to an individual chassis directly from a Cisco MGM menu.

An optional extension, the Cisco Voice CORBA Gateway, provides a language-independent Application Programming Interface (API) from which higher-level managers can configure and monitor the Cisco MGX 8260 Media Gateways. This interface supports both Cisco and third-party management applications.

Management Tasks by Interface

Depending on the management task, you use one of three interfaces:

- Cisco EMF user interface
- Cisco WebViewer user interface
- Cisco Voice CORBA Gateway programatic interface

The following table organizes management tasks by management interface:

Table 1-1 Management Tasks by Cisco MGM Interface

Management Task	Cisco MGM GUI	WebViewer/CLI	Cisco VCG[1]
Automatic discovery of network elements	Yes	–	–
Configure system date and time	Yes[2]	Yes	Yes
Configure Dsx1/Dsx3/SONET/Fast Ethernet	–	Yes	Yes
Configure D1SapProfile, MacSapProfile, D channel	–	Yes	Yes
Configure MGCP parameters	–	Yes	Yes
Configure IPDC parameters	–	Yes	–
Configure Backhaul Sets, Groups, and Sessions	–	Yes	Yes
Subchassis discovery and synchronization	Yes	–	Yes
Software image and config file download	Yes	Yes	Yes
Upgrade image and configure redundancy	–	Yes	–
View Dsx1/Dsx3/Sonet line statistics information	–	Yes	Yes
View Dsx1/Dsx3/Sonet line performance history information	–	Yes	Yes

1. The Cisco Voice CORBA Gateway is an optional addin for the Cisco MGM product.
2. This is a standard Cisco EMF feature.

Cisco WebViewer Features

Using the Cisco WebViewer, you can perform the following tasks:

- Enforce security

  The Cisco MGX 8260 Media Gateway enforces security with user accounts and access levels. Users must log onto the Cisco MGX 8260 Media Gateway before performing any task, and authenticated users can perform only those tasks permitted by their access level. The Cisco MGX 8260 Media Gateway supports up to 20 user accounts, each with access privileges ranging from full control to guest.

- Manage Cisco MGX 8260 Media Gateway nodes and the services they provide

  The Cisco WebViewer provides dedicated Cisco MGX 8260 Media Gateway information, including system settings, node configurations, service provisioning, and system test features. The Cisco WebViewer get information from the SNMP core, but presents it in simple text and graphic forms.

- Monitor the Cisco MGX 8260 status and alarms

  The Cisco WebViewer provides real-time information on Cisco MGX 8260 status, alarms, events, and statistics. Using Java scripts and applets, the Cisco WebViewer constantly monitors the Cisco MGX 8260 Media Gateway and updates the user interface.

  Every screen has a prominent alarm indicator that shows the current operational status. With a single click, users can obtain detailed information on outstanding alarms and events.

  Also, the Cisco MGX 8260 Media Gateway can notify users by email when alarms or events occur.

- Monitor performance

  The Cisco WebViewer reports current and historical performance data, and displays performance statistics when performance drops below user-defined levels. Using this feature, operators can react to problems that could degrade performance before the system fails.

- Maintain the system

  Using the alarm and test features, maintenance personnel can often diagnose and solve equipment problems directly from the Cisco WebViewer. For example, if a DS1 line raises a performance alarm, maintenance personnel can diagnose the problem with loopback and BERT tests and initiate corrective action.

Cisco Voice CORBA Gateway Features

Network management layer applications can communicate with Cisco MGM through an optional CORBA/IDL interface provided by the Cisco Voice CORBA Gateway. Using this gateway, network managers can monitor and configure Cisco MGX 8260 Media Gateways.

Cisco VCG provides the following network management interfaces:

- Alarm surveillance

  An event notification service filters and reports alarms and events to client applications. Clients register for the desired alarms.

- Configuration management

  An object access process traverses the object hierarchy to discover and upload MGX 8260 objects in bulk. Client applications can configure individual attributes on a single chassis, or perform bulk configurations across multiple chassis.

- Performance management

  Client applications can retrieve performance statistics for DS1, DS3, and SONET lines through the Cisco VCG interface.

For more information, see the *Cisco Voice CORBA Gateway for the MGX 8260 Media Gateway User Guide*.

CHAPTER 2

Cisco MGM Installation

Cisco MGM is based on the Cisco EMF, 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 installing Cisco MGM.

This chapter covers the following topics:

- Deployment Options, page 2-1
- System Requirements, page 2-3
- Installing the Cisco MGM Server, page 2-5
- Installing Cisco MGM Clients, page 2-7
- Changing the Installation, page 2-8
- Initializing Cisco MGX 8260 Media Gateway Nodes, page 2-10

Deployment Options

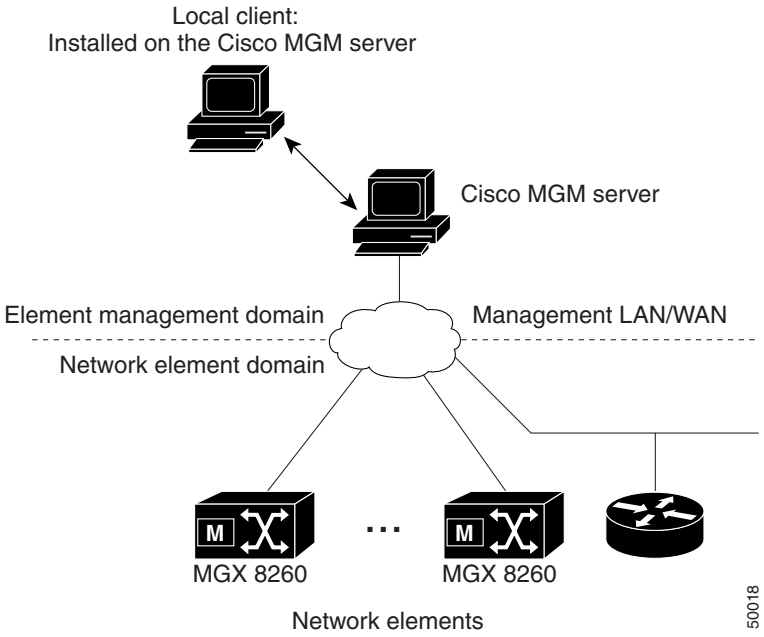
You deploy Cisco MGM as a server with clients in a distributed environment. The following types of deployment are available:

- 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 separate Sun workstation.

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, events, and so on. 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

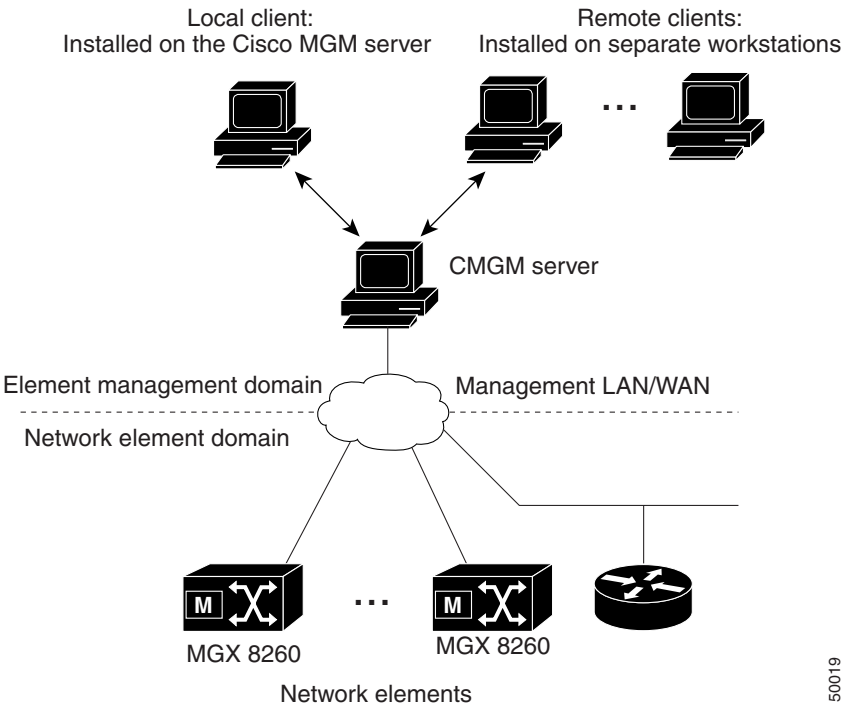


Note You can also log onto the system from a PC running x-window emulation software, such as ReflectionX v7.20 or Exceed v6.1.

Server with Remote Clients

A Cisco EMF deployment may 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. Typically, you can install client software from a local CD ROM drive and do not need to mount files across a network.

Figure 2-2 Server with Remote Clients



System Requirements

This section describes the platform and software requirements for a Cisco MGM system.

Platform Requirements

The platform resources you need depend on the number of Cisco MGX 8260 Media Gateways and their configurations. A basic installation requires 2 GB of free disk space in a file system (for example /opt) for Cisco EMF and Cisco MGM.

Table 2-1 Minimum Platform Requirements

Resource	Cisco MGM Server	Cisco MGM Client
Hardware	Sun Ultra 60 Workstation	Sun Ultra 5 workstation
Operating system	Solaris 2.6 with CDE 1.3 or SunOS 5.6	Solaris 2.6 with CDE 1.3 or SunOS 5.6
Memory	1 GB RAM	256MB RAM
Disk space	Four hard disks, 9GB or larger[1]	One hard disk, 9GB or larger
Processor	Two x 360Mhz	333Mhz
Swap space	2GB	2GB
Monitor	17" color	17" color
Graphics card	24bit	24bit
CD ROM	Local or remote	Local or remote

1. Do not substitute a smaller number of larger drives.

Allocate the server's hard disks as follows:

- Database and transaction log (2 drives)
- Solaris operating system and swap space (1 drive)
- Cisco MGM and Cisco EMF software, including the Cisco EMF database (1 drive)

A Cisco MGM server supports 5 concurrent Cisco MGM user sessions. Cisco MGM clients can support 5 additional users. Therefore, the maximum number of concurrent users for a client/server configuration is 10. Each MGX 8260 chassis supports 5 concurrent Cisco WebViewer sessions.

Note OpenWindows is not supported on Cisco EMF.

Software Requirements

You need the following software for this installation:

- Cisco EMF version 3.1
- Cisco MGM version 1.0
- Netscape 4.5 for Solaris (for Cisco WebViewer)
- Cisco MGX 8260 Media Gateway, software version 1.2
- Cisco Voice CORBA Gateway version 1.0 (optional)

Installing the Cisco MGM Server

To install the server, perform these major steps:

Step 1 Install the Netscape browser.

Step 2 Install Cisco EMF server.

Step 3 Configure RAW partitions.

Step 4 Install Cisco MGM server.

Installing a Netscape Browser

Cisco WebViewer requires a full installation of the Netscape browser to operate correctly. Refer to the Netscape documentation for installation procedures.

Record the path to the Netscape executable; you use this information when installing Cisco MGM.

Installing Cisco EMF Server Software

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

Note Answer No when the installation scripts asks if you want to use a RAW partition.

Configuring Raw Partitions

Perform this procedure after installing Cisco EMF if you want to use a raw file partition for the database and database transaction log.

To configure a raw partition, follow these steps:

Step 1 Log in as the root user.

Step 2 Configure one or more disk drive for raw partitioning using the UNIX format command. Consult with your system administrator if you are not familiar with this command.

Step 3 Stop the Cisco EMF server:

```
<CEMF_ROOT>/bin/cemf stop
```

where CEMF_ROOT is the CEMF installation directory

Step 4 Stop ObjectStore:

```
/etc/rc2.d/S80ostore4 stop
```

Step 5 Stop the AV License Manager:

```
/etc/rc2.d/S98avlm stop
```

Step 6 Start a Cisco EMF shell:

```
<CEMF_ROOT>/bin/cemf shell
```

Step 7 Edit the host name server parameters file, as follows:

a. Using a text editor, open the hostname server parameters file in <CEMF_ROOT>/ODI/OS5.1/ostore/etc

b. Comment out the line for the transaction.log. This places the log in a raw partition.

c. Add an entry for each raw partition that ObjectStore uses. Each entry is of the format:

Partition<X>: PARTITION <raw partition drive name>

where X is an integer starting at 0 for the first partition and incrementing 1 for each subsequent entry. The raw partition name can be of the format /dev/rdsk/c2t9d0s0.

For example:

```
#Log File: /opt/transact.log
Partition0: PARTITION /dev/rdsk/c2t9d0s0
Partition1: PARTITION /dev/rdsk/c2t10d0s0
```

Step 8 Reinitialize ObjectStore:

```
<CEMF_ROOT>/ODI/OS5.1/ostore/lib/osserver -i
```

Step 9 Reset the Cisco EMF database:

```
<CEMF_ROOT>/bin/cemf reset
```

Step 10 Start CEMF:

```
<CEMF_ROOT>/bin/cemf start
```

The system resumes normal operation.

Installing Cisco MGM Server Software

Before installing Cisco MGM server software, uninstall any previous Cisco MGM versions. For more information, see Uninstalling Cisco MGM Server or Client, page 2-9.

To install the Cisco MGM server, follow these steps:

Step 1 Log in as the root user.

Step 2 Change to the cmgm1.0pkg package directory on the CD ROM.

```
cd <CDROM>/cmgm1.0pkg
```

Step 3 Start the installation script.

```
./cmgminstall
```

Tips To get help, enter cmgminstall -h

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

- When prompted for the type of installation, select a **cmgmpkg Server Package** option.
- When prompted for the path of the Netscape browser, use the full path of the Netscape browser rather than the path to the Cisco EMF browser.
- When prompted for trap forwarding, answer Yes if you want to forward MGX8260 traps to a remote management system, otherwise answer No. You can change this decision later.

Note Make sure you specify the full and correct path to Netscape; it's difficult to change later.

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

```
/var/adm/Atlantech/avinstall/cmgmpkg_Server_Package/logfile
```

Step 6 Verify that the cmgmCtlr process is running. For example:

```
/opt/cemf/bin/cemf query
```

The Cisco MGM plugin automatically starts on Cisco EMF.

Installing Cisco MGM Clients

To install the client, perform these major steps:

Step 1 Install the Netscape browser.

Step 2 Install the Cisco EMF client.

Step 3 Install the Cisco MGM client.

Installing a Netscape Browser

Cisco WebViewer requires a full installation of the Netscape browser to operate correctly. Refer to the Netscape documentation for installation procedures.

Record the path to the Netscape executable; you use this information when installing the Cisco MGM client.

Installing Cisco EMF Client Software

Before installing a client, remove any previous Cisco MGM client versions. For more information, see Uninstalling Cisco MGM Server or Client, page 2-9.

To install Cisco MGM client, follow these steps:

Step 1 Log in as the root user.

Step 2 Change to the cmgm1.0pkg package directory on the CD ROM.

```
cd <CDROM>/cmgm1.0pkg
```

Step 3 Start the installation script.

```
./cmgminstall
```

Tips To get help, enter cmgminstall -h

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

- When prompted for the type of installation, select a **cmgmpkg Client Package** option.
- When prompted for the path of the Netscape browser, use the full path of the Netscape browser rather than the path to the Cisco EMF browser.

Note Make sure you specify the full and correct path to Netscape; it's difficult to change later.

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

```
/var/adm/Atlantech/avinstall/cmgmpkg_Client_Package/logfile
```

The Cisco MGM client automatically starts.

Changing the Installation

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

Updating Trap Forwarding

To enable trap forwarding to other hosts, follow these steps:

Step 1 Log in as the root user.

Step 2 Change to the directory for scripts.

```
cd <CEMF_ROOT>/config/scripts/cmgm
```

Step 3 Run the installation script.

```
./updTrapForward
```

Tips To get help, enter updTrapForward -h

Step 4 Change to the directory for executables.

```
cd <CEMF_ROOT>/bin
```

Step 5 Restart Cisco EMF.

```
cemf stop
cemf start
```

The system begins forwarding traps.

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 <CEMF_ROOT>/config/scripts/cmgm
```

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

```
./cmgminstall -s
```

The script displays software information

Uninstalling Cisco MGM Server or Client

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

To remove Cisco MGM, follow these steps:

Step 1 Log in as the root user.

Step 2 Change to the scrip directory.

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

Step 3 Run the deinstallation script.

```
./cmgminstall -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/cmgmpkg_Server_Package/logfile
```

The client log file is in the following location:

```
/var/adm/Atlantech/avinstall/cmgmpkg_Client_Package/logfile
```

Initializing Cisco MGX 8260 Media Gateway Nodes

For the Cisco MGM to communicate with Cisco MGX 8260 Media Gateways, initialize the following parameters for each MGX 8260 chassis.

- Management IP address
- Site name (sysLocation parameter)
- Community strings
- Trap registrations

You can configure these settings using the CLI or Cisco WebViewer. Nodes usually have an IP address and site name (sysLocation parameter) configured, but you may need to initialize SNMP communities and register traps. Check with your system administrator before assigning or changing IP addresses.

CHAPTER 3

Using the Management Interfaces

This chapter provides the logon procedures and explains the basic features of the user interfaces. You use the following user interfaces when managing networks of Cisco MGX 8260 Media Gateways:

- Cisco EMF User Sessions, page 3-1
- Cisco WebViewer Sessions, page 3-4
- Telnet Sessions, page 3-8

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. If, upon starting, you receive a message that Cisco EMF is not running, contact your system administrator.

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

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

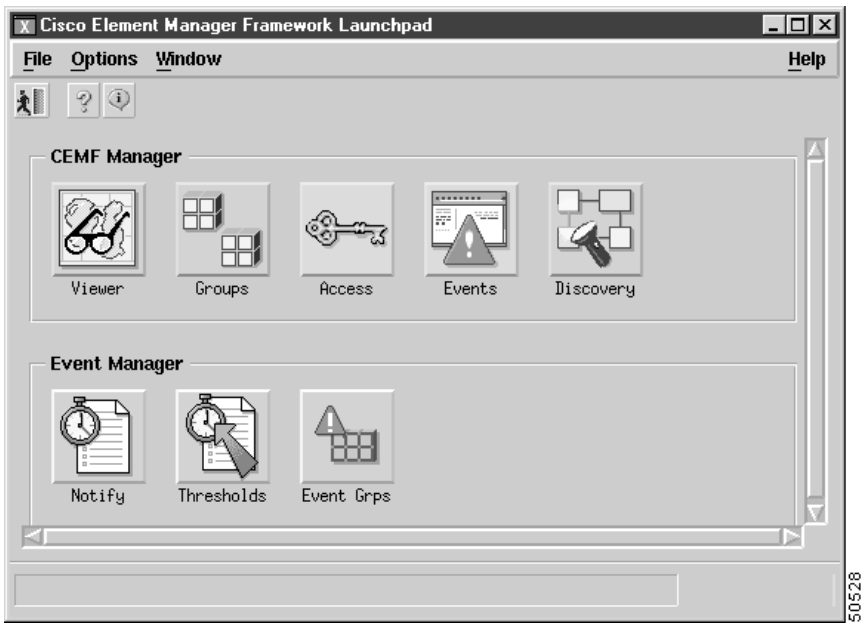
where <CEMF_ROOT> is the root directory for Cisco EMF installation (for example, **/opt/cemf**).

The Cisco EMF Login window opens.

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

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

Figure 3-1 Cisco EMF Launchpad



The icons on the Launchpad represent applications provided by this Cisco EMF installation. The icons appear in a frame identified by the package name.

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.

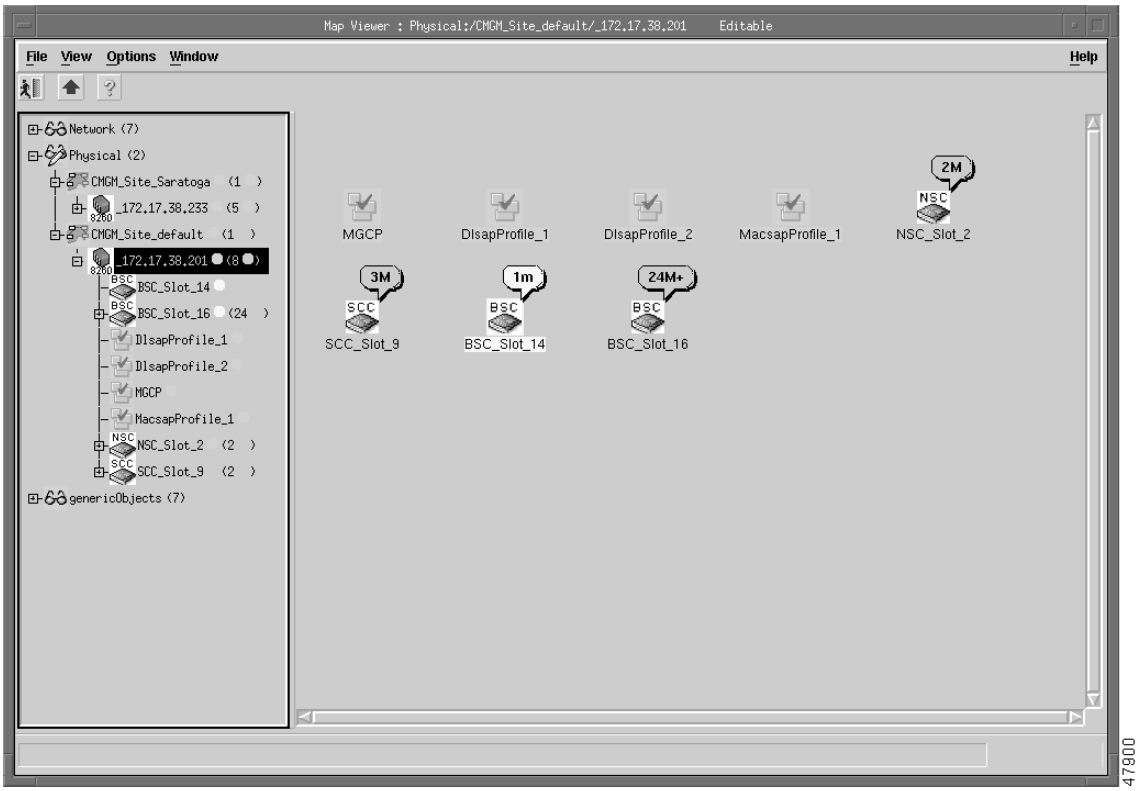
Launching an Application

From the **Cisco EMF Launchpad,** click on the desired application icon. The selected application is launched. A "busy" icon and a message in the status bar is displayed during launch. More than one instance of an application can be opened simultaneously.

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

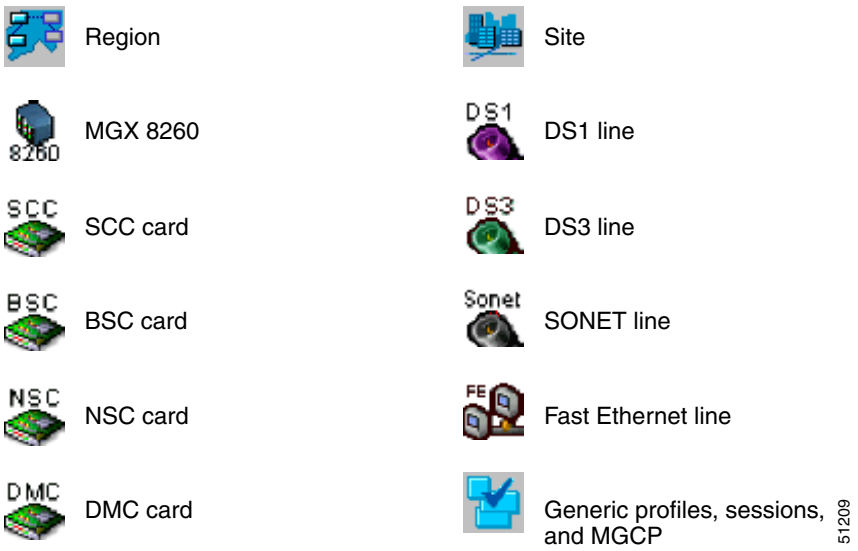
For Cisco MGM, the Map Viewer application displays information about the Cisco MGX 8260 Media Gateway nodes, cards, and other network equipment (see Figure 3-2).

Figure 3-2 Cisco MGM Topology View



Cisco MGM displays Cisco MGX 8260 Media Gateway components as icons (see Figure 3-3).

Figure 3-3 MGX 8260 Icons



Quitting a Cisco EMF User Session

Step 1 From the **File** menu, select **Quit** or press **Ctrl + Q** or click the **Close** icon from the Toolbar.

Step 2 A dialog box asking, `Do you wish to quit the CEMF Manager System?` is displayed. Click **Yes** to quit the session.

All active applications are closed, and the session terminates.

Cisco WebViewer Sessions

Before you can configure the Cisco MGX 8260 Media Gateway, you must log on as a user with the privileges necessary to change system parameters. You need SuperUser privileges to change most system-level settings.

Starting a Cisco WebViewer Session

This section explains how to log on and use Cisco WebViewer to manage Cisco MGX 8260 Media Gateway chassis and subchassis components.

To log on, follow these steps:

Step 1 On the MapViewer, right-click the desired MGX 8260 chassis; then click **Tools**; then click **Launch Web Viewer**.

The WebViewer **login** screen opens.

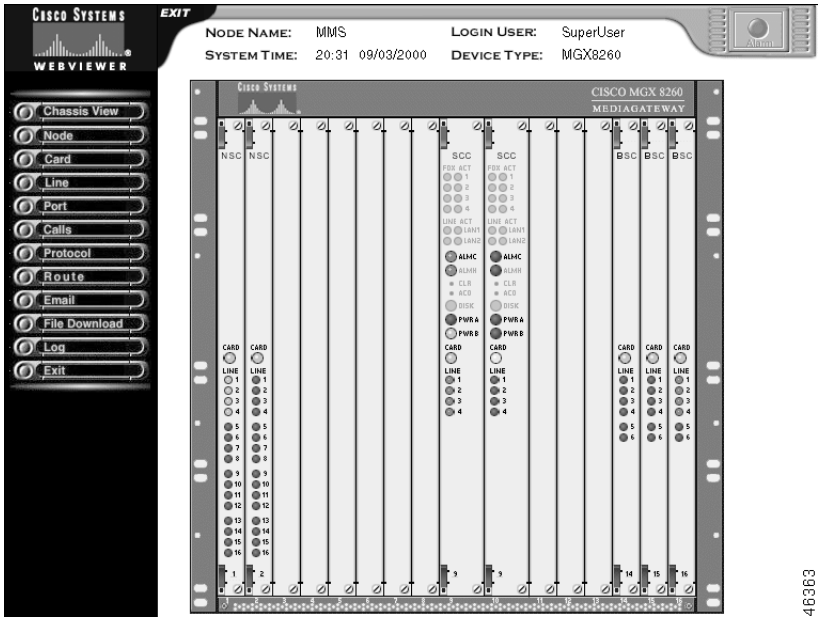
Step 2 In the **User Name** field, type the name of a valid MGX 8260 account name. On a new system, use **SuperUser**.

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

Step 4 Click **Log On**. Grant requests for additional privileges, if necessary.

The Cisco MGX 8260 Media Gateway displays the chassis view (see Figure 3-4).

Figure 3-4 MGX 8260 Chassis View



Step 5 From the navigation pane on the left, select the operation you want to perform. For example, to set node parameters click **Node** and then click a submenu item.

Understanding Cisco WebViewer Panes

Every Cisco WebViewer screen has three panes:

1. System information

   The Cisco WebViewer displays real-time system information at the top of the display in the System Information pane. It includes the node name, date and time, current user, device type, and alarm status. The system updates this pane every two minutes.

   You can view a summary of alarms by clicking the alarm indicator, or you can configure system settings by clicking anywhere in the middle of the pane. (These are shortcuts to screens that you can also reach from the Navigation pane.)

2. Navigation

   The Navigation Pane contains a set of sliding menus that control the content in the adjacent Display and Control pane. When you click a menu item, an additional submenu may slide out. From this pane you can access most Cisco WebViewer configuration screens.

3. Display and control

   The Display and Control pane shows details about the menu item selected in the Navigation pane. The opening screen shows a graphic image of the chassis; other views display operation status or configuration forms. Some screens contain additional buttons or hyperlinks that facilitate configuration tasks.

Common Display and Control Screens

The Cisco WebViewer presents Cisco MGX 8260 status and configuration information in the following views:

- Chassis View
- Status screens
- Configuration forms

Chassis View

The Chassis View shows the Cisco MGX 8260 front panel, including the installed cards and their LED states. The cards and LEDs are active areas on the screen, so you can get more information about an LED indication by clicking it. To view configuration information about a card, click elsewhere on the desired card.

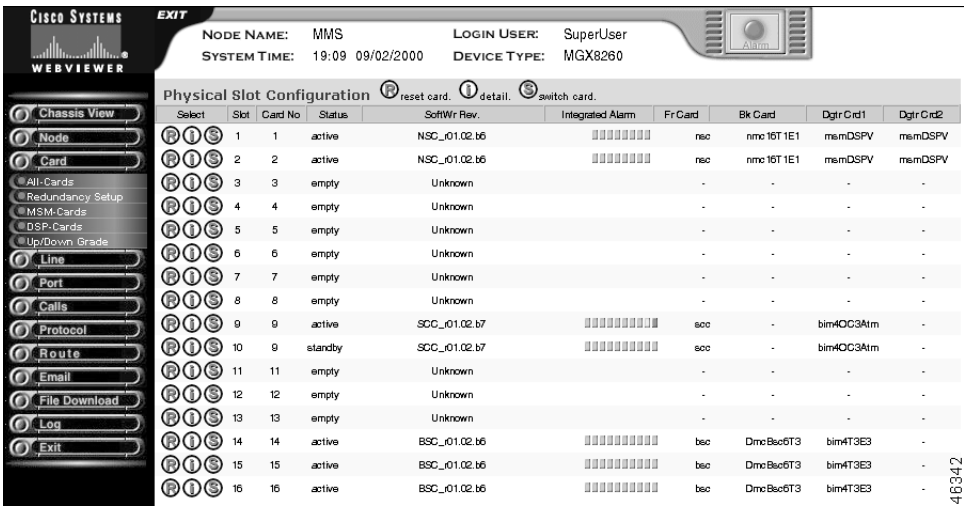
In the Chassis View, the following LEDs are displayed and updated in real time:

- BSC, NSC, and DMC—Card Status and Line Status LEDs
- Active SCC—ALAC, PWRA, PWRB, Card Status, and Line Status LEDs
- Standby SCC—Card Status LED only

Status Screens

Status screens display a summary of installed cards, configured services, or other information. Figure 3-5 shows an example of a screen that displays card configuration and status information.

Figure 3-5 Card Configuration and Status Screen



Many status screens contain buttons that open other configuration screens. For example, the plus icon links to the form for adding a card.

The table below shows the icons used to launch line configuration tasks:

Table 3-1 Icons Used On Line Configuration Screens

Icon	Task
-	Delete one or more lines.
i	Display alarm and configuration information.
C	Display error counters and performance alarms.
A	Set the performance alarm thresholds.
P	Display performance statistics or SONET path information.
S	Display DS0 details or SONET section information.
L	Display DS1 details or SONET line information.
+	Add a line.
R	Reset a card.

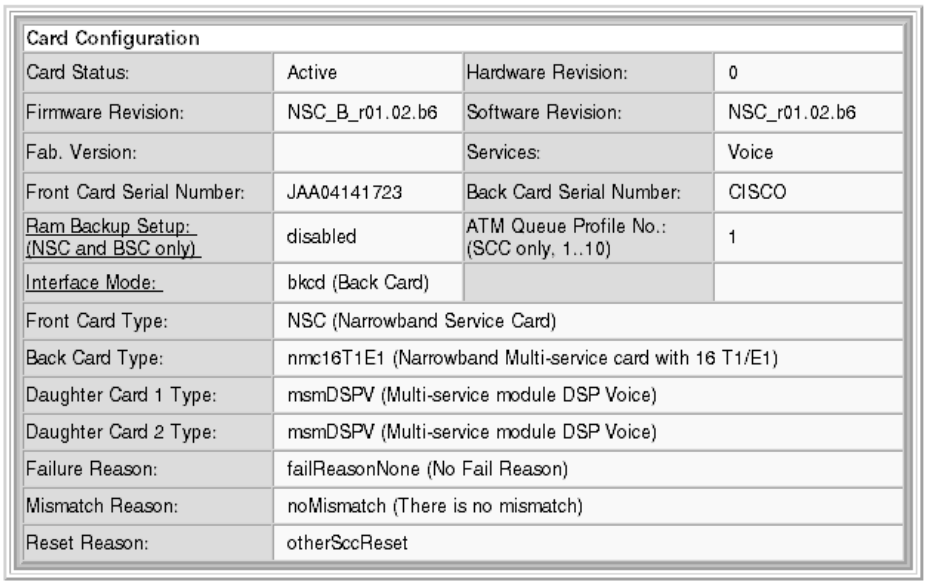
The first six icons in Table 3-1 are displayed in the Select column for each line on the line configuration forms. Click on the desired icon to perform the specified line configuration task.

Along the top of the line configuration forms is another row of icons, some of which are active buttons. Use the + and - icons in this group to add or delete lines. The rest of these icons are legends for the icons in the Select column.

Configuration Forms

Use configuration forms to define the parameters for a given card or service. Figure 3-6 shows an example of a card configuration form.

Figure 3-6 Card Configuration Screen



The configuration forms contain both pre-set and user-defined fields. In some cases, the fields contain hyperlinks to additional configuration forms. Because of security restrictions, not all users can access configuration forms.

Quitting a Cisco WebViewer Session

To log out and quit a Cisco WebViewer session, click the **Exit** button at the top of the navigation pane. The logon screen opens.

Telnet Sessions

To initiate a telnet session, follow these steps:

Step 1 On the MapViewer, right-click the desired MGX 8260 chassis; then click **Tools**; then click **Telnet**.

The telnet screen opens.

Step 2 At the User prompt, type the name of a valid MGX 8260 account name. On a new system, use **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

Security Management

Service providers may be obligated under law to protect sensitive information contained within management systems. Cisco MGM and Cisco WebViewer enforce security with user names and passwords. Both applications manage user accounts individually and in groups. Access groups simplify the process of assigning privileges to individual users, because they define a set of privileges for each type of user. This chapter explains security in the following topics:

- Cisco EMF User Accounts, page 4-1
- Cisco MGX 8260 Media Gateway User Accounts, page 4-3
- Cisco MGM Community String Configuration, page 4-4

Cisco EMF User Accounts

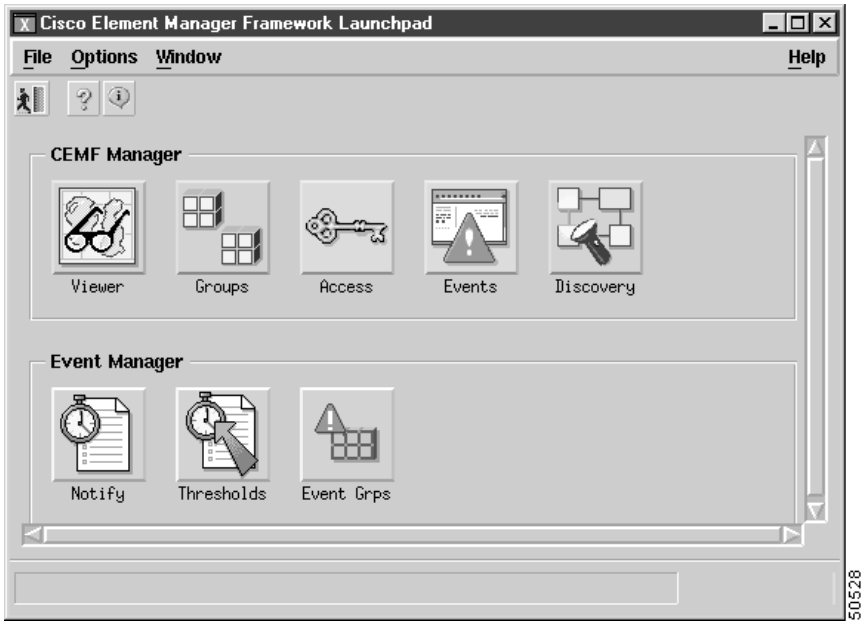
Cisco EMF enforces security with the following types of accounts.

Table 4-1 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

Cisco EMF user accounts can be grouped by an administrator. These user groups can be used to model user roles; for example, administrators typically set up a user group for administrative users and system operators. These features are available from the Access application, launched from the Cisco EMF Launchpad (see Figure 4-1).

Figure 4-1 Cisco EMF Launchpad



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

Changing Passwords

All users can change your own password; 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** box.

Step 4 Enter a new password in the **New Password** box, and re-enter the new password to verify your choice.

Step 5 Click **Apply**.

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 MGX 8260 Media Gateway User Accounts

The Cisco MGX 8260 Media Gateway enforces security with user accounts and access levels. Users must log onto the Cisco MGX 8260 Media Gateway before performing any task, and authenticated users can perform only those tasks permitted by their access level. The Cisco MGX 8260 Media Gateway supports up to 20 user accounts, each with access privileges ranging from full control to guest.

Table 4-2 User Accounts and Access Privileges

Access Level	Account type	Privileges
1	SuperUser	Access all features
2	Administrator	Configure and view all features except user profiles and community strings
3	Provisioning	Configure and view system, port, lines, end points, and connections
4	Maintenance	Access selected level 3 commands
5	Operator	View system, port, lines, end points, and connections
6	Guest	View system, common lines and ports

A new system has a default SuperUser account. To prohibit unauthorized access to the equipment, replace the default account with a unique one and create new accounts for other personnel.

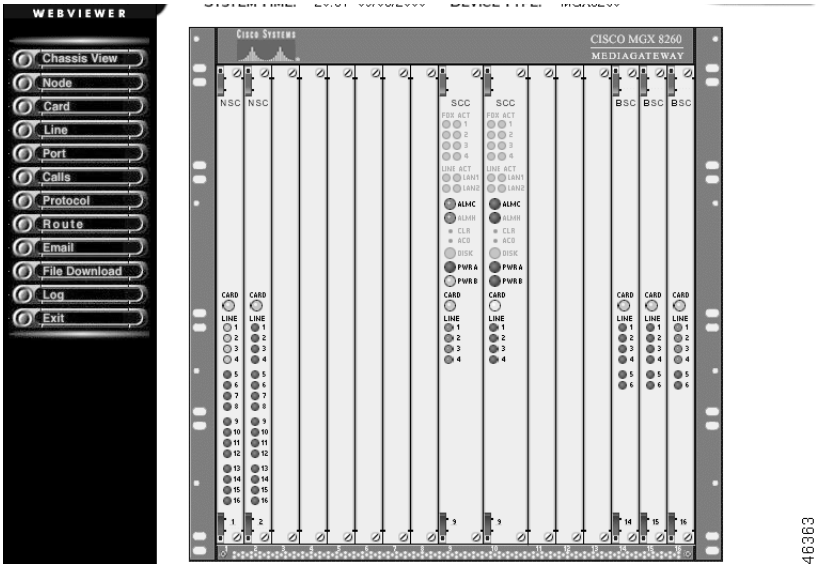
Setting Up Accounts

You control access by configuring accounts and monitoring usage. The following information pertains to access control:

- Accounts—User number, name, password, and access level
- Logins—Users, hosts, and session statistics

You manage user accounts from the Cisco WebViewer user profile screen (see Table 4-2).

Figure 4-2 User Profile Screen



The following table summarizes the Cisco WebViewer support for system parameter configuration.

Table 4-3 System Configuration Map

Configuration Task	Navigation Tree Selection	Screen	Screen Link
User account management	Node>User Profile	User Profile	**+** to add **i** to modify **-** to delete
Change password	Node>User Profile>Change Password	New Password Setting	none
View active logins	Node>User Profile>Login Session	User Session	none

Cisco MGM Community String Configuration

When Cisco MGM communicates with Cisco MGX 8260 Media Gateways, security is enforced with password-like community strings. SNMP communities group workstations and servers (or gateways) that can manage the Cisco MGX 8260 Media Gateway according to their access privileges.

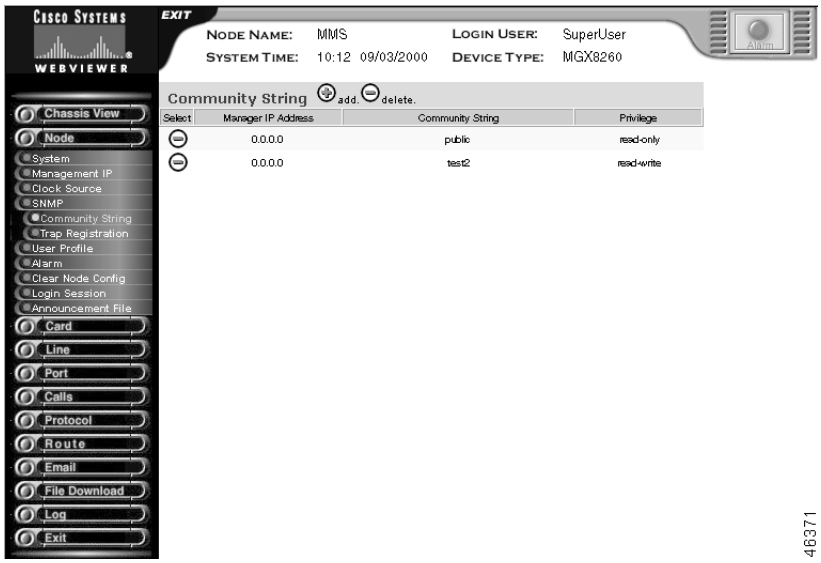
Cisco MGM uses the default public community string to read Cisco MGX 8260 Media Gateway information during automatic discovery and subchassis synchronization processes. For Cisco MGM to configure Cisco MGX 8260 Media Gateways, both must agree on a community string. Community string configuration is a multistep process, starting with each Cisco MGX 8260 Media Gateway and ending with the Cisco MGM that manages them.

Initializing Cisco MGX 8260 Community Strings

You can configure up to 15 community strings for the Cisco MGX 8260 Media Gateway. Community strings define the IP address, string, and privilege.

You configure community strings from the Cisco WebViewer community string screen (see Table 4-3).

Figure 4-3 Community String Screen



The following table summarizes the Cisco WebViewer support for community string configuration.

Table 4-4 MGX 8260 Community String Configuration Map

Configuration Task	Navigation Tree Selection	Screen	Screen Link
Configure community strings	Node>SNMP>Community String	Community string	**+** to add **-** to delete
Register traps	Node>SNMP>Trap Registration	Trap registration	**+** to add **i** to change **-** to delete

Initializing Cisco MGM Community Strings

When configuring community strings for Cisco MGM, consider the following points:

- You need to know the Cisco MGX 8260 Media Gateway community strings when configuring Cisco MGM. The read community string you specified for autodiscovery is the default read community for all the managed objects on the Cisco MGX 8260 Media Gateway and its children. The default write community for Cisco MGM is public.
- Always use the **Open SNMP Community String Configuration Dialog ...** from the chassis or site level to modify read and write community strings.
- The connection between Cisco MGM and each Cisco MGX 8260 Media Gateway has its own community string. Therefore, there are multiple community string values, one for each managed object. The dialog box only displays the last value stored locally.

To configure Cisco MGM community strings, follow these steps:

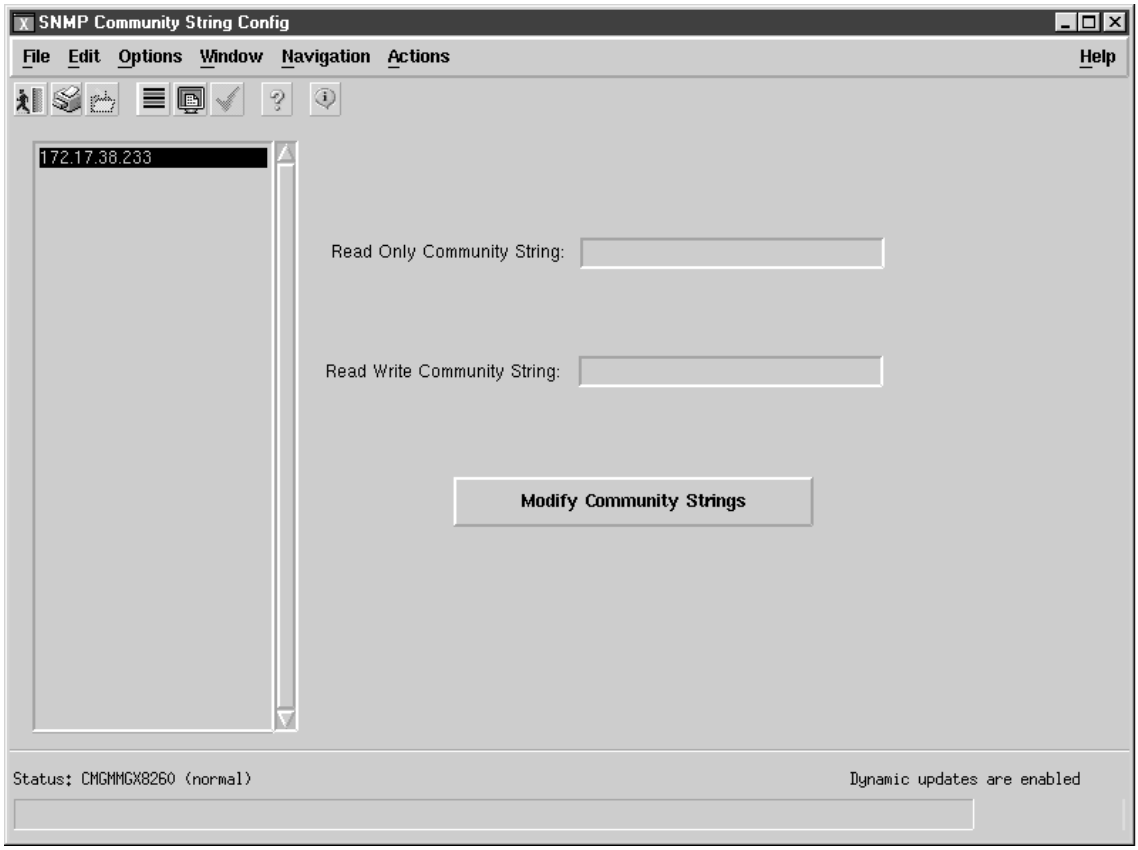
Step 1 Log onto Cisco MGM.

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

Step 3 Expand the object tree and right-click on the desired site or object; then click **Open SNMP Community String Configuration Dialog**.

The SNMP Community String Config dialog box opens (see Figure 4-4).

Figure 4-4 SNMP Community String Dialog Box



Note For security reasons, the form does not display the current community string values.

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

Step 5 Type a read-only community string in the Read Only Community String field.

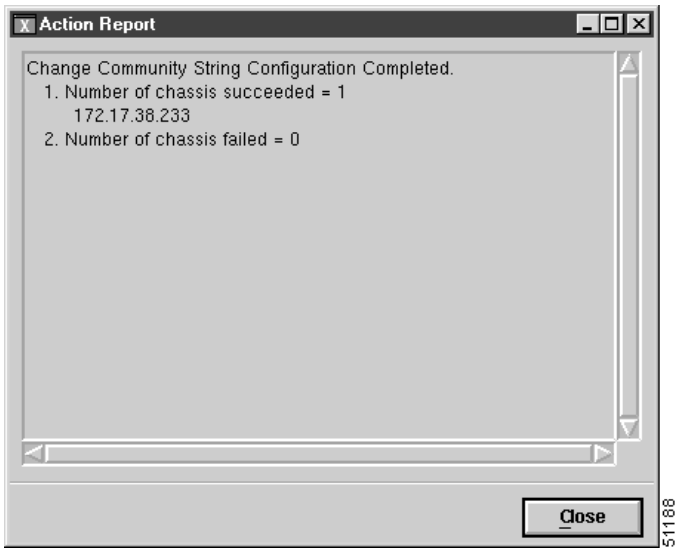
Step 6 Type a read-write community string in the Read Write Community String field.

Step 7 Click **Modify Community Strings**.

Note Cisco EMF 3.1 scrambles the community strings, so you can not view them later.

A confirmation screen opens that reports the successful and unsuccessful configuration attempts (see Figure 4-5).

Figure 4-5 Action Report Dialog Box



Step 8 Click **Close**.

CHAPTER 5

Network Management

Cisco MGM automatically discovers network elements and displays them on the Map Viewer screen. From this map you can view operational status and navigate to screens that support node configuration and software upgrades. This chapter includes the following network management topics:

- Cisco MGM Sites, page 5-1
- Site Discovery, page 5-1
- Inventory Discovery, page 5-2
- Downloading Software Images and Configuration Files, page 5-4
- Upgrading Card Software, page 5-5

Cisco MGM Sites

Cisco MGM organizes Cisco MGX 8260 Media Gateway nodes by site. An MGX 8260 site contains all nodes with the same sysLocation attribute. The autodiscovery procedure queries the sysLocation value of each MGX 8260 chassis it discovers, and either adds the chassis to an existing site or creates a new one for it. If the sysLocation of a MGX 8260 chassis is an empty string, then it is added to default Cisco MGM site. MGX 8260 sites are displayed in hierarchy display only, not in the topology map. A Cisco MGM site remains in the system even if you delete all its nodes. Use **Deployment>Delete Object** to remove an empty site.

For more information on configuring the sysLocation, see Configuring System Parameters, page 7-1.

Site Discovery

Automatic discovery occurs in two phases:

1. Automatic discovery of MGX 8260 nodes in a subnet
2. Subchassis synchronization of MGX 8260 subcomponents

You initiate Automatic Discovery from the Cisco EMF GUI by specifying the desired IP address range. Cisco EMF then automatically discovers MGX 8260 nodes with IP addresses that fall within this range. For more information, see the "Cisco MGM Community String Configuration" section on page 4-4.

Invoking Automatic Discovery

When you initiate automatic discovery, Cisco EMF pings each IP addresses in the given range. If a response is received, it initiates an SNMP GET request for the enterprise object id (OID). If the OID matches any of the predefined Cisco EMF Class mappings, such as MGX 8260, an object of that class is created and displayed. If no mapping is found, the process creates a generic SNMP device under the Physical level of the hierarchy. Generic devices can't be managed.

To discover network elements, follow these steps:

Step 1 Start Cisco EMF.

```
<CEMF_ROOT>/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.

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 MGX 8260 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 8260 Media Gateway and displays them on the user interface. This process is automatically invoked after autodiscovery.

Subchassis discovery inspects SNMP MIBs for the following configurable objects:

- MGX 8260 Chassis and Status
- MGX 8260 Card Configuration and Status, including SCC, NCC, BSC, and DMC cards
- MGX 8260 Line Configuration and Status, including DS1, DS3, SONET, Fast Ethernet, and D channel
- ISDN Configurations, including Dlsap Profile and Macsap Profiles
- Backhaul Session Configurations, including Sets, Groups, and Sessions

Upon completion of subchassis discovery, 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 MGX 8260 icons. Similarly, you can expand the hierarchy to display lines by clicking the **+** sign next to each card. A number next to the MGX 8260 object indicates the number of contained cards or lines.

The SCC contains either SONET or Fast Ethernet lines. The NSCs contain Dsx1or E1 lines. The BSCs contains Dsx3 lines, which may be channelized for Dsx1 lines. DMCs contain Dsx3 lines that map to NSC Dsx1 lines.

Manual Initiation of Subchassis Synchronization

You can manually invoke the subchassis syncup process from the pulldown menu of Cisco EMF GUI. The subchassis discovery process retrieves subchassis component information from each Cisco MGX 8260 Media Gateway and displays corresponding objects on the 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 Expand the tree of objects to display the list of MGX 8260 sites and nodes.

Step 4 Right click the desired site or MGX 8260 node; then click **Open SubChassis Sync Up**. The SubChassis Sync Up screen opens.

Step 5 Select the desired MGX 8260 nodes from the list.

Step 6 Click **Start Sync Up**.

The system synchronizes the user display with subchassis components.

Periodic Subchassis Synchronization

Periodic subchassis synchronization discovers the subchassis components of each Cisco MGX 8260 Media Gateway 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.

Downloading Software Images and Configuration Files

The software download feature facilitates downloading of software image files for the System Controller Card (SCC), Narrowband Service Card (NSC), and Broadband Service Card (BSC) on multiple systems. Downloading the software does not automatically activate it; the system continues to operate on the current software until you perform the upgrade procedure. When downloading software images, Cisco MGM accepts a list of MGX 8260 nodes and the fully-qualified name of the image or configuration file. After download, the system reports successes and failures by chassis name.

To download software, 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 Expand the tree of objects to display the list of MGX 8260 sites and nodes.

Step 4 Right-click on the icon for the desired site; then click **Open Software DownLoad Dialog**. The Software Downlaod screen opens.

Step 5 Select one or more MGX 8260 nodes from the list.

Step 6 Enter the file information:

Field	Description
Image/Config Source File Name	The fully-qualified name and path of the file to download.
Image/Config Destination File Name	The name of the software image or configuration file. The file format for a software image is: <card type>_<software version>.img.<key> The card type is scc, bsc, or nsc. The version indicates the major release, minor release, and version. The file extension is .img for software images and .cnf for configuration files. The key is the tftp security key for the destination chassis. You can view the key using the MGX 8260 command, **lskey**. For example: scc_r01.02.03.img.123456 indicates SCC software for release 1.2.3. The release and version information (r01.02.03) must be exactly 9 characters in length; the key (123456) is exactly 6 characters long.

Step 7 Click **Start Image/Config File Download**.

The system downloads the software to each chassis and reports the results.

Step 8 Repeat steps 1 to 4 for other card images. Each card type in your system, such as SCC or BSC, has its own software image file.

Upgrading Card Software

The upgrade process for redundant cards is graceful and does not interrupt service. When you invoke the process, the system upgrades and restarts only the standby card. You then have the option to commit or cancel the upgrade. When you commit the software, the system switches to the standby card and then upgrades the other card.

Warning **Upgrading nonredundant cards interrupts service. Perform nonredundant upgrades during light traffic periods or during a prearranged maintenance window.**

Although you can download software in bulk to multiple nodes, you have to upgrade the software image manually, one card type at a time. You perform this task from the Cisco WebViewer tool.

To upgrade the software image:

Step 1 Initiate a Cisco WebViewer session with the Cisco MGX 8260 Media Gateway. For more information, see the "Cisco WebViewer Sessions" section on page 3-4.

Step 2 Log in as the SuperUser or a user with level 1 privileges

Step 3 Click **Card>Up/Down Grade**. The Upgradeable or Downgradeable Logical Card display opens.

Step 4 Click the **+** icon for the card you want to upgrade. The Upgrade Software Image and DBM form opens.

Step 5 Specify the name of the upgrade file.

Parameter	Description
Upgrade FileName	The name of the software image. This name indicates the card type, major release, minor release, and version, followed by the .fw extension. For example, SCC_R01.02.03.FW indicates SCC software release 1.2.3. The release and version information (R01.02.03) must be 9 characters in length. This name is the same as the downloaded file name except for the extension.

Step 6 Click **Up-Grade**.

Step 7 For redundant cards, click **Up-Grade Commit**. The system switches to the standby card and upgrades the other one. If you don't want to use the new software, click **Up-Grade Cancel**.

Note You cannot cancel an upgrade for nonredundant cards.

Step 8 For redundant BSC or NSC upgrades, force a switchback. This is important because the standby card cannot protect the active card. To force a switchback, click **Card>All-Cards**; then click the **S** icon of the desired card.

Step 9 Repeat this procedure for each card type and each Cisco MGX 8260 Media Gateway.

CHAPTER 6

Fault and Performance Management

Fault and performance management includes the following topics:

- Monitoring Alarms and Events, page 6-2
- Launching the Event Browser, page 6-5
- Viewing Cisco MGM Logs, page 6-5
- Registering Cisco MGX 8260 Traps, page 6-5
- Monitoring Alarms from the Cisco WebViewer, page 6-7
- Monitoring Performance from the Cisco WebViewer, page 6-8

Alarm Management

The Cisco MGM Alarm component, which is a customized component of the CEMF3.1 platform, handles Cisco MGX 8260 Media Gateway alarms and events. Cisco MGM receives alarm and event messages from managed objects and displays them in the Map Viewer and Event Browser. The Map Viewer 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 8260 Media Gateway to forward. You register traps using the Cisco WebViewer tool. You can also view MGX 8260 alarms and events directly from the Cisco WebViewer.

Performance Management

The Cisco MGX 8260 Media Gateway reports performance information for DS1, E1, DS3, and SONET lines. In addition, you can set performance thresholds and assign alarm severities that the nodes report. You view this information using the Cisco WebViewer tool. For more information, see the "Cisco WebViewer Sessions" section on page 3-4.

An optional product, the Cisco Voice CORBA Gateway, forwards Cisco MGX 8260 Media Gateway performance information to higher-level managers.

Monitoring Alarms and Events

You can monitor alarms and events from two screens:

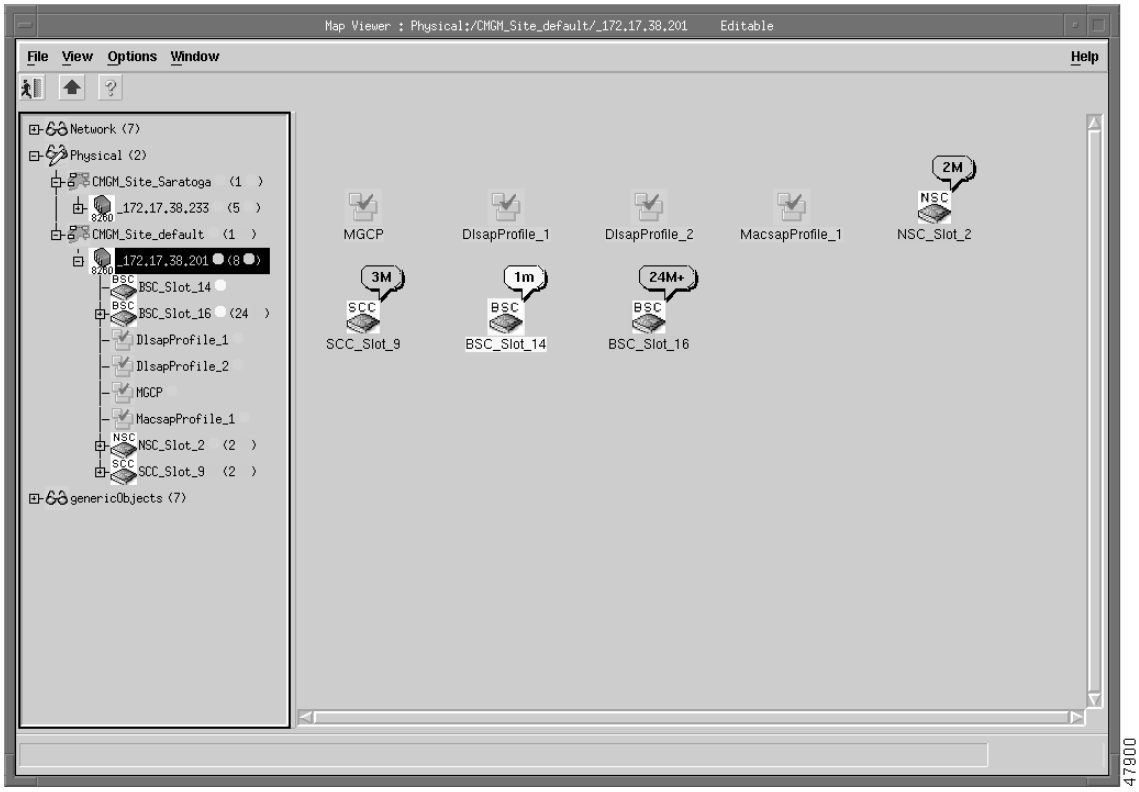
- Map Viewer—Shows icons that indicate the most severe alarm
- Event browser—Shows a table of alarms and events

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*; these sections are provided only as an orientation.

Map Viewer Display

For Cisco MGM, the Map Viewer displays information about the Cisco MGX 8260 nodes, cards, and other network equipment (see Figure 7-1).

Figure 6-1 Cisco MGM Topology View

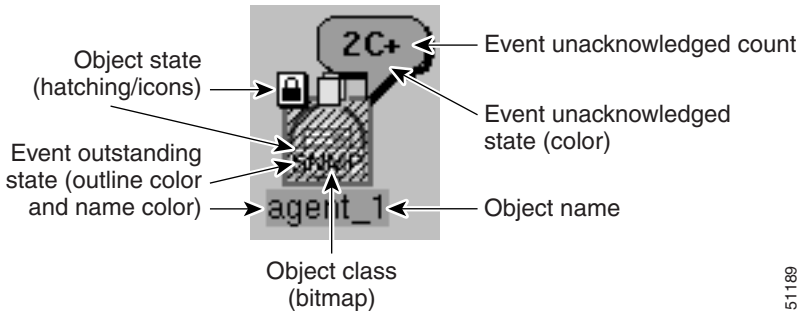


Each object shown in the right window provides graphical cues about its network element. The information can be structural information, for example, a network element name, or state and event information, such as “out of service.” If an object becomes unreachable, it displays as a bomb icon.

Each object may 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 6-2 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 7-1.

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

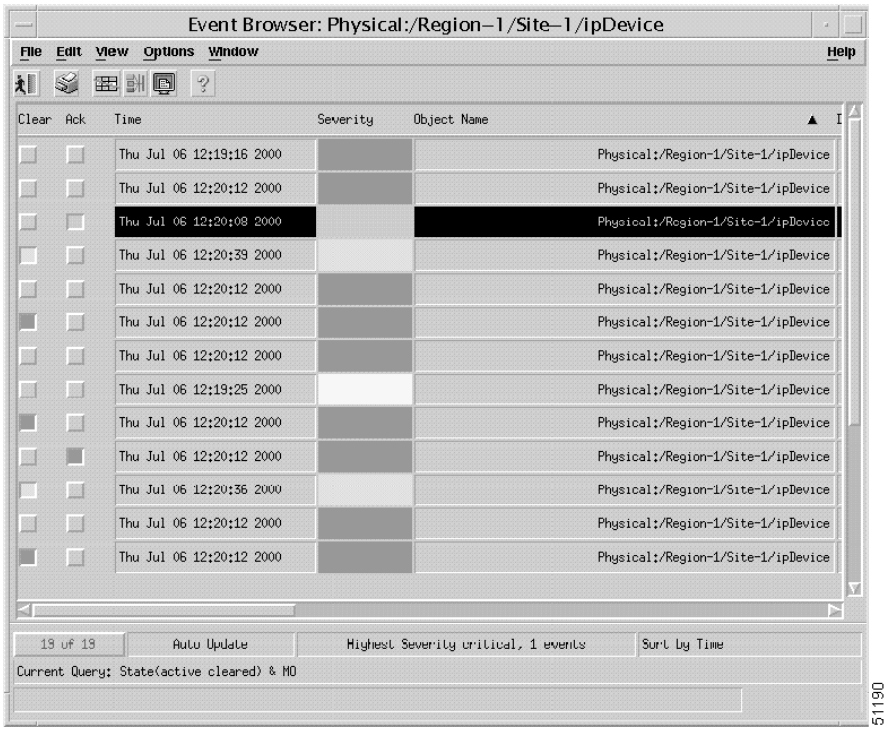
When the event status of an object changes in the network, the graphical cues change to reflect the new status.

Event Browser Display

The event status of objects contained in a map can affect the event status of the parent icon. In other words, if the event status changes on a map object, this is propagated to the parent icon. The event status 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 Figure 6-3 is displayed.

Figure 6-3 Cisco EMF Event Browser Window



The Event Browser provides a tool to manage the network efficiently; you can list, query, and sort all or some events according to how you want to manage the network. Services can be invoked on events so faults can be attended to from the window that shows the event.

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

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

- Object name (the managed resource name)
- Time the event was raised
- Severity of the event (color-coded), refer to the "Alarm Severity Colors and Codes" section on page 6-3
- Description of the event

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

- Clear (an indicator to show if an event is active or cleared)
- Ack (an indicator to show if 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, this button can be deselected so the event can be reassigned. The Clear button is highlighted when the fault has been rectified to indicate 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 select the **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. The following table summarizes the important logs:

Table 6-2 Log Files

File	Description
<CEMF_ROOT>/logs/cmgmCtlr.log	Controller event log
<CEMF_ROOT>/logs/LogercmgmCtlr.log	Cisco MGM-specific log

Registering Cisco MGX 8260 Traps

Cisco MGX 8260 Media Gateway nodes notify Cisco MGM of alarms and events using trap messages. Before Cisco EMF can display alarms, you must register traps at each MGX 8260 node.

When working with traps, you configure the following parameters:

- Manager address—The IP address of the Cisco MGM manager to receive traps
- Community string—The SNMP community strings for read and read-write access
- Trap registrations—The specific conditions to report and their severity

You register traps using the Cisco WebViewer. The following table summarizes the Cisco WebViewer procedures for trap registration and community string configuration. for more information, see the "Cisco MGM Community String Configuration" section on page 4-4.

Table 6-3 Trap Registration Map

Configuration Task	Navigation Tree Selection	Screen	Screen Link
Trap configuration	Node>SNMP>Trap Registration	Trap Registration	**+** to add **i** to change **-** to delete
Community string configuration	Node>SNMP>Community String	Community String	**+** to add **-** to delete

The Cisco MGX 8260 Media Gateway supports the following trap categories:

Table 6-4 Trap Categories

Bit	Trap	Description
0	Severity	Major (trap severity selection)
1	Severity	Minor (trap severity selection)
2	Severity	Information (trap severity selection)
3	1000 to 1099	Shelf
4	1100 to 1199	Card
5	1200 to 1299	SNMP
6	1300 to 1399	Dsx1 Line
7	1400 to 1499	Dsx3 Line
8	1500 to 1599	Sonet Line
9	1600 to 1699	Ether Line
10	1700 to 1799	Voice Port
11	–	Ether Channel
12	–	Voice Channel
13	1800 to 1899	EMM
14	1900 to 1999	Clock
15	2000 to 2099	DSP
16	2100 to 2199	DMCMAP
17	2200 to 2299	ISDN
18	2300 to 2399	MGCP
19	2400 to 2499	Backhaul Session

The Cisco WebViewer displays the entire list of traps on the configuration forms.

Monitoring Alarms from the Cisco WebViewer

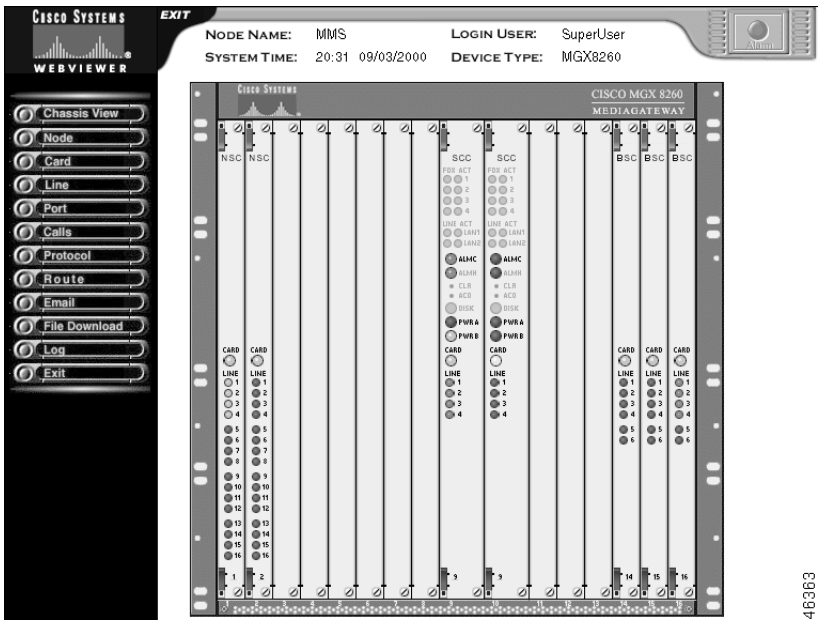
The Cisco MGX 8260 Media Gateway notifies maintenance or operations personnel about equipment alarms at several levels:

- Shelf
- Card
- Line

You can view the event log for notices about changes in the system. For example, inserting a new card adds an event to the log.

The WebViewer displays the most severe alarm in the upper right corner of every screen (see Figure 6-4).

Figure 6-4 Chassis View with Alarms



The alarm indicator is a rectangular icon, which is green for normal operation and flashes red or yellow for alarms. You can obtain more information about the alarm by clicking the alarm indicator.

The chassis view also shows a graphical representation of the front panel, including alarm indications for each card. To obtain more information about a specific card, click the corresponding Card or Line indicator.

The Cisco MGX 8260 Media Gateway reports the alarms from the following sources:

- Alarm status
- Card alarms
- DS1, E1, DS3, Fast Ethernet, and SONET alarms
- Environmental alarms

The following table summarizes the Cisco WebViewer support for monitoring alarms.

Table 6-5 Alarm Surveillance Map

Surveillance Task	Navigation Tree Selection	Screen	Screen Link
View alarm status	Node>Alarm	Alarm Status	**i** for environmental
View card alarms	Card>All-Cards	Physical Slot Configuration	**i** for card details
View DS1 alarms	Line>Dsx1-T1>All-Lines	Dsx1-T1 Line Configuration	**i** for line details
Set DS1 alarm thresholds	Line>Dsx1-T1>All-Lines	Dsx1-T1 Line Configuration	**A** for thresholds
View E1 alarms	Line>Dsx1-E1>All-Lines	Dsx1-E1 Line Configuration	**i** for line details
Set E1 alarm thresholds	Line>Dsx1-E1>All-Lines	Dsx1-E1 Line Configuration	**A** for thresholds
View DS3 alarms	Line>Dxs3>All-Lines	Dsx3 Line Configuration	**i** for line details
Set DS3 alarm thresholds	Line>Dsx3>All-Lines	Dsx3 Line Configuration	**A** for thresholds
View SONET alarms	Line>Sonet>All-Lines	Sonet Line Configuration	**i** for card details
Set SONET alarm thresholds	Line>Sonet>All-Lines	Sonet Line Configuration	**A** for thresholds
View Fast Ethernet alarms	Line>Ether>All-Lines	Ether Line Configuration	
View trap log	Log>Trap Log	Trap Log	

Monitoring Performance from the Cisco WebViewer

The Cisco MGX 8260 Media Gateway reports performance statistics for the following lines:

- DS1 performance, real-time and interval statistics
- E1 performance, real-time, and interval statistics
- DS3 performance, real-time and interval statistics
- SONET performance, real-time and interval statistics for section, path, and line segments

The following table summarizes the Cisco WebViewer support for monitoring performance.

Table 6-6 Performance Surveillance Map

Surveillance Task	Navigation Tree Selection	Screen	Screen Link
View DS1 performance	Line>Dsx1-T1>All-Lines	Dsx1-T1 Line Configuration	**C** for performance
View real-time DS1 statistics	Line>Dsx1-T1>Counters and Alarm	T1 Line Counters/Alarm	
View interval DS1 statistics	Line>Dsx1-T1>All-Lines	Dsx1-T1 Line Configuration	**P** for statistics
View E1 performance	Line>Dsx1-E1>All-Lines	E1 Line Configuration	**C** for performance
View real-time E1 statistics	Line>Dsx1-E1>Counters and Alarm	E1 Line Counters/Alarm	
View interval E1 statistics	Line>Dsx1-E1>All-Lines	E1 Line Configuration	**P** for statistics
View DS3 performance	Line>Dxs3>All-Lines	Dsx3 Line Configuration	**C** for performance
View real-time E1 statistics	Line>Dsx3>Counters and Alarm	Dsx3 Line Counters	

Table 6-6 Performance Surveillance Map (continued)

Surveillance Task	Navigation Tree Selection	Screen	Screen Link
View interval E1 statistics	Line>Dxs3>All-Lines	Dsx3 Line Configuration	**P** for statistics
View SONET performance	Line>Sonet>All-Lines	Sonet Line Configuration	**C** for performance
View real-time SONET section statistics	Line>Sonet>Section Performance	Sonet Section Counters	–
View real-time SONET line statistics	Line>Sonet>Line Performance	Sonet Line Counters	–
View real-time SONET path statistics	Line>Sonet>Path Performance	Sonet Path Counters	–
View interval SONET statistics	Line>Sonet>All-Lines	Sonet Line Configuration	**S** for section **L** for line **P** for path

CHAPTER 7

Cisco MGX 8260 Node Management

You configure Cisco MGX 8260 Media Gateway nodes from the Cisco WebViewer (see the "Cisco WebViewer Sessions" section on page 3-4). This chapter includes the following topics:

- Configuring System Parameters, page 7-1
- Configuring the Management Interfaces, page 7-2
- Synchronizing the System Clock, page 7-2
- Configuring Lines, page 7-3
- Configuring Voice Ports, page 7-4
- Viewing Active Calls, page 7-4
- Understanding MGCP, page 7-5
- Configuring MGCP, page 7-5
- Understanding Sessions, page 7-6
- Configuring Sessions, page 7-7
- Understanding ISDN D Channels Usage, page 7-7
- Configuring D Channels, page 7-8
- Configuring IPDC, page 7-9
- Managing Announcement Files, page 7-10

Configuring System Parameters

The Cisco MGX 8260 Media Gateway system parameters include the following:

- General system parameters—Rack and node information
- System group parameters—Location, status, and services information
- DS1 mode—Operational mode for the chassis, either DS1 or E1
- Protocol mode—Call control mode for the chassis, either MGCP or IPDC
- Date and time

The following table summarizes the Cisco WebViewer support for system parameter configuration.

Table 7-1 System Configuration Map

Configuration Task	Navigation Tree Selection	Screen	Screen Link
System and group parameters, DS1 mode, or protocol mode	Node>System	System Configuration	Set
Date and time	Node>System	System Configuration	Set

Configuring the Management Interfaces

You configure the MGX 8260 management interface for local or remote operation by setting the appropriate IP addresses and management paths. Assign management IP addresses for each of the following management interfaces that you plan to use:

- Ethernet 10BaseT management interface—IP addresses for the interfaces
- IP route setup—Destination, gateway, protocol, and routing table information

Note If you change the IP address of the port the WebViewer is using, you will interrupt the session.

The following table summarizes the Cisco WebViewer support for management interface configuration.

Table 7-2 Management Interface Configuration Map

Configuration Task	Navigation Tree Selection	Screen	Screen Link
IP addresses	Node>Management IP	Management IP Settings	**Set**
IP route setup	Route>IP Route Setup	IP Route	**I** for details **+** to add a route **-** to delete a route

Synchronizing the System Clock

The MGX 8260 clock module has three synchronization options:

- Building Integrated Timing Source (BITS)—A high quality timing source that synchronizes all equipment in the building
- Line—A clock derived from the SONET, DS3, or DS1 line
- Local—An internal MGX 8260 timing source

You assign one clock as the primary source and another as the secondary source. When using the line clock source, specify both the line and slot associated with the source.

During normal operation, the primary clock is the active source and the secondary clock is the backup. If the active source fails, the Cisco MGX 8260 Media Gateway switches to the backup clock and reports an alarm. Also, you can switch to the backup source manually. This section explains how to set primary and secondary clocks and view clock status.

The following table summarizes the Cisco WebViewer support for clock source configuration.

Table 7-3 Clock Source Configuration Map

Configuration Task	Navigation Tree Selection	Screen	Screen Link
Primary and secondary clock source for serial lines	Node>Clock Source	Clock Source	**Set**
Switching clock sources	Route>Clock Source	IP Route	**Switch Clock Source**

Configuring Lines

Line and port management screens facilitate viewing, configuring, and deleting voice and data services. The following list summarizes the line configuration parameters:

- DS0—Line number, port, and operational status
- DS1 or E1—Line number, port, parameters, and operational status
- DS3—Line number, port, parameters, and operational status
- DMC mapping—Source and destination DS1 and DS3 lines
- Fast Ethernet—IP address, gateway, protocol, and operational status
- Static Route—Destination, line, port, and priority

Note The DS1 and E1 modes are mutually exclusive.

The DMC maps source DS1 channels from the DS3 interface to destination DS1 channels on the NSCs. The mapping is one-to-one and can connect any source DS1 to any destination DS1.

Note The NSC should be in the backplane more for correct DMC operation.

Table 7-4 Line Configuration Map

Task	Navigation Tree Selection	Screen	Screen Link
View all lines	Line>All-Lines>All-Lines	Common Line	**i** for details
DS0 channel configuration	Line>Dsx0>All-Dsx0	Dsx0 Status	**-** to delete
DS1 line configuration	Line>Dsx1-T1>All-Lines	Dsx1-T1 Line Configuration	**+** to add **i** to change **-** to delete
E1 line configuration	Line>E1>All-Lines	E1 Line Configuration	**+** to add **i** to change **-** to delete
DS3 line configuration	Line>Dsx3>All-Lines	Dsx3 Line Configuration	**+** to add **i** to change **-** to delete

Table 7-4 Line Configuration Map (continued)

Task	Navigation Tree Selection	Screen	Screen Link
DMC line mapping	Line>DMC T3-T1 Mapping	DMC T3-T1 Mapping	**+** to map **i** to change **-** to delete
Fast Ethernet line configuration	Line>Ether>All-Lines	Ether Line Configuration	**+** to add **i** to change **-** to delete
Fast Ethernet admin status change	Line>Ether>All-Lines	Ether Line Configuration	**Link Up** or **Link Down**
OC-3 line configuration	Line>SONET>All-Lines	Sonet Line Configuration	**+** to add **i** to change **-** to delete
SONET E-RDI and trace configuration	Line>SONET>All-Lines	Sonet Line Configuration	**i** to change

Configuring Voice Ports

This section describes the procedure for viewing, adding, or changing voice ports. Voice ports identify the physical location and characteristics of a voice interface at a DS0 level. A Media Gateway Controller manages SVC (Switched Virtual Circuit) end points and connections.

The Cisco MGX 8260 Media Gateway identifies a voice port by a logical port number that is independent of the port's physical location. The following parameters describe the physical location:

- Slot number
- Port number
- DS0 number

NSC lines always need a voice port configured; BSC lines have a default configuration. When you add or change a voice port, you associate a logical port number with these physical descriptors. Voice ports have settings for dejitter, packet loading, and other voice parameters.

Table 7-5 Voice Port Configuration Map

Task	Navigation Tree Selection	Screen	Screen Link
View all ports	Port>All-Ports	Common Port	**i** for details
View voice ports	Port>Voice>All-Ports	Voice Port Configuration	**+** to add **i** to change **-** to delete

Viewing Active Calls

Active call information is useful for audits or trouble analysis. The Cisco MGX 8260 Media Gateway displays active calls as follows

- Viewing calls by physical resource
- Viewing calls by transaction

The following table summarizes the Cisco WebViewer support for active calls:

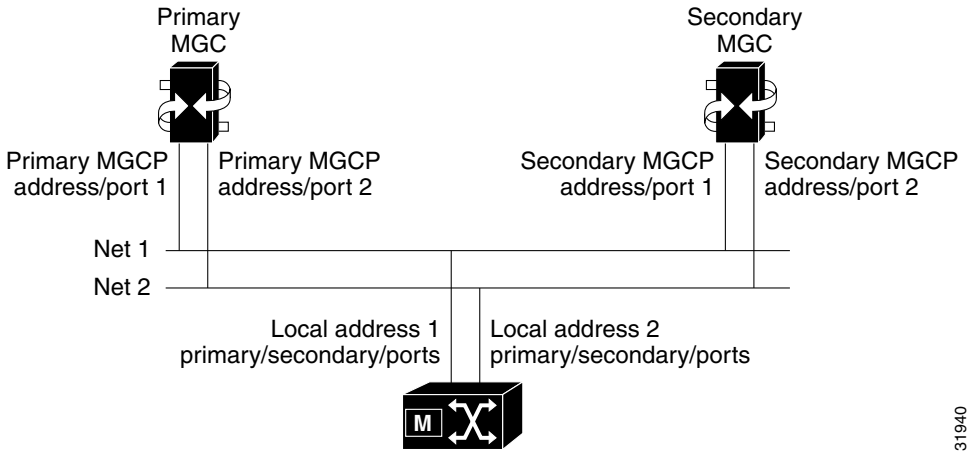
Table 7-6 Active Call Status Map

Task	Navigation Tree Selection	Screen	Screen Link
View calls by resource	Calls>Physical Calls>All-Calls	Active Call Physical Table	None
View calls by transaction	Calls>All-Calls>All-Calls	Active Call Physical Table	None

Understanding MGCP

This section describes how to configure and view MGCP (Media Gateway Control Protocol). The following diagram shows how to configure MGCP IP addresses in a fullyredundant system (see Figure 7-1).

Figure 7-1 MGCP Addresses and Ports



A non-redundant system consists of a primary MGC network, the Cisco MGX 8260 Media Gateway, and an IP network. You can add the secondary network or MGC for more reliable operation.

Configuring MGCP

To configure MGCP, you perform the following tasks:

- Set the domain name
- Set IP addresses and ports—The primary MGC, secondary MGC, and local addresses
- Configure MGCP core settings—The protocol timers and retry settings
- View message statistics
- Set MPC scalars—The voice channel encoding type, echo cancellation, and so on

The following table summarizes the Cisco WebViewer support for MGCP:

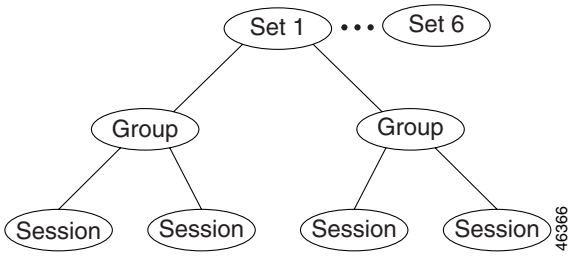
Table 7-7 MGCP Configuration Map

Task	Navigation Tree Selection	Screen	Screen Link
Switch from IPDC to MGCP	Node>System	System Configuration	**Set**
View connection status	Protocol>MGCP>Default	MGCP Default Setting	
Domain name configuration	Protocol>MGCP>Default	MGCP Default Setting	**Set**
IP address configuration for primary MGC, secondary MGC, and local port	Protocol>MGCP>Default	MGCP Default Setting	**Set**
Core MGCP parameter configuration	Protocol>MGCP>Core	MGCP Core Setting	**Set**
View message statistics	Protocol>MGCP>Message Stats	MGCP Message Statistics	
Default call setup parameters	Protocol>MGCP>MPC Scalars	MPC Scalar	**Set**

Understanding Sessions

The session manager organizes individual sessions into groups and sets (see Figure 7-2).

Figure 7-2 Organization of Sessions

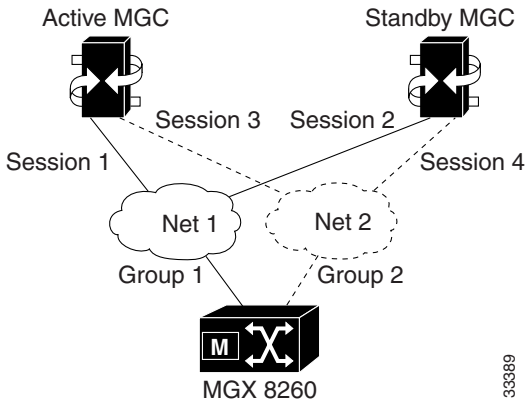


The backhaul sessions and groups include the following components:

- Session—A connection between two points, defined by a local IP address and port and a remote IP address and port. The Cisco MGX 8260 Media Gateway supports four sessions per set, two for each session group.
- Session Group—A collection of one or more sessions for a single MGC. Typically, the individual sessions implement network redundancy. The Cisco MGX 8260 Media Gateway supports two session groups per set.
- Session Set—A collection of session groups, typically used to group session groups for redundant MGCs. The Cisco MGX 8260 Media Gateway supports up to six session sets for a total of up to 24 sessions.

When adding sessions, you create a structure that supports reliable operation. The goal for a fully redundant system is to provide multiple management sessions to multiple MGCs via multiple physical networks (see Figure 7-3).

Figure 7-3 Logical Session Model



If the MGC cannot handle all D Channels in one session set, then configure another similar set using different UDP ports and D Channels.

Configuring Sessions

To configure ISDN backhaul signaling, set the following parameters:

- Session sets—The redundancy mode and range of lines to control
- Session groups—The group number and associated session set number
- Sessions—The local IP address and port, and associated group and set numbers

The following table summarizes the Cisco WebViewer support for sessions:

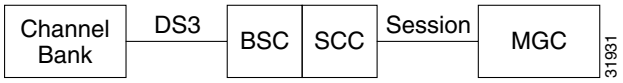
Table 7-8 Session Configuration Map

Task	Navigation Tree Selection	Screen	Screen Link
Session set configuration	Protocol>Backhaul>Set	Session Set	**+** to add **-** to delete
Session group configuration	Protocol>Backhaul>Group	Session Group	**+** to add **-** to delete
Session configuration	Protocol>Backhaul>Session	Session	**+** to add **-** to delete **c** for counters

Understanding ISDN D Channels Usage

The Cisco MGX 8260 Media Gateway extends D Channel signaling to an MGC via a backhaul channel (see Figure 7-4).

Figure 7-4 D Channel to Media Gateway Controller



Each BSC contains 168 T1 lines, each a potential Primary Rate ISDN line. An ISDN line contains 24 channels, one of which is the D Channel that carries the signaling information for the other 23 channels. The BSC card can terminate a D Channel signaling stack and pass the payload to an MGC, via the SCC, using a backhaul session.

The following procedures describe how to configure a D Channel for a backhaul session. The procedures assume you already have a DS3 line, and have provisioned a PRI ISDN line on one of its circuits. ISDN D Channels can be difficult to configure because they have many settings, so the Cisco MGX 8260 Media Gateway simplifies the process by grouping common settings into two types of profiles:

- Digital Link Service Access Profile (DLSAP)
- Media Access Control Service Access Profile (MACSAP)

When adding D Channels, you simply specify suitable profiles that contain the desired configuration set. You can create profiles using default settings that accommodate the signaling requirements for common applications.

Configuring D Channels

The Cisco MGX 8260 Media Gateway simplifies the process of creating D Channels with DLSAP and MACSAP profiles. These profiles provide a template of parameter settings that you apply when adding D Channels. Changes you make to the profiles apply only to lines you subsequently add, not to lines that already exist. If you want to change the configuration of a D Channel, delete it first and then recreate a new one using the new template.

The following section describes the high-level procedure for configuring a D Channel on an existing DS3 trunk:

Step 1 Define a DLSAP profile.

Step 2 Define a MACSAP profile.

Step 3 Define a D Channel on a PRI ISDN line within the DS3 trunk, using the profiles you defined in Steps 1 and 2.

The following table summarizes the Cisco WebViewer support for D Channels:

Table 7-9 D Channel Configuration Map

Task	Navigation Tree Selection	Screen	Screen Link
MACSAP profile configuration	Protocol>ISDN>Macsap Profile	Macsap Profile	**+** to add **-** to delete
D Channel configuration	Protocol>DChan Config	D Chan Config	**+** to add **-** to delete **i** for details **c** for MACSAP counters **A** for DLSAP counters
Viewing LAPD parameters	Protocol>ISDN>Lapd	LAPD Card Table	none

Configuring IPDC

IPDC is an alternative to the MGCP protocol for controlling voice calls through the Cisco MGX 8260 Media Gateway. When using IPDC, you do not have to configure sessions or backhaul channels.

Note Cisco MGM does not support IPDC.

To configure IPDC, configure the following parameters:

- MGCP or IPDC mode
- IP addresses and ports—The IP addresses and health check status for IPDC
- Core settings—The protocol operational timers and settings
- COT tones—The continuity test receive and transmit tones
- IPDC timers—The IPDC link timer settings

The following table summarizes the Cisco WebViewer support for IPDC:

Table 7-10 IPDC Configuration Map

Task	Navigation Tree Selection	Screen	Screen Link
Switch from MGCP to IPDC	Node>System	System Configuration	**Set**
View IPDC status	Protocol>IPDC>Configuration	IPDC Configuration	
IP address configuration	Protocol>IPDC>Configuration	IPDC Configuration, Soft Switch Configuration pane	**Set**
Pseudo IP address configuration for Fast Ethernet ports	Protocol>IPDC>Configuration	IPDC Configuration, Status and Core Setting pane	**Set**
IPDC core protocol settings	Protocol>IPDC>Configuration	IPDC Configuration, Status and Core Setting pane	**Set**
COT configuration	Protocol>IPDC>Configuration	IPDC Configuration, COT Configuration pane	**Set**

Table 7-10 IPDC Configuration Map (continued)

Task	Navigation Tree Selection	Screen	Screen Link
IPDC timer configuration	Protocol>IPDC>Timer	IPDC Timer Configuration	**Set**
IPDC and health check activation	Protocol>IPDC>Configuration	IPDC Configuration, Soft Switch Configuration pane	**Set**

Managing Announcement Files

Announcement files contain voice messages that the system can play for users. The announcement file parameters include the following:

- Message duration
- File ID, name, size, and encoding

The following table summarizes the Cisco WebViewer support for announcement file configuration.

Table 7-11 Announcement File Configuration Map

Configuration Task	Navigation Tree Selection	Screen	Screen Link
View duration information	Node>Announcement File>Duration	Duration Information for Announcement Files	
Activate, deactivate, or remove a file	Node>Announcement File>File	Announcement File	**+** to activate **-** to deactivate **R** to remove

INDEX

A

access control
  changing a password **4-2**
active calls, view **7-4**
alarms, monitor **6-7**
announcement files, manage **7-10**
automatic discovery, invoking **5-2**

C

chassis view **3-6**
Cisco EMF
  required disk space **2-4**
Cisco EMF Launchpad **3-2**
Cisco EMF user session
  quit **3-4**
  start **3-1**
Cisco MGM clients, install **2-7**
Cisco MGM server, install **2-5**
Cisco MGX 8260 media gateway nodes, initialize **2-10**
Cisco WebViewer
  panes **3-5**
  quit **3-8**
  screens
    chassis view **3-6**
    configuration forms **3-7**
    forms **3-7**
    main **3-4**
    status **3-6**
  start **3-4**
community strings
  Cisco MGM **4-5**
  Cisco MGX 8260 **4-5**
community strings, configuration **4-4**

D

D Channels, configure **7-8**
deployment options **2-1**
disk space, required **2-4**

E

event
  outstanding state **6-3**
  status change **6-3**
  unacknowledged count **6-3**
  unacknowledged state **6-3**
Event Browser
  launch **6-5**

F

features
  Cisco Voice Corba Gateway **1-5**
  Cisco WebViewer **1-5**
features, management **1-2**

I

icon
  balloon, event counter **6-3**
  Cisco EMF Launchpad **3-2**
  color **6-3**
  displayed information **6-3**

event number **6-3**
letter, event severity **6-3**
MGX 8260 objects **3-3**
plus sign, event information **6-3**
icon object
class **6-3**
name **6-3**
state **6-3**
installation
changing **2-8**
required disk space **2-4**
inventory discovery **5-2**
IPDC, configure **7-9**
ISDN D Channels **7-7**

L

lines, configure **7-3**
log files **6-5**

M

management **1-2**
management feature
configuration **1-2**
fault **1-2**
performance **1-2**
security **1-3**
management interface, configure **7-2**
management tasks, by interface **1-4**
MGCP **7-5**
MGCP, configure **7-5**

N

netscape browser, install **2-7**

P

performance, monitoring **6-8**
platform requirements **2-4**

R

raw partitions, configuring **2-5**
requirements
software **2-4**
system **2-3**

S

sessions **7-6**
configure **7-7**
sites
about **5-1**
discovery **5-1**
software
download **5-4**
upgrade **5-5**
sub-chassis synchronization
manual **5-3**
periodic **5-3**
system clock, synchronize **7-2**
system parameters, configure **7-1**

T

Telecommunications Management Network **1-1**
telnet sessions **3-8**
tool
launch **3-2**
trap forwarding **2-8**
traps, registration **6-5**

U

uninstalling, Cisco MGM server or client **2-9**
user accounts
  Cisco EMF **4-1**
  Cisco MGM **4-3**
  setting up **4-3**

V

version information, viewing **2-9**
voice ports, configure **7-4**