



## Cisco Media Gateway Controller Node Manager User's Guide 1.0

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

Customer Order Number:  
Text Part Number: 78-11085-01

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 NON-INFRINGEMENT 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.

Access Registrar, AccessPath, Any to Any, Are You Ready, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco *NetWorks* logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, IQ Breakthrough, IQ Expertise, IQ FastTrack, IQ Readiness Scorecard, The IQ Logo, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, *The Cell*, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Aironet, ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, CollisionFree, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document 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. (0005R)

*Cisco Media Gateway Controller Node Manager User's Guide 1.0*  
Copyright © <2000>, Cisco Systems, Inc.  
All rights reserved.



## **Preface xi**

Document Objectives	<b>xi</b>
Audience	<b>xi</b>
Document Organization	<b>xi</b>
Documentation Suite	<b>xii</b>
Cisco MGC Documentation	<b>xii</b>
Cisco Element Management Framework Documentation	<b>xiii</b>
Billing and Measurements Server Documentation	<b>xiii</b>
Document Conventions	<b>xiii</b>
Obtaining Documentation	<b>xiv</b>
World Wide Web	<b>xiv</b>
Documentation CD-ROM	<b>xv</b>
Ordering Documentation	<b>xv</b>
Obtaining Technical Assistance	<b>xv</b>
Cisco Connection Online	<b>xv</b>
Technical Assistance Center	<b>xvi</b>
Documentation Feedback	<b>xvi</b>

---

## **CHAPTER 1**

### **Overview of Cisco Media Gateway Controller Node Manager 1-1**

Introduction	<b>1-1</b>
Terms Used in This Document	<b>1-1</b>
Overview of the Cisco MGC Node Architecture	<b>1-2</b>
Key Features of CMNM	<b>1-2</b>
Overview of CEMF	<b>1-4</b>
CEMF Components	<b>1-4</b>
How CEMF Models the Network	<b>1-5</b>
How CMNM Models the Cisco MGC Node	<b>1-7</b>
Network Interfaces	<b>1-7</b>
Cisco MGC Host Connectivity Network	<b>1-8</b>
Cisco MGC Host Connectivity Objects	<b>1-9</b>
Containment Hierarchy of the Connectivity Network	<b>1-10</b>
Viewing the Network Connectivity Map	<b>1-11</b>

CHAPTER 2

**Installing CMNM 2-1**

- Introduction to CMNM Installation 2-1
- Before You Start 2-1
  - Task Checklist 2-1
- Hardware Requirements 2-1
  - Hard Drive Partitioning 2-2
  - Suggested Layout for Cooked Partitions (CEMF Default) 2-3
  - Suggested Layout for Raw Partitions 2-4
  - Configuring Raw File Systems in ObjectStore 2-4
  - Suggested Layout for the CEMF Client 2-6
- Software Requirements 2-6
- Recommended Performance Enhancements for CEMF 2-6
  - Performance Enhancements for Cooked Partitions 2-7
  - Performance Enhancements for Raw Partitions 2-8
- DNS Requirements 2-9
  - Workstation Uses DNS 2-9
  - Workstation Does Not Use DNS 2-10
- Installing the Cisco Element Manager Framework 2-10
- Installing CMNM 2-10
  - Verifying the Installation of CMNM 2-11
  - Verifying the Installation of CiscoView 5.1 2-12
  - Upgrading CMNM 2-13
  - Upgrading CiscoView 5.1 2-13
- Uninstalling CMNM 2-14
  - Backing Up Your Databases 2-14
  - Uninstalling the CMNM Software 2-14
  - Verifying Uninstallation of CMNM 2-14
- Installing the Cisco MGC Host Provisioning Tool 2-14
- Configuring Reflection 2-14
  - Creating an XDMCP Connection 2-15
  - Fixing the Insufficient Colors Problem 2-15

CHAPTER 3

**Configuring Network Devices for Management 3-1**

- Introduction to Device Configuration 3-1
- Configuring the Cisco MGC 3-1

Configuring a Cisco SLT (2600)	3-2
Configuring a LAN Switch (Catalyst 2900XL)	3-4
Configuring the LAN Switch (Catalyst 5500)	3-5
Configuring the Cisco MGX 8260	3-5
Configuring BAMS	3-6

---

**CHAPTER 4**

<b>Getting Started with CMNM</b>	<b>4-1</b>
Starting a CMNM Session	4-1
Starting Applications from the CEMF Launchpad	4-2
Quitting a CMNM Session	4-4
Using CMNM Tools	4-4
Using the Mouse	4-4
Shortcut Keys	4-5
Selecting from Lists in CMNM	4-5
Using Diagnostic Tools	4-7
Viewing Status Information	4-7
Using the Toolbar	4-8
Enabling the Toolbar	4-8
Disabling the Toolbar	4-8
Showing or Hiding Tooltips	4-9
Printing the View Displayed in the Window	4-9
Closing a Window	4-9
Accessing Help	4-9
Moving Between Open Windows	4-10

---

**CHAPTER 5**

<b>Setting Up CMNM Security</b>	<b>5-1</b>
Introduction to CMNM Security	5-1
Setting Up Accounts	5-4
Setting Up New Accounts	5-4
Creating User Groups	5-8
Creating New Access Specifications	5-11
Creating Typical Types of Users	5-16
Modifying Users	5-16
Modifying User Groups	5-17
Modifying Access Specifications	5-18
Changing the Administrative Password	5-21

CHAPTER 6

**Deploying a Site, Object, or Network 6-1**

- Introduction to Deployment 6-1
  - Meeting Password Requirements 6-1
- Device Inventory 6-1
  - Alternate Cisco MGC Configurations 6-2
  - Cisco SLT and LAN Switch Inventory 6-2
  - Interfaces 6-2
  - Cisco MGC Host Inventory 6-4
  - Connectivity Network Inventory 6-5
- Synchronization 6-5
- Deploying a Network Using a Seed File 6-6
  - Seed File Attributes 6-6
  - Specifying a Deployment Seed File 6-7
- Manually Deploying a Site, Object, or Network 6-9
  - Deployment Attributes 6-10
  - Opening the Deployment Wizard 6-11
  - Deploying a Site 6-11
  - Deploying a Media Gateway Network 6-15
  - Deploying a Cisco MGC Host 6-17
  - Deploying a Cisco SLT 6-17
  - Deploying a LAN Switch 6-18
  - Deploying a Cisco MGX 8260 6-18
  - Deploying a Billing and Measurements Server (BAMS) 6-18

CHAPTER 7

**Using Polling to Monitor Network Performance 7-1**

- Introduction to Performance Monitoring 7-1
- How Performance Data Is Collected 7-3
  - Performance Data Collected for the Active Cisco MGC Host 7-3
  - Common Performance Data Collected for the Cisco SLT and LAN Switch 7-4
  - Performance Data Collected for the Cisco SLT Network Interfaces 7-5
  - Performance Data Collected for the LAN Switch Network Interfaces 7-6
- Opening the Performance Manager 7-6
- Setting Polling Frequencies 7-8
  - Changing Polling Frequency 7-9
- Starting Polling On a Device 7-11

Understanding the Different Polling States of a Device	7-12
Decommissioning and Rediscovering Devices	7-16
Viewing Performance Data	7-16
Viewing Raw Data	7-20
Viewing a Chart	7-20
Viewing a Performance Log	7-21
Setting How Performance Data Is Archived	7-21
Printing a Performance File	7-22

## CHAPTER 8

**Managing Traps and Events 8-1**

Introduction to Fault Management	8-1
How CEMF Models Events	8-3
Event Information	8-3
Event Propagation	8-4
How CMNM Manages Faults	8-5
Presence Polling	8-6
How Traps Are Managed for Network Devices	8-6
Cisco SLT Traps	8-6
LAN Switch 5500 Traps	8-7
Catalyst 2900XL Traps	8-7
Catalyst 2900 Traps	8-8
Cisco MGC Host Traps	8-8
Cisco MGX 8260 Traps	8-8
Forwarding Traps to Other Systems	8-11
Opening the Event Browser	8-13
Overview of the Event Browser Screen	8-13
Filtering Events Using Queries	8-15
Opening the Query Editor	8-15
Setting Filtering Criteria	8-16
Modifying Filtering Criteria	8-23
Sorting Events	8-24
Setting Up Sort Options	8-24
Managing Events	8-25
Managing an Event from the Window	8-25
Managing an Event from the Menu Bar	8-26
Enabling Auto or Manual Update	8-26

- Setting How Events Are Color-Coded 8-27
  - Selecting the Type of Color Coding to Be Used 8-27
- Viewing the Event History 8-27
- Refreshing the Event Window 8-28
- Viewing a Full Description of an Event 8-28
- Managing Cisco MGX 8260 Faults 8-30
- Using the Cisco MGC Tool Bar 8-31
  - Alarm and Measurements Viewer 8-32
  - CDR Viewer 8-34
  - CONFIG-LIB Viewer 8-36
  - Log Viewer 8-37
  - Trace Viewer 8-38
  - Translation Verification 8-39
  - File Options 8-40
- Setting How Long Alarms Are Stored 8-41

CHAPTER 9

**Viewing Information About Network Devices 9-1**

- Introduction 9-1
- Viewing Accounts and Properties 9-1
  - Viewing Cisco MGC Host Accounts 9-2
  - Viewing Cisco MGC Host Properties 9-3
  - Viewing Cisco SLT Accounts 9-6
  - Viewing Cisco SLT Properties 9-7
  - Viewing LAN Switch Accounts 9-11
  - Viewing LAN Switch Properties 9-12
  - Viewing BAMS Accounts 9-16
  - Viewing BAMS Properties 9-17
  - Viewing Ethernet Interface Properties 9-18
  - Viewing TDM Interface Properties 9-19
  - Viewing Serial Interface Properties 9-26
- Attributes for Fields in Accounts and Properties 9-28
  - Host Controller Attributes 9-29
  - IP Manageable Attributes 9-29
  - SNMP Attributes 9-30
  - Interface Attributes 9-30
  - TCP Attributes 9-31



UDP Attributes 9-32

Memory Pool Attributes 9-32

BAMS Chassis Attributes 9-32

Cisco MGC TDM Attributes 9-33





## Preface

---

### Document Objectives

This User's Guide provides step-by-step instructions for most of the tasks you perform using Cisco Media Gateway Controller Node Manager (CMNM). It contains information you need to install and configure CMNM and to prepare the system for users. It also contains reference information that may be needed by administrators, service technicians, and users.

CMNM provides a means to manage fault, configuration, and performance of the service provider's Cisco MGC nodes. CMNM is based on the Cisco Element Manager Framework (CEMF).

This document describes how to:

- Provide fault and performance management of the Cisco MGC node and its subcomponents
- Configure network elements using CiscoView and other tools
- Display and manage the Cisco MGC, Cisco SLT, and LAN connectivity network

### Audience

This document has two primary audiences:

- System administrators who install and configure CMNM
- Network Operations Center (NOC) personnel who use CMNM to monitor the network and respond to events and alarms

### Document Organization

This document contains the following chapters:

*Table 1 Document Contents*

Chapters	Title	Content
Chapter 1	Overview of Cisco Media Gateway Controller Node Manager	This chapter provides an overview of CMNM and the various tasks you perform.

**Table 1** Document Contents

Chapter 2	Installing CMNM	This chapter contains information about hardware and software requirements for CMNM and instructions for installing the software.
Chapter 3	Configuring Network Devices for Management	This chapter shows you how to configure each network device so that it can be managed by CMNM.
Chapter 4	Getting Started with CMNM	This chapter describes CMNM concepts.
Chapter 5	Setting Up CMNM Security	The administrator must set up security for the system and users. CMNM provides a number of security features necessary for a typical service provider's environment, such as user login IDs and alphanumeric passwords and per-user privileges and control of administrative functions. This chapter shows you how to set up defaults for users and security for the system.
Chapter 6	Deploying a Site, Object, or Network	CMNM provides two methods to configure Cisco MGC nodes and subobjects: manual and seed file. This chapter shows you how to deploy using either method.
Chapter 7	Using Polling to Monitor Network Performance	CMNM collects performance information from the Cisco MGC node, allowing you to monitor the health and performance of the network. CMNM allows you to view performance data associated with a given object and graph that data over time. This chapter shows you how to monitor performance data.
Chapter 8	Managing Traps and Events	CMNM provides fault management of the Cisco MGC, including the Cisco MGC host, Cisco SLT, and LAN switch. This chapter shows you how to view, acknowledge, and clear alarms for a given object.
Chapter 9	Viewing Information About Network Devices	This chapter shows you how to view a variety of different information about network devices.

## Documentation Suite

Consult the following related documentation for additional information about the Cisco MGC software.

### Cisco MGC Documentation

- *Cisco Media Gateway Controller Hardware Installation Guide*

- *Regulatory Compliance and Safety Information for Cisco Media Gateway Controller Hardware*
- *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*
- *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*
- *Cisco Media Gateway Controller Software Release 7 Reference Guide*
- *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide*
- *Release Notes for Cisco Media Gateway Controller Software Release 7*
- *Cisco Media Gateway Controller Online Documentation Notice*
- *Cisco Media Gateway Controller SLT Documentation Notice*
- *Cisco Media Gateway Installation and Configuration Guide*

## Cisco Element Management Framework Documentation

Consult the following related documentation for additional information about the Cisco Element Management Framework (CEMF):

- *Cisco Element Management Framework Installation and Licensing Guide*
- *Cisco Element Management Framework Release Notes*
- *Cisco Element Management Framework User Guide*

## Billing and Measurements Server Documentation

Consult the following related documentation for additional information about the Billing and Measurements Server (BAMS):

- *Billing and Measurements Server (BAMS) User's Manual*

## Document Conventions

Command descriptions use the following conventions:

<b>boldface font</b>	Commands and keywords are in <b>boldface</b> .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[ ]	Elements in square brackets are optional.
{ x   y   z }	Alternative keywords are grouped in braces and separated by vertical bars.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use the following conventions:

screen font	Terminal sessions and information the system displays are in <i>screen font</i> .
<b>boldface screen font</b>	Information you must enter is in <b>boldface screen font</b> .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
→	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control. For example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



#### Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.



#### 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*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.



#### Caution

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

## Obtaining Documentation

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <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. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

## Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

## Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online 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.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, 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 CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: [www.cisco.com](http://www.cisco.com)
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to [cco-team@cisco.com](mailto:cco-team@cisco.com).

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use [www.cisco.com/techsupport](http://www.cisco.com/techsupport).

To contact by e-mail, use one of the following:

Language	E-mail Address
English	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Hanzi (Chinese)	<a href="mailto:chinese-tac@cisco.com">chinese-tac@cisco.com</a>
Kanji (Japanese)	<a href="mailto:japan-tac@cisco.com">japan-tac@cisco.com</a>
Hangul (Korean)	<a href="mailto:korea-tac@cisco.com">korea-tac@cisco.com</a>
Spanish	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Thai	<a href="mailto:thai-tac@cisco.com">thai-tac@cisco.com</a>

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site:  
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

## 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](mailto: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 and value your comments.





# Overview of Cisco Media Gateway Controller Node Manager

---

## Introduction

Cisco Media Gateway Controller Node Manager (CMNM) integrates the management interfaces and management functionality of the Cisco MGC node components into one comprehensive human interface and data repository. The Cisco MGC node consists of the Cisco MGC itself, one or more Cisco Signaling Link Terminals (Cisco SLTs) and the Catalyst 2900, Catalyst 5000, or Catalyst 5500 LAN switch. CMNM provides fault, configuration, and performance management for all components of the Cisco MGC node.

CMNM provides the element-specific management features for the Cisco MGC node. It blends the management framework features of the Cisco Element Management Framework (CEMF) with the individual interfaces and object structures of each managed element to produce an integrated management application.

## Terms Used in This Document

The following terms are used in this document:

- **BAMS**—Billing and Measurements Server. The Billing and Measurements Server (BAMS) is a UNIX-based software application that accepts individual usage records generated by Cisco's Virtual Switch Controllers (VSCs), validates and correlates the records into a merged usage record, facilitates traffic-oriented statistical analysis, and generates Bellcore Automatic Message Accounting (AMA) Format (BAF) records on a per-call basis.
- **Cisco Element Management Framework (CEMF)**—The element management framework upon which CMNM is built.
- **Cisco MGC**—Cisco Media Gateway Controller. The Cisco Virtual Switch Controller (Cisco VSC) and the Cisco Signaling Controller (Cisco SC) are key to Cisco's voice domain solutions. The Cisco VSC and the Cisco SC are collectively called a Cisco Media Gateway Controller (Cisco MGC) node. The Cisco MGC node itself is comprised of a number of different devices: the Cisco MGC host, a LAN switch, and a Cisco Signaling Link Terminal (Cisco SLT).
- **Cisco MGC host**—A Sun host server running Cisco MGC software. For the Cisco SC2200 and the Cisco VSC3000, this is also called a Cisco MGC host.
- **Cisco MGC node**—A generic term encompassing both the Cisco SC node and the Cisco VSC node. The logical grouping of the active and standby Cisco MGC hosts, the control signaling network, and the Cisco SLTs.

- CiscoView—A graphical device management tool based on Simple Network Management Protocol (SNMP) that provides real-time views of networked Cisco Systems devices.
- CMM and VSPT—Cisco MGC Manager and Voice Services Provisioning Tool  
You can use two different Cisco VSC3000 and Cisco SC2200 provisioning tools, depending on the network architecture you are running. If you are running the Cisco SS7 PRI Gateway Solution or the Cisco Tandem Offload Solution, you use VSPT. For all other architectures, you use CMM.
- Web Viewer—A web-based device management tool that facilitates managing the Cisco MGX 8260 media gateway.

## Overview of the Cisco MGC Node Architecture

The Cisco Virtual Switch Controller (VSC) and the Cisco Signaling Controller (SC) (collectively referred to as the Cisco MGC) are key to Cisco's voice domain solutions.

The Cisco MGC node itself comprises the:

- Cisco MGC host—The Cisco MGC host is a suite of software running on a Sun Solaris server and is responsible for most of the Cisco MGC functionality, including (depending on the configuration) number analysis, routing, switching, and so on.
- Cisco Signaling Link Terminal (Cisco SLT)—The Cisco SLT is responsible for terminating SS7 signaling lines from the PSTN.
- LAN switch—The LAN switch acts as an Ethernet switch connecting the Cisco SLT and the Cisco MGC host to external equipment.  
The standard Cisco MGC node design defines that a Cisco 2611 should be configured as the Cisco SLT and that a Catalyst 2900XL, 5500, or 5000 should be used as the LAN switch.
- BAMS—BAMS is used for optional third-party accounting and billing packages.

A Cisco MGC node is (optionally) fully redundant. This means that each Cisco Virtual Switch Controller or Cisco Signaling Controller may actually have multiples of each type of subcomponent. At any given time, one Cisco MGC host is considered active and the other standby. When the active Cisco MGC host goes down, the standby host becomes active. There is no concept of active or standby with the LAN switches or Cisco SLTs (both are active at all times).

## Key Features of CMNM

The most common form of a CEMF installation includes plug-in modules referred to as Element Managers or Element Management Systems (EMS). In the Cisco MGC node architecture, CMNM is a CEMF-based EMS that is responsible for managing the Cisco MGC node. CMNM adds custom graphical user interface (GUI) windows and modeling behavior to the standard CEMF system to allow the management of specific types of network elements. For more information about the Element Managers installed with CMNM, see Table 2-11 in the “Verifying Element Managers” section on page 2-11.

CMNM uses CEMF to manage the following components of the Cisco MGC node:

- Cisco MGC
- Cisco SLT
- LAN Switch (Catalyst 2900, 5000, and 5500 only)
- BAMS

The key features of CMNM are:

- Performance monitoring

CMNM collects and displays performance information from the Cisco MGC node, allowing you to monitor the health and performance of the network. CMNM collects performance information from all the components of the Cisco MGC node.

You can:

- Graph and display the performance information
- View performance data associated with a given object and graph that data over time
- Configure the objects being polled and the frequency of the polling
- Export the performance data for use by other applications

For more information on performance monitoring, see Chapter 7, “Using Polling to Monitor Network Performance.”

- Fault management

CMNM provides fault management of the Cisco MGC node, including the Cisco MGC host, the Cisco MGX 8260, the Cisco SLT, and the LAN switch. You see the traps generated by these elements in the CMNM system.

When the Cisco MGC host detects a problem with one of its logical connections, it generates a trap. CMNM receives these traps and delegates them to the object that represents that logical connection. For example, if CMNM receives a trap that the link to a media gateway is down, CMNM delegates that trap to the object that represents the media gateway link. You can acknowledge and clear alarms and forward traps.

CMNM periodically polls each managed object to ensure that the device is still reachable using SNMP. If the device is not reachable, an annotation appears on the map display, an alarm is generated, and the object is placed in an errored state. After the object loses connectivity, CMNM continues to poll the object until it can be reached. Once connectivity is reestablished, the alarm is cleared, the annotation on the map viewer is removed, and the object is returned to the normal state.

For more information on fault management, see Chapter 8, “Managing Traps and Events.”

- Security

CMNM supports role-based access to its management functions. The administrator defines user groups and assigns users to these groups. CMNM supports control of administrative state variables for Cisco MGC node resources. For more information on access control, see Chapter 5, “Setting Up CMNM Security.”

- Billing and Measurements

Third-party accounting and billing packages are supported directly on the Billing and Measurements Server (BAMS), a component of the Cisco MGC node.

- Configuration

You can launch the following configuration tools from CMNM:

- Cisco MGC Manager (CMM), a generic Cisco MGC host configuration tool used in all network architectures except those using the Voice Services Provisioning Tool.
- CiscoView, which allows you to configure the Cisco SLT (Cisco 2611) and the LAN switch (Catalyst 2900, 5000, and 5500) devices.
- Voice Services Provisioning Tool, a Cisco MGC host configuration tool used in the Cisco SS7 PRI Gateway Solution and the Cisco Tandem Offload Solution. For all other architectures, use CMM.

- Web Viewer, the tool used to view and configure the Cisco MGX 8260.
- Troubleshooting
  - CMNM provides CDR Viewer, Log Viewer, Trace Viewer, and Translation Verification Viewer for diagnostic and troubleshooting information.

## Overview of CEMF

CMNM is based on the Cisco Element Management Framework (CEMF), a carrier-class network management framework. This framework was designed to address the challenges of developing and deploying robust, large-scale, multivendor, multitechnology management solutions.

CEMF has been designed to overcome the limitations of traditional enterprise network management solutions, particularly in the broadband access market, and also in other network management applications where the aforementioned characteristics are important. CEMF is used to quickly develop and deploy element, network, and service-level applications in technologies ranging from Digital Subscriber Line (DSL), used for high-speed Internet access; cable modems; and Voice over IP to complex ATM/IP routing multiservice switches.

## CEMF Components

CEMF consists of:

- A series of applications that form a front-end GUI to process input
- A series of back-end server processes that maintain a model of the network and carry out the actual interfacing to the network elements (see Figure 1-1)

*Figure 1-1 CEMF Processes*



CEMF comes with the following set of applications:

- Launchpad
- Map Viewer
- Auto Discovery
- Access Manager
- Event Browser
- Object Group Manager
- Performance Manager
- Deployment Wizard
- Event Manager
- Netscape Help Browser

## How CEMF Models the Network

CEMF keeps a model of the managed network within its database. This model is used to keep track of the current state of the various network elements and various abstractions of this network.

The CEMF model of the network uses the following components:

- Objects—Each element managed by CEMF is modeled as an object.

An object can represent:

- Some part of the network, such as a router or a switch

- An abstraction of the network, such as a site or a region
- Some of the services provided by the network, such as a permanent virtual connection (PVC)
- Something (or someone) that interacts with the network, such as a subscriber or a customer
- Object classes—Each object within CEMF has an associated object class. Each class of object simply indicates a different kind of element. Examples of classes are routers, line cards, sites, and so on. Each class of object has different data stored against it and displays different behavior.

In the Map Viewer application, the class of the object is indicated with a different icon used within the Map View browser.

The use of classes also allows powerful queries to be carried out based upon the kind of object. Examples of this type of query could be: show all events in the system from cable modems or create a group of router objects.

- Object types and attributes—Each object has a number of attributes that can be accessed. An attribute is a piece of information either stored against the object or accessible from the object through some network protocol. Examples of attributes are IP address, interface table, upstream power, and so on.

These attributes are associated with the object according to the granularity of object types. A type is simply a collection of related attributes and each class usually has a number of types. An object's class defines which types and, therefore, which attributes it is allowed to have and which types it has by default.

An example of the association between classes and types is shown in Figure 1-2.

**Figure 1-2 Example of Object Types and Attributes**



In Figure 1-2, a UnixWorkstation class is specified. This class of object includes two types: System and snmpManageable. The System type includes the sysDesc, sysUpTime, and sysObjectId attributes. The snmpManageable type includes the read-community and write-community attributes.

- Views—A view is a collection of objects in a hierarchical relationship. Each object can have a number of parents and children.

You can access CEMF objects by navigating through one of the views to find the object. Each view represents a different way of containing and grouping the objects. The standard views provided are the Physical view and the Network view. CMNM adds additional views onto the standard set supplied by CEMF.

- Network view—Used to represent the network devices within their relevant networks and subnets. This view is used by the Auto Discovery subsystem of CEMF to calculate which devices have already been added to the system so that it does not try to discover the same device multiple times.
- Physical view—Used to show the actual physical location of an element. An example of a physical containment relationship is shown in Figure 1-3.

**Figure 1-3 Example of a Physical View**



- *xxx*Containment view—Where *xxx* represents an object class. For example, the *sltContainment* view represents the Cisco SLTs. These containment views are useful for looking at information about a set of similar devices.
- Object groups—An object group is simply a collection of objects which are related in some way. They may all be the same type of equipment or all belong to the same customer.  
Object groups can be built either manually or by building a query. Object groups are accessible through the Object Group Manager application.

## How CMNM Models the Cisco MGC Node

This section provides information about how CMNM models:

- Network interfaces
- Cisco MGC host connectivity network

### Network Interfaces

In CMNM, the network interfaces for the Cisco MGC host, BAMS, Cisco SLT, LAN switch, and Cisco MGX 8260 are modeled. These include all Ethernet interfaces and, on the Cisco SLT, all time-division multiplexing (TDM) and serial interfaces.

Figure 1-4 shows a graphical view of the model.

*Figure 1-4 Cisco MGC Node Model*

## Cisco MGC Host Connectivity Network

CMNM displays the status of the Cisco MGC host connectivity network on the Map Viewer interface. This includes showing the status of the logical connections from the active Cisco MGC host to the:

- Interfaces (Ethernet, TDM)
- Signal transfer points (STPs)
- Destination point code (SS7 Routes)
- Connected Cisco MGCs
- TCAP nodes
- Media gateways
- Cisco SLT and LAN switches

When the common Cisco MGC host object is first deployed, the CEMF object database is populated with nodes that represent the logical connections from the active Cisco MGC host to the external devices. CMNM then monitors the status of these connections and, when necessary, informs you of any loss of connectivity.



As new connections are deployed, the connectivity network is updated to reflect the current configuration and network status of the active Cisco MGC host.

CMNM monitors the status of the connectivity network by processing and decoding traps from the active Cisco MGC host. Upon receipt of an appropriate trap, CMNM maps the trap to the node representing the logical connection. An alarm associated with the node is displayed.

The logical connections from the active Cisco MGC host are shown as subnodes under the common Cisco MGC host object. If the standby Cisco MGC host is not processing calls, only the network connectivity of the active host is shown.

CMNM communicates to the Cisco MGC host using:

- Simple Network Management Protocol (SNMP)—SNMP is used for receiving alarm information.
- File Transfer Protocol (FTP)—FTP is used for bulk file transfer of performance statistics.
- Man-Machine Language (MML)—MML (the TL1-based interface on the Cisco MGC host) is used to retrieve the Cisco MGC host configuration information needed to manage the node.

## Cisco MGC Host Connectivity Objects

The Cisco MGC host software defines over 20 different types of network connectivity component types. CMNM queries the configuration of the active Cisco MGC host and represents them in the display.

The hierarchical structure or relationship of the components is based on the configuration defined by the active Cisco MGC host. This configuration can vary from installation to installation. CMNM, however, is able to handle any type of configuration that may be present on the host.

CMNM defines a class representing each network connectivity element type. For example, there is a class for an IP link, point code, and external node. The attributes associated with each class exactly match the attributes of the MML command used to provision the object.

The classes used to represent the connectivity network in CMNM are described in Table 1-1.

**Table 1-1** *Classes Representing Connectivity Network*

MML Type	Name	Description
apc	Adjacent point code	Defines an SS7 STP or external switch through which the Cisco MGC connects to external switches and other Service Switching Points (SSPs).
c7iplnk	C7 IP link	Identifies a link between a Cisco SLT's IP address and port and the SS7 network.
card	Card	Network card or adapter that is operating in the Cisco MGC.
eisuppath	EISUP path	Signaling service or signaling path to an externally located Cisco MGC.
enetif	Ethernet interface	Physical line interface between a Cisco MGC Ethernet network card/adapter and the physical Ethernet network.
extnode	External node	Cisco MGW with which the Cisco MGC communicates.
faspath	FAS path	Service or signaling path to a particular destination using either ISDN-PRI or DPNSS.
ipfaspath	IP FAS path	Transport service or signaling path from a gateway to a Cisco MGC.

**Table 1-1** *Classes Representing Connectivity Network*

iplnk	IP link	IP connection between a Cisco MGC's Ethernet interface and a Cisco MGW.
lnkset	Linkset	Group of all communication links that connect from the Cisco MGC to an adjacent STP.
mgcppath	MGCP path	Signaling service or signaling path to a trunking gateway.
naspath	NAS path	Q.931 protocol path between the Cisco MGC and the Cisco MGW.
ptcode	Point code	An SS7 network address that identifies an SS7 network node.
sgcpath	SGCP path	Protocol path between the Cisco MGC and the Cisco MGW.
ss7path	SS7 path	Specifies the protocol variant and the path that the Cisco MGC uses to communicate with a remote switch (SSP) sending bearer traffic to the Cisco MGWs.
ss7route	SS7 route	Path, by way of a linkset, from the Cisco MGC to another Cisco MGC or TDM switch.
ss7subsys	SS7 subsystem	Logical entity that mates two Signal Transfer Points (STPs).
tcapipath	TCAP IP path	Signaling service path to an STP or SCP.
tdmif	TDM interface	Physical line interface between a Cisco MGC TDM network card/adaptor and the physical TDM network.
tdmlnk	TDM link	Communications link between a TDM interface card on the Cisco MGC and TDM hardware element.

## Containment Hierarchy of the Connectivity Network

When CMNM retrieves the current configuration from the active Cisco MGC host, it establishes the containment hierarchy of the connectivity network. A hierarchical model example is shown in Figure 1-5.

*Figure 1-5 Hierarchical Model Example*



In the MML file, the destination point code (DPC) component represents a TDM switch. Likewise, the adjacent point code (APC) component represents an STP.

The external node component in the MML file represents one of a number of different elements. These include:

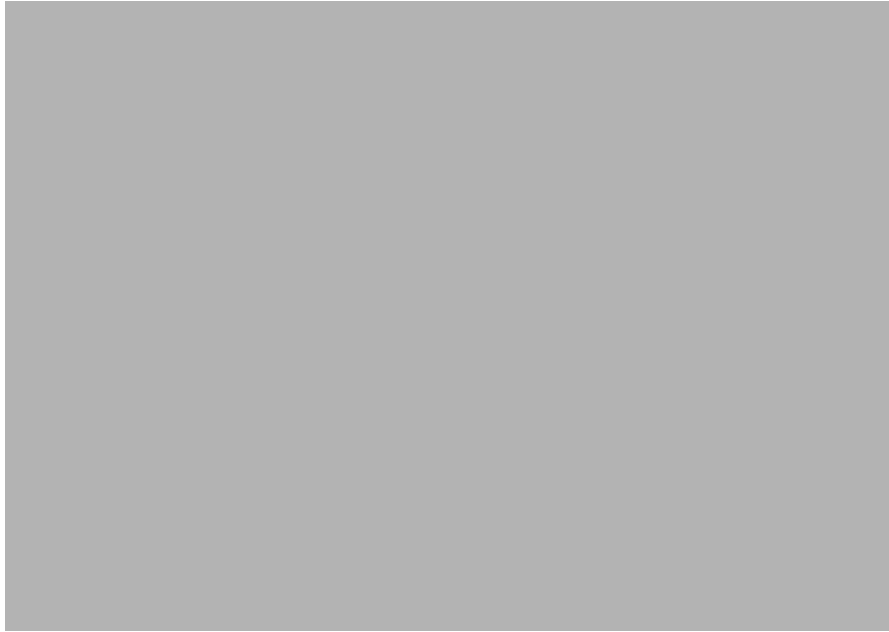
- Media gateways
- Connected Cisco Media Gateway Controllers
- SS7 Service Control Points

## Viewing the Network Connectivity Map

To view the Network Connectivity Map:

- 
- Step 1** From the CEMF Launchpad, click **Viewer**.
- Step 2** In the Physical view, navigate to the Cisco MGC host, expand its tree, then click the **Connectivity** icon. You see a map of the network and object connections as shown in Figure 1-6.

*Figure 1-6 Map Viewer Screen—Connectivity*





## Installing CMNM

---

### Introduction to CMNM Installation

The CMNM installation program and installation software are found on a CMNM product CD. Cisco Media Gateway Controller Manager (CMM) or Voice Services Provisioning Tool (VSPT) are required for voice provisioning, depending on the network configuration. Both must be installed before CMNM. CMM is found on the CMNM CD and Voice Services Provisioning Tool is downloaded from the Web.

### Before You Start

Before you install CMNM you must have the required hardware and software and access to the CMNM Installation site on the Web.

### Task Checklist

Perform the following steps before beginning installation of the CMNM:

- 
- Step 1 Check the web site for latest bulletins and updates.
  - Step 2 Check the minimum hardware requirements.
  - Step 3 Check the software requirement list to be sure that you have all the necessary software.
  - Step 4 Partition hard drives on the workstation.
  - Step 5 Install CEMF 3.0.4 and latest patches (minimum Patch 7 is required).
  - Step 6 Make CEMF performance modifications.
  - Step 7 Install CMNM on client and manager workstations as appropriate.
  - Step 8 Install the relevant Cisco MGC host provisioning tool.
- 

### Hardware Requirements

Both client and server minimum hardware requirements must be met.



**Note** CMNM supports a maximum of six users at a time.

The CMNM application runs on a separate machine than the Cisco MGC host. The requirements of this machine are described in Table 2-1.

**Table 2-1 Hardware Requirements for CMNM Host Machine**

Resources	CEMF Server Large Network > 10 VSC/SC's	CEMF Server Medium Network 5-10 VSC/SC's	CEMF Server Small Network <5 VSC/SC's	CEMF Client
Hardware	Sun E450	Sun E450	Sun Ultra 60	Sun Ultra 5
OS	Sun Solaris 2.6 *	Sun Solaris 2.6 *	Sun Solaris 2.6 *	Sun Solaris 2.6 *
Memory	4 GB	2 GB	1 GB	512 MB
Disk Drives	Six 9-GB drives (raw file system)	Four 9-GB drives (raw file system)	Four 9-GB drives (raw file system)	One 9-GB drive
Processor	Four x 400 or faster	Two x 400 or faster	Two x 360 or faster	One x 333 or faster
Swap Space	2.0 GB	2.0 GB	2.0 GB	1.0 GB
Monitor	17-inch color	17-inch color	17-inch color	17-inch color
Graphics Card	24-bit	24-bit	24-bit	24-bit
Miscellaneous	CD-ROM drive	CD-ROM drive	CD-ROM drive	CD-ROM drive

\* Solaris 2.6 (05/98 release) with latest 2.6 Recommended patches from Sun



**Note** Disk drive requirements are based on the number of drives. The CEMF host machine requires at least the number of drives indicated in Table 2-1.



**Note** Using multiple disk drives to store the CEMF databases helps alleviate I/O bottlenecks and substantially aids in the performance of the software. If cooked file partitions are used, installing more than four drives does not yield any performance improvements, because the CEMF databases cannot span multiple partitions.



**Note** These are *recommendations*. The total amount of disk space required depends on the amount of alarm and performance data saved.

## Hard Drive Partitioning

By default, the CEMF software is installed with standard UNIX cooked partitions (partitions with readable directory structures.) However, raw partitions (partitions without a readable directory structure) offer the following advantages over cooked partitions:

- A large performance gain

- The capability of having databases over 2 gigabytes in size

Listed below are the *suggested* partitioning layouts for both cooked and raw partitions. For detailed information on configuring CEMF with raw file systems, refer to the “ObjectStore Installation Options” section in the *Installing, Licensing, and Configuring Cisco EMF* manual. CEMF uses ObjectStore for its database. ObjectStore is installed with CEMF.

## Suggested Layout for Cooked Partitions (CEMF Default)



**Note** ObjectStore requires all raw partitions to be identical in size.



**Note** For information about suggested performance enhancements for cooked partitions, see the “Performance Enhancements for Cooked Partitions” section on page 2-7.

The following tables give the mount point and size for creating cooked partitions.

**Table 2-2 Drive 1 —Operating System Drive—9 GB or Larger**

Mount Point	Size
/ (root)	512 MB
<swap>	2.0 GB
/var	1.0 GB
/usr	4.0 GB
/home	Remainder

**Table 2-3 Drive 2**

Mount Point	Size
<swap>	2.0 GB
/opt	Remainder

**Table 2-4 Drive 3**

Mount Point	Size
/opt/CSCOcemf/db	Remainder

**Table 2-5 Drive 4**

Mount Point	Size
/ostore/transaction	1.0 GB
/ostore/cache	Remainder

## Suggested Layout for Raw Partitions

The following tables give the mount point and size for creating raw partitions.



Note

ObjectStore requires all raw partitions to be identical in size.



Note

For information about suggested performance enhancements for raw partitions, see the “Performance Enhancements for Raw Partitions” section on page 2-8.

**Table 2-6 Drive 1 —Operating System Drive—9 GB or Larger**

Mount Point	Size
/ (root)	512 MB
<swap>	2.0 GB
/var	1.0 GB
/usr	4.0 GB
/home	Remainder

**Table 2-7 Drive 2**

Mount Point	Size
<swap>	2.0 GB
/opt	Remainder

**Table 2-8 Drives 3, 4, 5, and 6 (If Appropriate)**

Mount Point	Size
<Raw file system>	Remainder

## Configuring Raw File Systems in ObjectStore

Note the following:

- You must partition the hard drives when installing the Sun Solaris operating system.
- To get the installation directory for the CEMF software, use the command **/bin/pkgparam CSCOcemfm BASEDIR**.
- All raw partitions must be exactly the same size (in megabytes). ObjectStore does not use partitions of different sizes.
- The raw partition names (for example, /dev/rdisk/c0t1d0s3) must be available before starting the configuration session.
- Determine the name of the machine (for example, cemfserver).



**Caution**

Adding, modifying, or deleting raw file systems resets the ObjectStore database and destroys any existing data.

To configure raw file systems in ObjectStore:

- 
- Step 1** Type **su - root** to become the root user.
- Step 2** Stop the current CEMF processes (**/etc/init.d/cemf stop**).
- Step 3** Shut down ObjectStore (for example, **/etc/rc2.d/S80ostore4 stop**).
- Step 4** Shut down the AV License Manager (for example, **/etc/rc2.d/S98avlm stop**).
- Step 5** Start a CEMF shell (for example, **/etc/rc2.d/S99cemf shell**).
- Step 6** Change to the CEMF installation directory (for example, **/opt/CSCOcemf**).
- Step 7** Change to the **./ODI/OS5.1/ostore/etc** directory (under **/opt/\$INSTALL\_DIR**).
- Step 8** Edit the host name server parameter file (for example, **cemfserver\_server\_parameters**) and make the following modifications:
- Put a comment character (**#**) at the beginning of the Log File line. (This places the transaction log in the raw partition.)
  - Add an entry for each raw partition that ObjectStore uses.
  - Each line must begin with **PartitionX:** (where **X** is a number starting with zero and incrementing by one). Do not forget the colon character.
  - Each line must have the word **PARTITION** as the second element.
  - Each line must have the raw partition listed as the last element. (Do not forget to use the **rdsd** partition identifier.)

For example (a **cemfserver\_server\_parameters** file):

```
unix-shell#> cd /opt/CSCOcemf/ODI/OS5.1/ostore/etc
unix-shell#> cat cemfserver_server_parameters
```

```
#Log File: /opt/transact.log
Partition0: PARTITION /dev/rdsd/c2t9d0s0
Partition1: PARTITION /dev/rdsd/c2t10d0s0
Partition2: PARTITION /dev/rdsd/c2t12d0s0
Partition3: PARTITION /dev/rdsd/c2t13d0s0
```

```
unix-shell#>
```

- Step 9** Change to the **CEMF\_INSTALL/ODI/OS5.1/ostore/lib** directory (for example, **opt/CSCOcemf/ODI/OS5.1/ostore/lib**).
- Step 10** Run the command **./osserver -i** to reinitialize ObjectStore. Answer **yes** when prompted to reinitialize the database.
- Step 11** Run the command **/etc/init.d/cemf reset** to reset the CEMF database. Answer **yes** when prompted.

**Step 12** Run the command `/etc/init.d/cemf start` to start the ObjectStore and CEMF processes.

## Suggested Layout for the CEMF Client

*Table 2-9 Single Drive for Client*

Mount Point	Size
/ (root)	512 MB
<swap>	2.0 GB
/var	1.0 GB
/usr	2.0 GB
/opt	Remainder

## Software Requirements

Both client and server minimum software requirements must be met.



**Caution**

Check the web site for the latest bulletins and upgrades for software before proceeding.

CMNM interacts with other software running on the various components of the Cisco MGC node. The software requirements for these components are described in Table 2-10.

*Table 2-10 External Software Versions*

External Software	Version
CEMF	3.0.4 Patch 7 or later
Cisco MGC host software	Latest version of 7.4
Cisco SLT IOS SS7 image	12.0.7 XR
LAN switch code	4.5(1)
Voice Services Provisioning Tool	1.1
BAMS	1.0.8

## Recommended Performance Enhancements for CEMF

The following enhancements are designed to get the maximum performance from a CEMF installation. For cooked and raw partitions, select Option 1 or Option 2 based on the system's physical memory size.

## Performance Enhancements for Cooked Partitions



**Note** Databases should be not be installed on the same drive as the CEMF software.



**Note** For more information about cooked partitions, see the “Hard Drive Partitioning” section on page 2-2.

### Option 1

If physical memory is less than 1 gigabyte, then the cache files should reside on a separate physical drive.

- 
- Step 1** On a separate drive, add a partition and mount that partition to `/ostart_cache`.
- Step 2** Create the file `localhost.sh` in the *CEMF Directory*/config/env directory and add the lines:
- ```
OS-CACHE_DIR=/ostore_cache ; export OS_CACHE_DIR
OS_COMMSEG_DIR=/ostore_cache ; export OS_COMMSEG_DIR
```
- Step 3** For the changes to take effect, you must restart the CEMF processes using the following commands.
- ```
/etc/init.d/cemf stop
/etc/init.d/cemf start
```
- 

### Option 2

If physical memory is greater than 1 gigabyte, then the cache files should reside in a memory file system (for example, tmpfs).

- 
- Step 1** Verify that `/etc/vfstab` has an entry for tmpfs mounted to `/tmp`. If not, perform the following steps:
- Type **su - root** to become the root user.
  - Change to the `/etc` directory.
  - Copy the `vfstab` file to a backup file.
  - Edit the `vfstab` file and add the following line:
 

```
swap - /tmp tmpfs - yes -
```
  - Reboot for changes to take effect.
- Step 2** Create the file `localhost.sh` in the *CEMF Directory*/config/env directory and add these lines:
- ```
OS-CACHE_DIR=/tmp/ostore
OS_COMMSEG_DIR=/tmp/ostore
```
- Step 3** Verify that the entry for the database transaction log is correctly identified in the file `hostname_server_parameter`, where `hostname` is the host name of the workstation. Enter the command:
- ```
cat CEMF Directory/ODI/OS5.1/ostore/etc/hostname_server_parameter
```
- You should see the line:

Log File: `/var/opt/cemf/logs/transact.log`

- Step 4** If the `transact.log` file is not correctly identified, edit the `hostname_server_parameter` file.
- Step 5** For the changes to take effect, you must restart the CEMF processes using the following commands.

```
/etc/init.d/cemf stop
/etc/init.d/cemf start
```

---

## Performance Enhancements for Raw Partitions



**Note** Raw partitions should be not be installed on the same drive as the CEMF software.

---



**Note** For more information about raw partitions, see the “Hard Drive Partitioning” section on page 2-2.

---

### Option 1

If physical memory is less than 1 gigabyte, then the cache files should reside on a separate physical drive and the database transaction log should be in the raw partition.

---

- Step 1** On a separate drive, add a partition and mount that partition to `/ostart_cache`.
- Step 2** Create the file `localhost.sh` in the `CEMF Directory/config/env` directory and add the lines:
- ```
OS-CACHE_DIR=/ostore_cache ; export OS_CACHE_DIR
OS_COMMSEG_DIR=/ostore_cache ; export OS_COMMSEG_DIR
```
- Step 3** The transaction log should be in the raw partition. The file `hostname_server_parameter`, where `hostname` is the host name of the workstation, should not have an entry for the transaction log. If the `hostname_server_parameter` file has an entry for the transaction log, edit the file and remove the line (the file is located in `CEMF Directory/ODI/OS5.1/ostore/etc/`).
- Step 4** For the changes to take effect, you must restart the CEMF processes using the following commands.
- ```
/etc/init.d/cemf stop
/etc/init.d/cemf start
```
- 

### Option 2

If physical memory is greater than 1 gigabyte, then the cache files should reside in a memory file system (for example, `tmpfs`) and the database transaction log should be in the raw partition.

---

- Step 1** Verify that `/etc/vfstab` has an entry for `tmpfs` mounted to `/tmp`. If not, perform the following steps:
- a. Type `su - root` to become the root user.

- b. Change to the `/etc` directory.
  - c. Copy the `vfstab` file to a backup file.
  - d. Edit the `vfstab` file and add the following line:
 

```
swap - /tmp tmpfs - yes -
```
  - e. Reboot for changes to take effect.
- Step 2** Create the file `localhost.sh` in the `CEMF Directory/config/env` directory and add these lines:
- ```
OS-CACHE_DIR=/tmp/ostore
OS_COMMSEG_DIR=/tmp/ostore
```
- Step 3** The transaction log should be in the raw partition. The file `hostname_server_parameter`, where `hostname` is the host name of the workstation, should not have an entry for the transaction log. If the `hostname_server_parameter` file has an entry for the transaction log, edit the file and remove the line (the file is located in `CEMF Directory/ODI/OS5.1/ostore/etc/`).
- Step 4** For the changes to take effect, you must restart the CEMF processes using the following commands.
- ```
/etc/init.d/cemf stop
/etc/init.d/cemf start
```
- 

## DNS Requirements

The following sections list requirements for configuring domain name system (DNS).

### Workstation Uses DNS

If the workstation uses DNS, you must configure DNS on the workstation before installing CEMF.



**Note**

If you change how DNS is configured after CEMF is installed, you must uninstall and reinstall CEMF.

If the CEMF workstation is set up to use DNS, then the host name of the workstation must also be configured on the DNS server. Just having the local hostname in the `/etc/hosts` file is not sufficient—regardless of how `/etc/nsswitch.conf` is configured.

To verify that DNS is configured and that the CEMF workstation is in DNS, perform the following steps:

- Step 1** Verify that a valid DNS server and domain name are defined in `/etc/resolv.conf`.
- Step 2** Verify that the workstation is configured in DNS using the following command:
 

```
nslookup hostname
```

**Note**

If the **nslookup** command fails, then CEMF cannot be installed until the CEMF workstation's host name is added to the DNS server.

## Workstation Does Not Use DNS

CEMF installs properly if a workstation does not use DNS. To verify this:

- Step 1** Verify that the file `/etc/resolv.conf` does not exist.
- Step 2** Verify that the hosts entry in the file `/etc/nsswitch.conf` looks exactly like the following line:

```
hosts:      files
```

**Note**

If `/etc/resolv.conf` exists, or the `hosts:` line in `/etc/nsswitch.conf` has anything else configured, then CEMF does not install properly.

## Installing the Cisco Element Manager Framework

If CEMF is not already installed, refer to the *Cisco Element Manager Framework Installation and Licensing Guide*.

## Installing CMNM

**Note**

You must install the CMNM software as root.

The CEMF, and therefore CMNM software, has both a manager (server) and client portion. The client can be installed on the same workstation as the manager or a separate workstation. CMNM must be installed on the manager and all client workstations on which CEMF is installed.

The CMNM installation process automatically detects if the CEMF manager or CEMF client is installed and then installs the correct CMNM component.

**Note**

The CMNM software is shipped with the Element Managers in Table 2-11. CMNM has not been tested with any other Element Managers. If you install additional Element Managers, they are not supported by CMNM.

- Step 1** Locate the CMNM installation media.
- Step 2** Type `su - root` to become the root user.

- Step 3** Verify that the Volume Management daemon is running:
- a. Type the command **ps -ef | grep vold**.
    - If it is running, you see the following output:
 

```
root    363  1  0   May 23 ?   0:01 /usr/sbin/vold
```
    - If the Volume Management daemon is not running, start the daemon using the following command:
 

```
/etc/init.d/volmgt start
```
  - b. Verify that the Volume Management daemon is running with the command provided above. If it is still not running, contact your system administrator.
- Step 4** Place the CMNM installation media into the CD-ROM drive.
- Step 5** Type **cd /cdrom/cdrom0**.
- Step 6** Type **./installCSCOcmnm**.
- 

## Verifying the Installation of CMNM

Verify that CMNM software is installed properly before starting CMNM.

### Verifying Element Managers

- Step 1** Verify that the CMNM Package is installed using the following command:
- ```
pkginfo CSCOcmnm
```
- The following message should appear:
- ```
application CSCOcmnm      Cisco MGC-Node Manager
```
- Step 2** Verify that the CMNM Element Managers have been installed. The CMNM software is shipped with the Element Managers in Table 2-11.

**Table 2-11 Element Managers**

bamEM	Element Manager for Billing and Measurements Server (BAMS)
hostEM	Element Manager for Cisco MGC host devices
m8260EM	Element Manager for Cisco MGX 8260 media gateway devices
mgcEM	Common Element Manager for logical Cisco MGC node devices
sltEM	Element Manager for Cisco SLT devices
switchEM	Element Manager for LAN switch (Catalyst 2900 XL, 5000, and 5500) devices

- Step 3** Run the following script to display the installed CMNM Element Managers and compare this with the list in the table above.

**CEMF Basedir/bin/cmmversion -verbose**

CSCOCmm Element Manager Versions

Name	Version	Patch Level	Build Num
bamEMm	1.0	00	060500
hostEMm	1.0	00	060500
m8260EMm	1.0	00	060500
mgcEMm	1.0	00	060500
sltEMm	1.0	00	060500
switchEMm	1.0	00	060500

## Verifying the Installation of CiscoView 5.1

**Note**

CiscoView is designed to work with CiscoWorks 2000. When installing CiscoView packages outside this environment, certain functions are not supported. The following CiscoView buttons do not work in the CMNM environment:

- Telnet
- CCO connection
- Preferences
- About
- Help

When running xdsu, the following exception is generated and can be ignored:

```
ERROR: exception occurred while examining Integration Utility
configuration: com.cisco.nm.nmim.nmic.IntgUtilCheckConfig
```

To verify the installation of CiscoView 5.1:

**Step 1** Verify that the CiscoView Application has been installed with the following command:

```
pkginfo CSCOcmcv
```

- If the package is installed, you see the following:  
application CSCOcmcv CiscoView 5.1 for Cisco MGC-Node Manager
- If the package is not installed, you see the following:  
ERROR: information for "CSCOcmcv" was not found

**Step 2** Verify that the CiscoView Packages have been installed. CiscoView is shipped with the packages in Table 2-12.

**Table 2-12 CiscoView Packages List**

CiscoView Packages	Version
Cat2900 XL	1.1



Table 2-12 CiscoView Packages List

Cat5000	1.2
Cat5500	1.2
Cat8500	2.0
Rtr2600	2.0
StackMaker	1.0
SwitchAddlets	1.3

- Step 3** Run either of the following commands to determine if the CiscoView packages listed in Table 2-12 are installed.

```
CEMF Directory/ciscoview5.1/bin/dsu -query -all
```

The dsu application displays to STDOUT the installed CiscoView packages.

```
CEMF Directory/ciscoview5.1/bin/xdsu
```

The xdsu application displays a GUI that lists the installed CiscoView packages.

## Upgrading CMNM

For information about CMNM patches and upgrades, check the web site.

## Upgrading CiscoView 5.1

- 
- Step 1** Check the CiscoView web site for the latest supported version of the package.
- Step 2** Download the latest CiscoView packages and place in a temporary directory; for example, /scratch/cvUpgrade.
- Step 3** Make sure that the package files are readable by the root user. If not, the packages do not appear in the CiscoView upgrade tool.
- Step 4** Type **su - root** to become the root user.
- Step 5** Change the directory to /scratch/cvUpgrade.
- Step 6** To run the CiscoView upgrade tool, type:
- ```
CEMF Directory/ciscoview5.1/bin/xdsu
```
- Step 7** Click **Install**. Ignore the following exception:
- ```
ERROR: exception occurred while examining Integration Utility
configuration: com.cisco.nm.nmic.IntgUtilCheckConfig
```
- Step 8** Type in the exact location of the CiscoView packages in the Directory box and press **Enter**. Or click **Browse**, navigate to your CiscoView packages' temporary directory, and click **Select**.
- Step 9** Select the CiscoView packages that you want to upgrade, click **Install**, and click the appropriate confirmation button.
-

## Uninstalling CMNM

Before uninstalling the CMNM software, be sure to back up your CEMF databases. See “Backing Up Your Databases” below.

### Backing Up Your Databases

See the “Cisco EMF Database Backup and Restore Procedures” section in the *Installing, Licensing, and Configuring Cisco EMF* manual.

### Uninstalling the CMNM Software

To uninstall the CMNM software, type the following command:

```
CEMF Directory/uninstall/uninstallCSCOcmnm
```

### Verifying Uninstallation of CMNM

---

**Step 1** To verify that the CMNM package is not installed, type **pkginfo CSCOcmmn**.

The following message should appear:

```
ERROR: information for "CSCOcmnm" was not found
```

**Step 2** Type **pkginfo | grep EM** to verify that no CMNM Element Managers are installed.

**Step 3** Type **pkginfo CSCOcmev** to verify that CiscoView is not installed.

The following message should appear:

```
ERROR: information for "CSCOcmev" was not found
```

---

## Installing the Cisco MGC Host Provisioning Tool

There are two different Cisco VSC3000 and Cisco SC2200 provisioning tools depending on what network architecture you are running. If you are running the Cisco SS7 PRI Gateway Solution or the Cisco Tandem Offload Solution, install the Voice Services Provisioning Tool (VSPT). For all other architectures, install CMM.

- For information on installing and upgrading VSPT, refer to the Cisco VSPT web site.
- For information on installing and upgrading CMM, refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

## Configuring Reflection

CMNM has been tested with the following Xserver software package:

- Reflection 7.20

## Creating an XDMCP Connection

For Reflection to display CMNM correctly, Reflection must be run in XDMCP mode.

- 
- Step 1** Start Reflection.
- Step 2** From the Connection menu, select **New XDMCP Connection**.
- Step 3** From the Method pull-down menu, select **Broadcast** or **Direct**, then continue with one of the following set of steps:
- For Broadcast method:
- Click **Connect**.
  - Select the appropriate XDMCP computer. If you do not know which computer to select, contact your system administrator.
- For Direct method:
- In the Host Name field, enter the host name of an XDMCP computer.
  - Click **Connect**.
- 

## Fixing the Insufficient Colors Problem

To fix the "... insufficient colors available for CEMF Manager" problem, obtain a copy of the Sun Solaris file `rgb.txt`, download it your Winxx workstation, and configure Reflection to use the UNIX `rgb.txt` file as opposed to the Reflection default `rgb.txt` file.

- 
- Step 1** Change directory to your Reflection user directory using the following command:
- ```
cd Reflection Directory\user
```
- Step 2** Back up your original `rgb.txt` file using the following command:
- ```
cp rgb.txt rgb.txt.orig
```
- Step 3** Copy the UNIX file, `/usr/openwin/lib/X11/rgb.txt`, from your Sun Solaris workstation to your Winxx Reflection directory. You can use either FTP or RCP. If you are unable to use FTP or RCP to copy the `rgb.txt` file, contact your system administrator.
- To use FTP, type the following commands:
- ```
ftp your_workstation
cd /usr/lib/X11
get rgb.txt rgb_unix.txt
```
- Step 4** Configure Reflection:
- Bring up Reflection X Manager.
  - From the Settings menu, select **Color**.
  - Look for the RGB Color File frame and change the setting from `Reflection Directory\user\rgb.txt` to `Reflection Directory\user\rgb_unix.txt`.
- Step 5** Stop Reflection and restart Reflection.

**Note**

---

Just resetting the Reflection Xserver does not work; you must stop and restart Reflection.

---



# Configuring Network Devices for Management

## Introduction to Device Configuration

You must configure each network device for SNMP before it can be managed by CMNM. You must configure:

- SNMP community strings
- SNMP trap destination (that is, CMNM)
- Other miscellaneous SNMP settings

You must configure SNMP for the following devices:

- Cisco MGC
- Cisco SLT (2600)
- LAN switch (Catalyst 2900XL and Catalyst 5500)
- Cisco MGX 8260
- BAMS



### Note

If you plan to configure CMNM to forward traps to northbound systems, you should only configure SNMP Version 1 traps on network devices. CMNM only forwards SNMP Version 1 traps to northbound systems. For more information on forwarding traps, see the “Forwarding Traps to Other Systems” section on page 8-11.

## Configuring the Cisco MGC

To configure a Cisco MGC for network management:

- Step 1** Access the Cisco MGC by entering the command:  
`telnet Cisco-MGC-IP-address`
- Step 2** Type **su - root** to become the root user.
- Step 3** Type `cd /opt/CiscoMGC/snmp`.
- Step 4** Use a text editor to edit the `snmpd.cnf` file.

- Step 5** Search for the keyword `sysName` and change the system name to the hostname of the Cisco MGC. The entry should be:

```
sysName Cisco-MGC-hostname
```

- Step 6** Search for the keyword `communityEntry` and configure the read-only and read-write community string to be public. The entry should be:

```
communityEntry localSnmpID public Anyone localSnmpID default -
nonVolatile
```

- Step 7** Search for the keyword `snmpNotifyEntry` and configure CMNM as the trap receiver. Add the following line after the existing `snmpNotifyEntry` line:

```
snmpNotifyEntry 32 rambler trap nonVolatile
```



**Note** In the example above, the second field on the line, 32, should have a value that is 1 greater than the existing line. The example above assumes that the existing line has 31 as the second field in the line.

- Step 8** Search for the keyword `snmpTargetAddrEntry` and add the following line after the existing `snmpTargetAddrEntry` lines:

```
snmpTargetAddrEntry 33 snmpUDPDomain 10.1.1.1:0 100 3 rambler \
v1ExampleParams nonVolatile 255.255.255.255:0
```



**Note** In the example above, the IP address of the NMS is 10.1.1.1. The second field on the line, 33 in the example above, should have a value that is 1 greater than the existing line. The example above assumes that the existing line has 32 as the second field in the line.

- Step 9** Save the changes you made to the `snmpd.cnf` file.

- Step 10** Signal the SNMP daemon to reread the SNMP configuration file. From the Sun Solaris command line, enter the command:

```
ps -ef | grep snmpdm
```

You see information that resembles the following:

```
root 565 1 0 Mar 20 ? 0:01 /opt/CiscoMGC/bin/snmpdm -d
mgcusr 7463 23729 0 12:33:04 pts/13 0:00 grep snmpdm
```

The process ID of the `snmpdm` daemon is the second field on the line that ends with `snmpdm -d`. In this example, the process ID of the SNMP daemon is 565.

- Step 11** Enter the command:

```
kill -1 SNMP-daemon-process-ID
```

## Configuring a Cisco SLT (2600)

To configure a Cisco SLT (a Cisco 2600 router) for network management:

- 
- Step 1** Access the Cisco SLT by entering the command:
- ```
telnet Cisco-SLT-IP-address
```
- You see the password prompt.
- Step 2** Enter the login password for the Cisco SLT.
- You see the slt prompt.
- Step 3** Enter the command **enable**.
- You see the password prompt.
- Step 4** Enter the enable password for the Cisco SLT.
- You see the slt prompt.
- Step 5** Enter the command **configure terminal**.
- You see the slt(config) prompt.
- Step 6** Configure SNMP community strings. For example, to set the read-only community string to public and the read-write community string to private, enter the commands:
- ```
snmp-server community public RO
snmp-server community public RW
```
- Step 7** Configure traps to be sent to CMNM.
- To configure the Cisco SLT to send all types of traps, enter the command:  

```
snmp-server enable traps
```
  - To configure the Cisco SLT to send traps for all syslog messages with a severity of warnings or worse, enter the command (you can set this severity to the level you want):  

```
logging history warnings
```
  - To configure the IP address of the CMNM to which traps are sent, enter the command (in this example the IP address of the CMNM is 10.1.1.1):  

```
snmp-server host 10.1.1.1 public
```
- Step 8** Set the SNMP trap source, which specifies the Cisco SLT interface from which traps are sent. The SNMP trap source should be the interface with the IP address that the CMNM is configured to use for SNMP communications.
- For example, suppose that the IP address 10.2.2.2 is assigned to interface Ethernet 0/0 on the Cisco SLT. If CMNM is configured to communicate with the Cisco SLT using IP address 10.2.2.2, then the trap interface on the Cisco SLT should be Ethernet 0/0. In this example you would enter the command:
- ```
snmp-server trap-source Ethernet0/0
```
- Step 9** Set the maximum SNMP packet size to 4k by entering the command:
- ```
snmp-server packetsize 4096
```
- Step 10** To exit configuration mode, press Ctrl+Z. Then enter the **write** command to write the configuration to flash memory.
-

## Configuring a LAN Switch (Catalyst 2900XL)

To configure a LAN switch (Catalyst 2900XL) for network management:

- 
- Step 1** Access the LAN switch by entering the command:
- ```
telnet LAN-switch-IP-address
```
- You see the password prompt.
- Step 2** Enter the login password for the LAN switch.
- You see the 2900xl prompt.
- Step 3** Enter the command **enable**.
- You see the password prompt.
- Step 4** Enter the enable password for the LAN switch.
- You see the 2900xl prompt.
- Step 5** Enter the command **configure terminal**.
- You see the 2900xl(config) prompt.
- Step 6** Configure SNMP community strings. For example, to set the read-only community string to public and the read-write community string to private, enter the commands:
- ```
snmp-server community public RO
snmp-server community public RW
```
- Step 7** Configure traps to be sent to CMNM.
- To configure the LAN switch to send all types of traps, enter the command:  

```
snmp-server enable traps
```
  - To configure the IP address of the CMNM to which traps are sent, enter the command (in this example the IP address of the CMNM is 10.1.1.1):  

```
snmp-server host 10.1.1.1 public
```
- Step 8** Set the SNMP trap source, which specifies the LAN switch interface from which traps are sent. The SNMP trap source should be the interface with the IP address that the CMNM is configured to use for SNMP communications.
- For example, suppose that the IP address 10.2.2.2 is assigned to interface VLAN1 on the LAN switch. If CMNM is configured to communicate with the LAN switch using IP address 10.2.2.2, then the trap interface on the LAN switch should be VLAN1. In this example you would enter the command:
- ```
snmp-server trap-source VLAN1
```
- Step 9** Set the maximum SNMP packet size to 4k by entering the command:
- ```
snmp-server packetsize 4096
```
- Step 10** To exit configuration mode, press Ctrl+Z. Then enter the **write** command to write the configuration to flash memory.
-



## Configuring the LAN Switch (Catalyst 5500)

To configure a LAN switch (Catalyst 5500) for network management:

- 
- Step 1** Access the LAN switch by entering the command:  
`telnet LAN-switch-IP-address`  
You see the password prompt.
- Step 2** Enter the login password for the LAN switch.  
You see the cat prompt.
- Step 3** Enter the command **enable**.  
You see the password prompt.
- Step 4** Enter the enable password for the LAN switch.  
You see the cat(enable) prompt.
- Step 5** Configure SNMP community strings. For example, to set the read-only community string to public and the read-write community string to private, enter the commands:  
`set snmp-community read-only public`  
`set snmp-community read-write private`
- Step 6** Configure traps to be sent to CMNM.  
a. To configure the LAN switch to send all types of traps, enter the command:  
`set snmp trap enable`  
b. To configure the IP address of the CMNM to which traps are sent, enter the command (in this example the IP address of the CMNM is 10.1.1.1):  
`set snmp trap 10.1.1.1 public`
- Step 7** To exit enable mode, type **exit**.
- 

## Configuring the Cisco MGX 8260

To configure a Cisco MGX 8260 for network management:

- 
- Step 1** Start the Cisco MGX 8260 Web Viewer application by entering the command:  
`netscape Cisco-MGX-8260-IP-address`  
The Cisco MGX 8260 Web Viewer application opens in the web browser.
- Step 2** In the right pane, select **Node**, then **SNMP**.
- Step 3** Set the SNMP community strings:
- Read-only: public
  - Read-write: private

- Step 4** Configure trap registration by configuring the IP address of the CMNM to which traps are sent. For example, if the IP address of the CMNM is 10.1.1.1, register the trap receiver as 10.1.1.1.
- 

## Configuring BAMS

To configure a BAMS 1.0 for network management:

---

- Step 1** Access the BAMS server by entering the command:
- ```
telnet BAMS-server-IP-address
```
- Step 2** Log in using the user ID `acec`.
- Step 3** Navigate to the directory containing the configuration program by entering the command:
- ```
cd /opt/VSCcmp/bin
```
- Step 4** Load the proper environment by entering the command:
- ```
. sym_defs
```
- Step 5** Launch the BAMS system configuration interface by entering the command:
- ```
samari &
```
- You see the BAMS system configuration interface (named `CMP BAMS-server-IP-address`).
- Step 6** Select **System**, then **Trap Management**.
- You see the SNMP Trap Configuration window.
- Step 7** Select **Actions**, then **Add**.
- You see the Add SNMP Trap window.
- Step 8** Configure the IP address of the CMNM to which traps are sent. For example, if the IP address of the CMNM is 10.1.1.1, register the trap receiver as 10.1.1.1. Set the following information in the window:
- Name: *hostname of the NMS*
- Domain Name: *domain name of the NMS*
- Trap Definition Address: *IP address of the CMNM*
- Trap Destination Port: 162
- SNMP Version: 2 is better, 1 is OK
- Step 9** Click **OK** to save the trap receiver changes, select **File**, then **Exit** to close the SNMP Trap Configuration window.
- Step 10** You can control the severity of the SNMP traps sent to the trap receiver. On the `CMP BAMS-server-IP-address` window, select **System**, then **Alarm Management**.
- You see the Alarms Configuration window.
- Step 11** Set the message forward level to minor.
- If you set this level to informational or warning, a large number of traps of limited value are sent to the CMNM.
- Step 12** For the changes to take effect, you must stop and restart the BAMS:
- On the `CMP BAMS-server-IP-address` window, select **File**, then **Stop System**.

- b. Wait for BAMS to stop; this may take a couple minutes. When it has stopped, select **File**, then **Start System**.
-





## Getting Started with CMNM

---

### Starting a CMNM Session



**Note** CEMF should already be running. If, upon starting, you receive a message that CEMF is not running, do the following:

---

To start CEMF:

---

**Step 1** Log in as root.

**Step 2** From the command line on the terminal window, type:

```
cd CMNM_ROOT/bin
```

where *CMNM\_ROOT* is the CMNM installation root directory (for example, /opt/CSCOmngcm).

**Step 3** Type:

```
cemf start
```

---

To start a CMNM session:

---

**Step 1** Log in as your user ID.

**Step 2** From the command line on the terminal window, type:

```
CMNM_ROOT/bin/cemf session
```

where *CMNM\_ROOT* is the CMNM installation root directory (for example, /opt/CSCOmngcm).

You see the CEMF Login screen shown in Figure 4-1.

*Figure 4-1 CEMF Login Screen*

**Step 3** Enter your user name and password, then click **Ok** to proceed.

If you enter an unknown user name or password, you see an error message.



**Note** The default user ID is admin and the default password is admin.

**Step 4** Click **Ok**, then enter a valid user name and corresponding password.

You have three attempts to specify a valid user name and corresponding password. When you specify a valid user name and password, the session starts and the CEMF Launchpad screen, shown in Figure 4-2, is displayed.

If, after three attempts, you do not specify a valid user name and password, the session does not start and the Login window closes.

## Starting Applications from the CEMF Launchpad

CMNM is built upon the Cisco Element Management Framework (CEMF). CEMF provides alarm filtering and sorting, enhanced auto-discovery, data collection, and object group management.

CMNM provides the Cisco MGC node-specific functionality as an extension to the base CEMF services.

The CEMF Launchpad, shown in Figure 4-2, is used to access CMNM's features.

**Figure 4-2** CEMF Launchpad Screen



- **Viewer**—You can view, build, and monitor a network with Map Viewer. You can monitor the networks using network and network object connections.
- **Groups**—You can organize network elements into object groups with the Object Group manager. You can create, delete, and modify object groups.
- **Access**—The Access menu allows an administrator to set up users and user groups, assign passwords, and define access parameters.
- **Events**—Clicking the Events button brings up the Event Browser and Query Editor. You can create object groups or browse events from these screens.
- **Discovery**—The Discovery feature allows you to examine the network for IP and SNMP devices and create a managed object for each new device discovered.

To launch an application:


- 
- Step 1** From the CEMF Launchpad, click the desired application's 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 at any one time.

**Note**

If an application is already open, it appears in the Windows list. Click **Window** and choose the application you require from the pull-down menu.

## Quitting a CMNM Session

- Step 1** You can quit in the following ways:
- From the File menu, select **Quit**.
  - Press **Ctrl + Q**.
  - Click the **Close** icon  from the Toolbar.
- Step 2** A dialog box prompts you if you want to quit the CEMF Manager System. Click **Yes** to quit the session. All active applications are closed and the session terminates.

## Using CMNM Tools

You can use either the mouse or the keyboard to access the various features provided by CMNM. The mouse buttons are used for the functions listed below.

### Using the Mouse

Each button on the mouse is consistently used for different functions in CMNM.

- Click the left mouse button to:
  - Select
  - Activate
  - Set the location of the cursor
- Click the middle mouse button to:
  - Copy
  - Move
  - Drag
- Click the right mouse button to access pop-up menus by clicking and holding the right mouse button on a managed object within applications, such as the Map Viewer and the Object Group Manager, and events in the Event Browser.



## Shortcut Keys

### Ctrl +

Standard CMNM menus are available from the Toolbar. Items can be selected from the menus or by typing the keys in Table 4-1 and Table 4-2.

**Table 4-1 File Menu Short Cut Keys**

| Key Sequence    | File Menu Function |
|-----------------|--------------------|
| <b>Ctrl + Q</b> | Quit               |
| <b>Ctrl + W</b> | Close              |
| <b>Ctrl + P</b> | Print              |
| <b>Ctrl + S</b> | Save               |
| <b>Ctrl + N</b> | New                |
| <b>Ctrl + O</b> | Open               |

**Table 4-2 Edit Menu Short Cut Keys**

| Key Sequence    | File Menu Function |
|-----------------|--------------------|
| <b>Ctrl + Z</b> | Undo               |
| <b>Ctrl + X</b> | Cut                |
| <b>Ctrl + C</b> | Copy               |
| <b>Ctrl + V</b> | Paste              |
| <b>Ctrl + A</b> | Select all         |
| <b>Ctrl + D</b> | Deselect all       |



Note

---

When a menu option is grayed out, it is not available for selection.

---

### Alt +

Items in the CMNM screens may be presented with the first (initial) letter underlined; for example, Actions. This means you can either select this option by left-clicking the mouse, or you can type **Alt + A** (in this example) from the keyboard.

## Selecting from Lists in CMNM

### Block Selecting Multiple Items by Clicking and the Shift Key

---

Step 1 Select the first item.

The item is highlighted.

**Step 2** Press and hold the **Shift** key.

**Step 3** Select the last item in the sequence.

**Step 4** Release the **Shift** key.

All items between the first and last item are highlighted.

---

## Selecting Multiple Items by Clicking and the Ctrl Key

---

**Step 1** Select a relevant item in the list.

The item is highlighted.

**Step 2** Place the cursor over the next item to be selected.

**Step 3** Press **Ctrl** and click the left mouse button.

The item is highlighted.

**Step 4** Repeat Step 2 and Step 3 until all the required items are highlighted.



**Note**

This means of selection is useful when the items you wish to select are interspersed with other items.

---

## Selecting All Items

---

**Step 1** Place the cursor anywhere in the relevant window.

**Step 2** Press and hold the right mouse button.

A pop-up menu is displayed. If you do not see a pop-up menu, then this procedure does not work in the current window.

**Step 3** Move the cursor to the **Select All** option.

All items in the list are highlighted. This option may not be available in all windows.

---

## Deselecting All Items

---

**Step 1** Place the cursor anywhere in the relevant window.

**Step 2** Press and hold the right mouse button.

A pop-up menu is displayed. If you do not see a pop-up menu, then this procedure does not work in the current window.

**Step 3** Move the cursor to the **Deselect** option.

All items in the list are deselected. This option may not be available in all windows.

## Using Diagnostic Tools

The CMNM lets you launch a number of different debug, configuration, and diagnostic tools including those listed in Table 4-3.

**Table 4-3** *Diagnostic and Configuration Tools*

| Diagnostic Tool   | Available Devices    | Description                                                                                                                                           |
|-------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telnet            | All IP devices       | Standard Telnet application                                                                                                                           |
| CMM               | Cisco MGC host       | Cisco MGC Manager—Generic Cisco MGC host configuration tool used in all network architecture except those using the Voice Services Provisioning Tool. |
| Cisco MGC Toolbar | Cisco MGC host       | Cisco MGC diagnostic tools toolbar                                                                                                                    |
| XTerm             | Cisco MGC host/BAMS  | Standard Xterm application                                                                                                                            |
| CiscoView         | Cisco SLT/LAN switch | Cisco View application for the Cisco 2600 series, the Catalyst 2900XL Switch, and the Catalyst 5500 Switch                                            |
| VSPT              | Cisco MGC node       | Voice Services Provisioning Tool used for provisioning the Cisco SS7 PRI Gateway Solution and Cisco Tandem Offload Solution.                          |
| Web Viewer        | Cisco MGX 8260       | Used to view and configure the Cisco MGX 8260.                                                                                                        |

## Viewing Status Information

The area at the bottom of most windows displays status information.

When you double-click in this area, you see the Status Dialog screen shown in Figure 4-3. This screen lists previous status messages.

*Figure 4-3 Status Dialog Screen*

## Using the Toolbar

The Toolbar contains icons which invoke various tools and menu options. The icons displayed in the Toolbar vary, depending on which window is being viewed. You can disable the Toolbar so it is not displayed in the window.

## Enabling the Toolbar

From the Options menu, select **Show Toolbar**. The square next to Show Toolbar in the Options pull-down menu appears. The Toolbar is displayed only in the current window. The display of all other windows' Toolbars is not affected.



### Note

---

The Show Toolbar option toggles the displaying of the Toolbar on and off. If a square is displayed to the left of Show Toolbar in the Options pull-down menu, the Toolbar relevant to the current window is displayed.

---

*Figure 4-4 Example Toolbar*

## Disabling the Toolbar

From the Options menu, select **Show Toolbar**.

**Note**

---

The Show Toolbar option toggles the displaying of the Toolbar on and off. When a square is displayed to the left of Show Toolbar on the Options drop-down menu, the Toolbar relevant to the current window is displayed.

---

The square next to Show Toolbar on the Options pull-down menu disappears. A Toolbar is not displayed in the current window. The display of all other windows' Toolbars is not affected.

## Showing or Hiding Tooltips

Tooltips provide a brief description or explanation of a toolbar button or window panel. Tooltips appear when the cursor is positioned over the item. You can choose to show or hide tooltips.

From the Options menu, select or clear the **Enable Tooltip**.


**Note**

---

The Enable Tooltip option toggles the tooltips on and off. When a square is displayed to the left of Enable Tooltips on the Options pull-down menu, tooltips are displayed.

---


## Printing the View Displayed in the Window

- 
- Step 1** You can print in the following ways:
- From the File menu, select **Print**.
  - Press **Ctrl + P**.
  - Click the **Print** icon  from the Toolbar.

The displayed view is printed.

---

## Closing a Window

- 
- Step 1** You can close a window in the following ways:
- From the File menu select **Close**.
  - Press **Ctrl + W**.
  - Click the **Close** icon  from the Toolbar.
- 

## Accessing Help

CMNM provides online help for all of its features. A help button is on each of the CMNM dialogs and windows.

To access help, click the Help icon,  or select **Help** from the menu bar.

Clicking on the help button brings up the Netscape browser and displays the CMNM Help home page. If the help icon is not visible, on the toolbar select the **Options menu**, then select **Show Toolbar**.

*Figure 4-5 Options Menu*



Select **Enable Tooltips** to display text associated with icons as the cursor passes over them.

## Moving Between Open Windows

Each window has a Window menu, as shown in Figure 4-6. When a window is open, it appears as an option in this menu. Select **Window**, then choose the window you want to open from the list of windows provided in the Window menu.

*Figure 4-6 Window Drop-down Menu*





# Setting Up CMNM Security

## Introduction to CMNM Security

CMNM provides user access control which allows a system administrator to control what different users are able to do. Each user has a different login name and password, with a specific set of privileges within the system.

A standard administrator user (admin) is available by default. The administrator user has access to all features at all times. The administrator user may not be edited other than to change the password.

CMNM requires every user to have a login ID and password. Before users can start the application, they must specify their login ID and enter the correct password. An administrator account is provided to allow for creating, modifying, resetting, and deleting user accounts.

Within CMNM, access to features can be restricted on the basis of the user's access level to a subset (or group) of these features.

For example, administration of particular managed objects should be performed only by operators who are responsible for that particular site or for a region in which that site belongs. However, these operators may also require visibility of objects outside their own area of control.

The basic building blocks used to control user access are described below.

### User Groups

CMNM user accounts can be collected by an administrator into groups. These user groups can be used to model user roles. A typical setup might involve a user group for system administrators, for network fault detail users, and for operators to manage a given site.

It is on the basis of these user groups that CMNM applies access control. The CMNM administrator configures access control by assigning access specifications to the relevant user groups.

### Feature Lists

All features offered to a user are grouped together into feature lists. The benefit of feature lists is that it is easy to give access to a related set of features by simply choosing a feature list instead of having to assign features individually. Any given feature may appear in more than one feature list.

The feature lists available in CMNM are described in Table 5-1.



**Note**

In CMNM, features are preassigned to feature lists and cannot be modified.

Table 5-1 Feature Lists in CMNM

| Feature List                | Description                                                                                        |
|-----------------------------|----------------------------------------------------------------------------------------------------|
| AccessManagement            | Set up users, user groups, assign passwords, and define access parameters.                         |
| AutoDiscovery               | Examine the network for IP and SNMP devices.                                                       |
| BAM-Accounts                | View BAMS account information.                                                                     |
| BAM-Properties              | View BAMS property information.                                                                    |
| BAM-Provisioning            | Deploy BAMS.                                                                                       |
| BAM-States                  | Start and stop BAMS polling and comission and decommission BAMS.                                   |
| BAM-Tools                   | Use Telnet.                                                                                        |
| ChangePassword              | Change user password.                                                                              |
| Deployment                  | Deploy sites, objects, and networks manually and using a seed file.                                |
| Events-Clear-Acknowledge    | Clear and acknowledge events.                                                                      |
| Events-View                 | View events.                                                                                       |
| GenericConfigApplication    | Work with object configuration.                                                                    |
| Help                        | Get help information.                                                                              |
| LAN-Switch-Accounts         | View LAN switch account information.                                                               |
| LAN-Switch-Properties       | View LAN switch property information.                                                              |
| LAN-Switch-Provisioning     | Deploy LAN switch.                                                                                 |
| LAN-Switch-States           | Start and stop LAN switch polling and comission and decommission LAN switch.                       |
| LAN-Switch-Tools            | Start CiscoView and use Telnet.                                                                    |
| Launchpad                   | Use the CEMF launchpad.                                                                            |
| MGC-Host-Accounts           | View Cisco MGC host account information.                                                           |
| MGC-Host-Connectivity       | View Cisco MGC host connectivity information.                                                      |
| MGC-Host-Performance        | Monitor Cisco MGC host performance statistics.                                                     |
| MGC-Host-Properties         | View Cisco MGC host property information.                                                          |
| MGC-Host-Provisioning       | Deploy Cisco MGC host.                                                                             |
| MGC-Host-States             | Start and stop Cisco MGC host polling and comission and decommission Cisco MGC host.               |
| MGC-Host-Tools              | Start Cisco Media Gateway Controller Manager (CMM), use the MGC Toolbar, and use Xterm.            |
| MGW-Network-Performance     | Monitor media gateway network performance.                                                         |
| MGW-Network-Provisioning    | Deploy media gateway network.                                                                      |
| MGW-Network-States          | Start and stop media gateway network polling and comission and decommission media gateway network. |
| MGW-Network-Tools           | Start the Voice Services Provisioning Tool (VSPT).                                                 |
| MGW-Network-Trap-Forwarding | Define trap forwarding destinations.                                                               |



**Table 5-1 Feature Lists in CMNM**

| Feature List          | Description                                                                          |
|-----------------------|--------------------------------------------------------------------------------------|
| MGX-8260-Accounts     | View Cisco MGX 8260 account information.                                             |
| MGX-8260-Properties   | View Cisco MGX 8260 property information.                                            |
| MGX-8260-Provisioning | Deploy Cisco MGX 8260.                                                               |
| MGX-8260-States       | Start and stop Cisco MGX 8260 polling and comission and decommission Cisco MGX 8260. |
| MGX-8260-Tools        | Start Web Viewer.                                                                    |
| ObjectGroups-Edit     | Edit object groups.                                                                  |
| ObjectGroups-View     | View object groups.                                                                  |
| PerformanceManager    | Work with Performance Manager.                                                       |
| SLT-Accounts          | View Cisco SLT account information.                                                  |
| SLT-Properties        | View Cisco SLT property information.                                                 |
| SLT-Provisioning      | Deploy Cisco SLT.                                                                    |
| SLT-States            | Start and stop Cisco SLT polling and comission and decommission Cisco SLT.           |
| SLT-Tools             | Start CiscoView and use Telnet.                                                      |
| Viewer-Edit           | Edit the Map Viewer.                                                                 |
| Viewer-View           | Use the Map Viewer.                                                                  |

## Access Specifications

Access specifications connect together the user groups, the features that can be invoked by a group, and the objects upon which these features can be invoked.

A number of access specifications are provided by default with the CMNM. More access specifications can be built at the discretion of the system administrator.

Each access specification may include the following components:

- Feature lists—Lists the CMNM features which the users in this group have access to. A feature list can appear in more than one access specification.
- User groups—CMNM user accounts can be collected by an administrator into groups. These user groups can be used to model user roles. It is on the basis of these user groups that CMNM applies access control.
- A permission level—For example, read-only, read-write, and so on.
- An optional object group—Where an object group is supplied, the users in the group have access to the features specified by this access specification only for those objects contained within the group. Where no object group is supplied, the access specification provides the specified access to features for all objects. This object group could be used to grant the administrative user group for a site read-write access to the objects on that site, while another access specification would be used for read-only access for non-administrative users.

# Setting Up Accounts

CMNM allows the administrator to associate privileges with user accounts. For example, regular users can be prevented from performing certain management functions, while more technically sophisticated users can be given full management privileges.

CMNM provides the following security features:

- User login IDs and alphanumeric passwords
- Per-user privileges and control of administrative functions
- Administrative control of accounts and password resets
- Attack alerts (the connection is closed after three unsuccessful login attempts)

## Setting Up New Accounts

You must set up new accounts for all users. You may also define user groups.

To create a new account for a user and assign a password:

- 
- Step 1** Click the **Access** icon on the CEMF Launchpad, as shown in Figure 5-1.

*Figure 5-1 CEMF Launchpad Screen*



You see the Access Manager screen.

- Step 2** From the Access Manager screen, select **Edit**, **Create**, then **User** as shown in Figure 5-2.

**Figure 5-2** Access Manager Screen—Edit->Create>User Option



You see the screen in Figure 5-3.

**Figure 5-3** Create User Screen



**Step 3** Enter the requested information and then click **Forward**.

You see the screen in Figure 5-4.

*Figure 5-4 Copy from existing User Screen*



- Step 4** To use an existing user as a template for the user you are adding, click **Yes**, select the user you want to copy, then click **Forward**. If you do not want to copy an existing user or none exists, click **No** then click **Forward**.

You see the screen in Figure 5-5.

*Figure 5-5 Select User Groups Screen*



- Step 5** Select a user group, click an arrow to move it to the select user groups list, and click **Forward**. If no user groups are defined at this time, you may define a user group later and assign the user to it at any time. For more information on user groups, see the “” section on page 5-8.

You see the screen in Figure 5-6.

*Figure 5-6 User Password Entry Screen*



- Step 6** Enter a password for the user and confirm it. Passwords must contain 8 to 32 alphanumeric characters and at least one punctuation character such as `_`, `%`, `(`, or `^`. Click **Forward**.

If you typed a valid password, you see the screen in Figure 5-7. If you typed an invalid password, you see Figure 5-6 again with an error message. Reenter a valid password.

*Figure 5-7 Summary Details for User Screen*



- Step 7** To make changes, click **Back** and enter the corrected information. To add the user, click **Finish**. You see the screen in Figure 5-8 listing the defined users.

*Figure 5-8 Access Manager Screen—List of Users*



---

## Creating User Groups

Users can be divided into groups by creating user groups.

- 
- Step 1** From the Access Manager screen, select **Edit, Create**, then **User Group** as shown in Figure 5-9.

*Figure 5-9 Access Manager Screen—Edit->Create->User Group Option*



You see the screen in Figure 5-10.

*Figure 5-10 Create User Group Screen*



**Step 2** Type the name of a user group in the field and click **Forward**.

**Step 3** You see the screen in Figure 5-11.

*Figure 5-11 Copy from existing User Group Screen*



**Step 4** If you:

- Want to use an existing user group as a template for the user group you are adding, click **Yes**, select the user group you want to copy, then click **Forward**. You see the screen in Figure 5-14.
- Do not want to copy an existing user group or none exists, click **No**, then click **Forward**. You see the screen in Figure 5-12.

*Figure 5-12 Select Users Screen*



- Step 5** Select each user you want in the new group and click the arrow to move each to the selected users list. When you are finished, click **Forward**.

You see the screen in Figure 5-13.

*Figure 5-13 Select Access Specifications Screen*



- Step 6** Select each access specification you want for the new group and click the arrow to move each to the selected access specification list. When you are finished, click **Forward**.



**Caution**

---

Giving a user group full access allows each user in the user group to add or delete other users and to change specifications for all other users.

---



For more information about access specifications, see the “Creating New Access Specifications” section on page 5-11.

You see the screen in Figure 5-14.

*Figure 5-14 Summary Details for User Group Screen*



**Step 7** To make changes, click **Back** and enter the corrected information. To add the user group, click **Finish**.

---

## Creating New Access Specifications

To create new access specifications:

**Step 1** From the Access Manager screen, select **Edit**, **Create**, then **Access Spec**, as shown in Figure 5-15.

*Figure 5-15 Access Manager Screen—Edit->Create->Access Spec Option*



You see the screen in Figure 5-16.

*Figure 5-16 Create Access Spec Screen*



- Step 2** Type the name of a new access specification and click **Forward**.  
You see the screen in Figure 5-17.

*Figure 5-17 Copy from existing Access Spec Screen*



- Step 3** If you:
- Want to use an existing access specification as a template for the access specification you are adding, click **Yes**, select the access specification you want to copy, then click **Forward**. You see the screen in Figure 5-22.
  - Do not want to copy an existing access specification or none exists, click **No**, then click **Forward**. You see the screen in Figure 5-18.

*Figure 5-18 Select Permission Screen*



**Step 4** Select the permission level desired and click **Forward**.

You see the screen in Figure 5-19.

*Figure 5-19 Select User Groups Screen*



**Step 5** Select a user group from the available user groups list and click the right arrow to move it to the selected user groups list. Click **Forward**.

You see the screen in Figure 5-20.

*Figure 5-20 Select Feature Lists Screen*



- Step 6** Select each feature you want for the new access specification and click the right arrow to move each to the selected feature list. When you are finished, click **Forward**.

You see the screen in Figure 5-21.

*Figure 5-21 Select Object Groups Screen*



- Step 7** Select each object group you want for the new access specification and click the right arrow to move each to the selected object groups list. When you are finished, click **Forward**.

You see the screen in Figure 5-22.

*Figure 5-22 Summary Details for Access Specification Screen*



- Step 8** To make changes, click **Back** and enter the corrected information. To add the access specification, click **Finish**.
-

## Creating Typical Types of Users

Table 5-2 summarizes how you would create three typical users.

*Table 5-2 Creating Typical Users*

| To Create This Type of Account:                                | Perform These Steps:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrator                                                  | Using the instructions in the “Setting Up New Accounts” section on page 5-4, create a new account and create the user by copying the existing administrator template.                                                                                                                                                                                                                                                                                                                                  |
| Operator with read permission that can deploy and launch tools | <p>Using the instructions in the “Creating New Access Specifications” section on page 5-11, create a new access specification with the following features:</p> <p>Using the instructions in the “Creating User Groups” section on page 5-8, create a new user group with the access specification you just created.</p> <p>Then using the instructions in the “Setting Up New Accounts” section on page 5-4, create a new account, create the user, and assign them to the group you just created.</p> |
| Operator with read-only permission                             | <p>Using the instructions in the “Creating New Access Specifications” section on page 5-11, create a new access specification with the following features:</p> <p>Using the instructions in the “Creating User Groups” section on page 5-8, create a new user group with the access specification you just created.</p> <p>Then using the instructions in the “Setting Up New Accounts” section on page 5-4, create a new account, create the user, and assign them to the group you just created.</p> |

## Modifying Users

To modify a user:

- 
- Step 1** From the Access Manager screen, select **Edit, Modify**, then **User**.

You see the screen in Figure 5-23.

*Figure 5-23 User Editor Screen*



- Step 2** Select a user from the list and change any information in the fields. To change the user groups that the user belongs to, click the **Select User Groups** tab and make any changes.
- Step 3** Click **Apply**. To cancel changes, click **Revert**.
- 

## Modifying User Groups

To modify a user group:

- Step 1** From the Access Manager screen, select **Edit, Modify**, then **User Group**.  
You see the screen in Figure 5-24.

*Figure 5-24 User Group Editor Screen—Select Users Tab*



- Step 2** Select a user group from the list of available user groups. Select users and click the arrows to add or remove users from the group.
- Step 3** To modify access specifications for the user group, click the **Select Access Specifications** tab.

You see the screen in Figure 5-25.

*Figure 5-25 User Group Editor Screen—Select Access Specifications Tab*



- Step 4 Select access specifications and click the arrows to add or remove access specifications from the group.
  - Step 5 Click **Apply**. To cancel changes, click **Revert**.
- 

## Modifying Access Specifications

To modify an access specification:

- Step 1 From the Access Manager screen, select **Edit, Modify**, then **Access Spec**.
- Step 2 You see the screen in Figure 5-26.



*Figure 5-26 Access Specification Editor Screen—Select Permission Tab*



- Step 3 Edit the permission if necessary.
- Step 4 Click the **Select User Groups** tab.
- Step 5 You see the screen in Figure 5-27.

*Figure 5-27 Access Specification Editor Screen—Select User Groups Tab*



- Step 6** Select user groups and click the arrows to add or remove users groups from the access specification.
- Step 7** Click the **Select Feature Lists** tab.  
You see the screen in Figure 5-28.

*Figure 5-28 Access Specification Editor Screen—Select Feature Lists Tab*



- Step 8** Select features and click the arrows to add or remove features from the access specification.
- Step 9** Click the **Select Object Groups** tab.
- Step 10** You see the screen in Figure 5-29.

*Figure 5-29 Access Specification Editor Screen—Select Object Groups Tab*



- Step 11** Select object groups and click the arrows to add or remove object groups from the access specification.

**Step 12** When you are finished, click **Apply**. To discard changes, click **Revert**. Click **Close**.

---

## Changing the Administrative Password

To change the administrative password:

**Step 1** From the Access Manager screen, select **Edit**, then **Change Admin Password**, as shown in Figure 5-30.

*Figure 5-30 Access Manager Screen—Edit>Change Admin Password Option*



You see the screen in Figure 5-31.

*Figure 5-31 Change User Password Screen*



**Step 2** Change the password and click **Apply**.

---





# Deploying a Site, Object, or Network

---

## Introduction to Deployment

This chapter describes how to deploy a site, object, or network. Deployment is the term used within CMNM to mean the addition of objects to the CEMF network model. CMNM provides two methods to deploy Cisco MGC nodes and subobjects:

- Manual deployment uses the standard CEMF deployment framework.
- Seed file deployment allows you to specify, on a bulk basis rather than on an individual basis, the components to be managed.

Seed file configuration requires that you define the Cisco MGC network or object (or a portion of it) in an external file that is read by CMNM. Based on the contents of this file, CMNM deploys the file to Cisco MGC nodes and subnodes.

## Meeting Password Requirements

IDs and passwords must be consistent across all of the devices being deployed or deployment does not fully succeed. As a result, you must use an additional CEMF dialog to specify the correct login ID and password for the devices. In addition, you have to manually discover the logical connectivity network for those devices.

Anytime a password is changed on a device, you must make a corresponding change in CMNM. Otherwise CMNM's saved passwords do not match those on the devices; polling and connectivity network discovery fail. The same is true for SNMP community strings on the Cisco SLTs and LAN switch.

- When using manual deployment, the deployment wizard templates prompt for the appropriate IDs and passwords.
- When using seed-file deployment, you are prompted to enter the name of the seed-file, the login IDs, and passwords.

## Device Inventory

Inventory attributes are shown for each type of device in the CMNM object model. This data is available using a number of dialogs that can be invoked against an object. The following sections outline the data that is available in these dialogs.

## Alternate Cisco MGC Configurations

CMNM is able to support any type of Cisco MGC configuration. As such, CMNM does not make any assumptions as to the presence of the various devices. For example, when directed SP links are used, SS7 signaling is terminated on the media gateway. Therefore there are no Cisco SLT devices. CMNM is designed so that it gracefully handles the absence of the Cisco SLTs and LAN switches. However, there must be at least one Cisco MGC host defined.

Different configurations result in changes to the elements in the connectivity network and the relationship between the connectivity network objects. However, CMNM is able to dynamically create the hierarchical representation of the configuration network regardless of how the Cisco MGC is being used.

## Cisco SLT and LAN Switch Inventory

The Cisco SLT and LAN switch are listed as generic network devices. The data in Table 6-1 is associated with each Cisco SLT and LAN switch. Some of the data is accessible using SNMP. The remaining data is stored as local attributes in the CEMF database.

**Table 6-1 Cisco SLT and LAN Switch Inventory**

| Attribute              | Description                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------|
| SNMPv2-MIB.sysContact  | Identification of the contact person for the device.                                                    |
| SNMPv2-MIB.sysDesc     | Textual description of the device.                                                                      |
| SNMPv2-MIB.sysLocation | Physical location of the device.                                                                        |
| SNMPv2-MIB.sysName     | Administratively assigned name for the device.                                                          |
| SNMPv2-MIB.sysUpTime   | Time (in hundredths of a second) since the network management portion of the system was re-initialized. |
| IP Address             | IP Address of the Cisco SLT/LAN switch host                                                             |
| Login ID               | IOS/Switch Code login ID                                                                                |
| Login Password         | IOS/Switch Code Telnet login password                                                                   |
| Enable Password        | Enable-mode password                                                                                    |
| SNMP Read Community    | SNMP read-community string                                                                              |
| SNMP Write Community   | SNMP write-community string                                                                             |

## Interfaces

Each Cisco SLT and LAN switch has numerous network interfaces. Tables from the IF-MIB are read to determine how many network interfaces are in each network element.

For each network interface, the inventory data in Table 6-2 is retrieved (using SNMP) and displayed.

**Table 6-2 Cisco SLT and LAN Switch Network Interface Inventory**

| Attribute      | Description                      |
|----------------|----------------------------------|
| IF-MIB.ifIndex | Unique value for each interface. |

**Table 6-2 Cisco SLT and LAN Switch Network Interface Inventory**

|                      |                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------|
| IF-MIB.ifAdminStatus | Desired state of the interface.                                                                                    |
| IF-MIB.ifDescr       | Textual string containing information about the interface.                                                         |
| IF-MIB.ifLastChange  | Value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable.                        |
| IF-MIB.ifMtu         | Size of the largest packet that can be sent or received on the interface, specified in octets.                     |
| IF-MIB.ifOperStatus  | Current operational state of the interface.                                                                        |
| IF-MIB.ifPhysAddress | Interface's address at its protocol sublayer.                                                                      |
| IF-MIB.ifSpecific    | Reference to MIB definitions specific to the particular media being used to realize the interface.                 |
| IF-MIB.ifSpeed       | Estimate of the interface's current bandwidth in bits per second.                                                  |
| IF-MIB.ifType        | Type of the interface.                                                                                             |
| IF-MIB.ifInErrors    | Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. |
| IF-MIB.ifInOctets    | Total number of octets received on the interface, including framing characters.                                    |
| IF-MIB.ifOutErrors   | Number of outbound packets that could not be transmitted because of errors.                                        |
| IF-MIB.ifOutOctets   | Total number of octets transmitted out of the interface, including framing characters.                             |

In addition to the network interfaces, each Cisco SLT has numerous TDM interfaces (the connections to the STPs). MIB tables from the RFC1406-MIB are read to determine how many TDM interfaces are present.

For each Cisco SLT TDM interface, the statistical data in Table 6-3 is retrieved (using SNMP) and displayed.

**Table 6-3 Cisco SLT and LAN Switch Network Interface Statistics**

| Attribute                         | Description                                                                                            |
|-----------------------------------|--------------------------------------------------------------------------------------------------------|
| RFC1406-MIB.dsx1IfIndex           | Value for this object is equal to the value of ifIndex from the Interfaces table of MIB II (RFC 1213). |
| RFC1406-MIB.dsx1CurrentESs        | Number of errored seconds encountered by a DS1 interface in the current interval.                      |
| RFC1406-MIB.dsx1CurrentSESs       | Number of severely errored seconds encountered by a DS1 interface in the current interval.             |
| RFC1406-MIB.dsx1IntervalESs       | Number of errored seconds encountered by a DS1 interface in a previous interval.                       |
| RFC1406-MIB.dsx1IntervalSESs      | Number of severely errored seconds encountered by a DS1 interface in a previous interval.              |
| RFC1406-MIB.dsx1FarEndIntervalESs | Number of far end errored seconds encountered by a DS1 interface in a previous interval.               |

**Table 6-3 Cisco SLT and LAN Switch Network Interface Statistics**

|                                    |                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------|
| RFC1406-MIB.dsx1FarEndIntervalSESs | Number of far end errored severely seconds encountered by a DS1 interface in a previous interval.  |
| RFC1406-MIB.dsx1FarEndCurrentESs   | Number of far end errored seconds encountered by a DS1 interface in the current interval.          |
| RFC1406-MIB.dsx1FarEndCurrentSESs  | Number of far end severely errored seconds encountered by a DS1 interface in the current interval. |

Each device supports a number of different memory pools (defined in the `ciscoMemoryPoolTable` table). At a minimum, a device that implements CISCO-MEMORY-POOL-MIB must support the processor memory pool. Any other memory pools are device-specific.

CMNM displays data from the Cisco SLT memory pools described in Table 6-4.

**Table 6-4 Cisco SLT Memory Pools**

| Memory Pool      | CiscoMemoryPoolTable Index |
|------------------|----------------------------|
| Processor Memory | 1                          |
| I/O Memory       | 2                          |

CMNM displays data from the LAN switch memory pools described in Table 6-5.

**Table 6-5 LAN Switch Memory Pools**

| Memory Pool      | CiscoMemoryPoolTable Index |
|------------------|----------------------------|
| Processor Memory | 1                          |
| Flash Memory     | 6                          |
| Non-Volatile RAM | 7                          |
| MBUF Memory      | 8                          |
| Cluster Memory   | 9                          |
| Malloc Memory    | 10                         |

## Cisco MGC Host Inventory

Unlike the Cisco SLT and LAN switch, no inventory data is retrieved via SNMP from the Cisco MGC host. Rather, certain (static) data, described in Table 6-6, is retrieved during object deployment.

**Table 6-6 Cisco MGC Host Inventory**

| Description              | Data Source                                           |
|--------------------------|-------------------------------------------------------|
| Desired Platform State   | XECfgParm.dat: desiredPlatformState                   |
| IP Peer Addresses        | XECfgParm.dat: ipAddrPeerA, ipAddrPeerB               |
| Network Addresses        | XECfgParm.dat: IP_Addr1, IP_Addr2, IP_Addr3, IP_Addr4 |
| Transpath Home Directory | XECfgParm.dat: homeDirRoot                            |
| Virtual Switch Indicator | XECfgParm.dat: SysVirtualSwitch                       |



**Table 6-6 Cisco MGC Host Inventory**

|                              |                                 |
|------------------------------|---------------------------------|
| MGC Host Vendor              | XECfgParm.dat: product.vendor   |
| MGC Host Version             | XECfgParm.dat: product.version  |
| Maximum Number of Links      | XECfgParm.dat: maxNumLinks      |
| Maximum Number of PRI Links  | XECfgParm.dat: maxNumPRIL3Links |
| Maximum Number of MGCP Links | XECfgParm.dat: maxNumMGCPLinks  |
| Solaris OS Release Level     | uname -r                        |
| Solaris OS Version           | uname -v                        |
| Solaris Hostname             | hostname or uname -n            |
| Solaris Host ID              | hostid                          |
| Solaris Serial Number        | sysinfo                         |
| Solaris Hardware Model       | sysinfo                         |
| Number of CPUs               | sysinfo                         |
| Last Boot Time               | sysinfo                         |
| Main Memory Size             | sysinfo                         |

Other data is stored in the local CEMF database. The data in Table 6-7 is entered during deployment of the Cisco MGC host objects and is used internally by the CMNM systems.

**Table 6-7 Cisco MGC Host Local Inventory**

| Attribute     | Description                                         |
|---------------|-----------------------------------------------------|
| IP Address    | IP Address of the Cisco MGC Host                    |
| MML Login ID  | Login ID for invoking an MML session                |
| MML Password  | Password for the specified ID                       |
| Root Password | Password for the root account (used when rebooting) |

## Connectivity Network Inventory

CMNM displays the logical connectivity network from the Cisco MGC host to external devices. Each one of these logical connections is represented as a node in the CEMF object viewer.

Each connectivity network object type has an inventory dialog associated with it. The contents of these inventory dialogs match the contents of the connectivity network object model.

## Synchronization

CMNM ensures that the EMS database (as provided by CEMF) is synchronized with the underlying network elements. All relevant management data within the EMS is automatically updated on receipt of a modification trap from the various network elements.

The traps in Table 6-8 are used to respond to changes in the network elements.

**Table 6-8 Network Element Configuration Traps**

| Network Element | Configuration Changed Trap         |
|-----------------|------------------------------------|
| Cisco MGC host  | POM: DynamicReconfiguration        |
| LAN switch      | coldStart, warmStart, configChange |
| Cisco SLT       | reload, configChange               |

When CMNM receives a POM:DynamicReconfiguration trap from the active Cisco MGC host, it resynchronizes its view of the connectivity network with that of the device.

## Deploying a Network Using a Seed File

For bulk deployment, you can use a deployment seed file. This seed file contains all of the information necessary to deploy an entire Cisco MGC network.



### Note

Only one site can be deployed at a time. Each site requires a separate seed file.

This seed file contains the IP addresses of all of the devices in the Cisco MGC network, plus the relationship (hierarchy) between the devices. Given this file, CMNM is able to automatically deploy all of the elements in the network.

The data in the seed file includes, but is not limited to the:

- Logical names of each Cisco MGC node in the network
- IP address of each Cisco MGC host for each Cisco MGC node
- IP address of each Cisco SLT for each Cisco MGC node
- IP address of each LAN switch for each Cisco MGC node

A sample seed file is shown in Example 6-1.

### Example 6-1 Sample Seed File

```
BAM (name=bam1, ip=172.18.137.103)
MGC (name=mgc1)
{
  HOST (ip = 172.18.145.30)
  SLT (name = 2600a, ip = 172.18.145.9)
  SLT (name = 2600b, ip = 172.18.145.10)
  SWITCH (name = n2900XL-a, ip = 172.18.145.12)
}
GATEWAY (name=gateway1, ip = 172.24.236.118) }
```

## Seed File Attributes

The seed file allows you to specify a number of attributes for each device. In some cases these attributes are required. Optional attributes assume a default value if they are not specified. The default values are specified in the seed file deployment dialog.

The supported attributes are described in Table 6-9.

Table 6-9 Seed File Attributes

| Attribute      | Device Types              | Required                                  | Description                               |
|----------------|---------------------------|-------------------------------------------|-------------------------------------------|
| name           | All                       | Only on Cisco MGC node, BAMS, and gateway | Name of the object as seen in the GUI     |
| ip             | All except Cisco MGC node | Yes                                       | IP Address of the network element         |
| login          | All except Cisco MGC node | No                                        | Login ID for the device                   |
| password       | All except Cisco MGC node | No                                        | Password to login to the device           |
| rootPassword   | Cisco MGC host            | No                                        | Root (super-user) password for the device |
| enablePassword | Cisco SLT, switch         | No                                        | IOS and Catalyst enable password          |
| read           | All except Cisco MGC node | No                                        | SNMP read-community string                |
| write          | All except Cisco MGC node | No                                        | SNMP write-community string               |

Each Cisco MGC can have, at most, one active host. You can define a maximum of two hosts per Cisco MGC, one representing the active Cisco MGC host and the other the standby Cisco MGC host. You do not have to define which host is active or standby; this is determined automatically by CMNM.

You must specify the name for each Cisco MGC node. Optionally, you can then specify names for the other elements. If no name is specified, a default name is generated. In addition, you can specify account information about the various devices: login IDs, passwords, and SNMP community strings. Each value is optional and, if missing, is initialized by the corresponding value in the seed file deployment dialog.

To perform seed file deployment, you launch a dialog from a site node or other type of CEMF container. This dialog prompts you for the name of the seed file and the login ID and password for the Cisco MGC host devices. You also specify SNMP read- and write-community passwords for the Cisco SLT and LAN switch.

## Specifying a Deployment Seed File

To deploy a network using a seed file:

- 
- Step 1 From the Map Viewer screen, select the site icon.
  - Step 2 Right-click to display the pull-down menu, select **Deployment**, then **Deploy Network Seed File**.




---

**Note** Only one site can be deployed at a time. Each site requires a separate seed file.

---

You see the screen in Figure 6-1.

*Figure 6-1 Deploy Network Screen—Display Tab*



- Step 3** To enter account information, click the **Accounts** tab.  
You see the screen in Figure 6-2.

*Figure 6-2 Deploy Network Screen—Account Tab*



- Step 4** If any fields for a type of device are not specified in the seed file, you can enter account information for each type of device on this screen. When you are finished, click the **Deploy** tab to return to the screen in Figure 6-1.
- Step 5** Enter a filename in the Seed Filename field and click **Deploy**.  
You see the screen in Figure 6-3.

*Figure 6-3 Deploy Confirmation Prompt*



- Step 6** Click **Yes**.  
The network is deployed.
- 

## Manually Deploying a Site, Object, or Network

The deployment wizard is the graphical interface used to create new objects representing the network elements to be managed with CMNM. The deployment wizard uses deployment profiles to prompt you for the information that is required by the deployment process. It can be accessed from different windows within CMNM as outlined below.

**Note**

Only one deployment wizard can be open at any time. If you attempt to open a second wizard, you see the message:

The Deployment Wizard is already active. Select it from the Window menu, or check for iconified or hidden windows.

Complete the first deployment task before proceeding.

CMNM defines a number of templates that allow you to manually configure Cisco MGC nodes and subobjects. The templates include:

- Template to deploy a top-level Cisco MGC node (This template also allows you to deploy a Cisco MGC host pair as a child of the Cisco MGC node.)
- Template to deploy a top-level gateway (Cisco MGX 8260)
- Template to deploy a top-level BAMS
- Template to deploy a Cisco MGC host pair as child of a Cisco MGC node
- Template to deploy a Cisco SLT as a child of a Cisco MGC node
- Template to deploy a LAN switch as a child of a Cisco MGC node

The deployment wizard reads the templates and presents screens prompting for information about the devices.

## Deployment Attributes

Table 6-10 describes deployment attributes.

**Table 6-10 Deployment Attributes Table**

| Attribute       | Device Type                           | Required               | Description                             |
|-----------------|---------------------------------------|------------------------|-----------------------------------------|
| Name            | All                                   | Yes                    | Name of the object as seen in the GUI   |
| Ip              | All except Cisco MGC and common host  | Yes                    | IP address of the network element       |
| Login           | Cisco MGC host, Cisco SLT, LAN switch | Yes for Cisco MGC host | Login ID for the device                 |
| Password        | Cisco MGC host, Cisco SLT, LAN switch | Yes                    | Password to login to the device         |
| Root password   | Cisco MGC host                        | Yes                    | Root (super-user) password for the host |
| Enable password | Cisco SLT, LAN switch                 | Yes                    | IOS/Catalyst enable password            |

Table 6-10 Deployment Attributes Table

|                 |                                      |     |                             |
|-----------------|--------------------------------------|-----|-----------------------------|
| Read Community  | All except Cisco MGC and common host | Yes | SNMP read-community string  |
| Write community | All except Cisco MGC and common host | Yes | SNMP write-community string |

## Opening the Deployment Wizard

To open the deployment wizard:

- 
- Step 1** Right-click the object below which you want to deploy.
  - Step 2** From the pop-up menu, select **Deployment**, then select **Deploy Generic Objects**.  
You see the screen in Figure 6-4.

Figure 6-4 Deployment Wizard Screen—Templates



## Deploying a Site

A site is a generic, non-technology-specific object.



**Note** When you launch the deployment wizard, you are presented with a set of all available generic deployment profiles.

To deploy a site:

- 
- Step 1** From the CEMF Launchpad screen, click the **Viewer** icon. The Map Viewer window opens.
- Step 2** On the left pane of the Map Viewer window, right-click the **Physical Site** icon, select **Deployment**, then **Deploy Generic Objects** as shown in Figure 6-5.

*Figure 6-5 Deployment Wizard Screen—Deploy Generic Objects Option*



You see the screen in Figure 6-6.

*Figure 6-6 Deployment Wizard Screen—Templates*



- Step 3** In the template options list, select **Site** and click **Forward**.

You see the screen in Figure 6-7.




---

**Note** You can cancel at any point before you click **Finish**.

---



*Figure 6-7 Deployment Wizard Screen—Object Parameters (Number of Sites)*



- Step 4** Enter the number of sites; the default is 1. Click **Forward**.  
You see the screen in Figure 6-8.

*Figure 6-8 Deployment Wizard Screen—Object Parameters (Site Name)*



- Step 5** Enter a name (one word with no spaces) as the Site name. Click **Forward**.  
You see a screen similar to Figure 6-9, only the fields are blank.

*Figure 6-9 Deployment Wizard Screen—Views*



- Step 6** Next to the Physical field, click **Select**.  
You see the screen in Figure 6-10.

*Figure 6-10 Object Selector Screen*



- Step 7** Click the **Physical** item to select it, then click **Apply**.  
The Object Selector window closes. In Figure 6-9, the Physical and genericObjects fields should be filled in with the word physical.
- Step 8** Click **Forward**.
- Step 9** If you entered more than one site in Step 4, continue with the screen in Figure 6-8.  
When you are done, you see the screen in Figure 6-11.

*Figure 6-11 Deployment Wizard Screen—Summary*



This screen summarizes the deployment you have created and allows you to commit or reject the deployment.

**Step 10** Click **Finish**.

You are informed if deployment has been successful. A site icon appears on the right pane of the Map Viewer window.

---

## Deploying a Media Gateway Network

To deploy a Cisco media gateway network:

---

- Step 1** Open the Map Viewer window.
- Step 2** Click to select a Site icon from the left panel of the Map viewer window.
- Step 3** Right-click the **Site** icon, select **Deployment**, then **Deploy Media Gateway Network**, as shown in Figure 6-12.

*Figure 6-12 Map Viewer Screen—Deployment>Deploy Media Gateway Network Option*



You see the screen in Figure 6-13.

*Figure 6-13 Deployment Wizard Screen—Templates*



**Step 4** Select the template you want to use and click **Forward**.

You see the screen in Figure 6-14.

*Figure 6-14 Deployment Wizard Screen—Object Parameters*



**Step 5** Enter the name of the media gateway controller (no spaces). Click **Forward**.

You see a screen similar to Figure 6-11. This screen summarizes the deployment you have created and allows you to commit or reject the deployment.

**Step 6** Click **Finish**.

You are informed if deployment has been successful. A Cisco MGC icon appears on the right pane of the Map Viewer window.

- Step 7** Deploy Cisco MGC hosts by following the instructions in the “Deploying a Cisco MGC Host” section on page 6-17.
  - Step 8** Deploy Cisco SLTs by following the instructions in the “Deploying a Cisco SLT” section on page 6-17.
  - Step 9** Deploy LAN switches by following the instructions in the “Deploying a LAN Switch” section on page 6-18.
  - Step 10** Deploy Cisco MGX 8260s by following the instructions in the “Deploying a Cisco MGX 8260” section on page 6-18.
  - Step 11** Deploy the optional Billing and Measurement Server by following the instructions in the “Deploying a Billing and Measurements Server (BAMS)” section on page 6-18.
- 

## Deploying a Cisco MGC Host

---

- Step 1** Open the Map Viewer window.
- Step 2** Click to select a MGC icon from the left panel of the Map Viewer window.
- Step 3** Right-click the **MGC** icon and select **Deployment**, then **Deploy MGC Host**.
- Step 4** Enter a number in the field Number of MGC Hosts; the default is 1. Click **Forward**.
- Step 5** Enter data for the host. See Table 6-10 on page 6-10 for descriptions of the fields. Click **Forward**.
- Step 6** Repeat Step 5 for each deployed host. Make sure that you enter the same login and passwords.
- Step 7** Click **Finish**.

A common-host icon appears on the right pane of the Map Viewer window. Also, a host icon appears on the left panel as a child node of the common-host node.

---

## Deploying a Cisco SLT

---

- Step 1** Open the Map Viewer window.
- Step 2** Click to select a Cisco MGC icon from the left panel of the Map Viewer window.
- Step 3** Right-click the **MGC** icon and select **Deployment**, then **Deploy SLT Chassis**.
- Step 4** Enter data for the Cisco SLT. See Table 6-10 on page 6-10 for descriptions of the fields. Click **Forward**.
- Step 5** Click **Finish**.

A Cisco SLT icon appears on the right pane of the Map Viewer window.

---

## Deploying a LAN Switch

---

- Step 1 Open the Map Viewer window.
  - Step 2 Click to select a Cisco MGC icon from the left panel of the Map Viewer window.
  - Step 3 Right-click the **MGC** icon and select **Deployment**, then **Deploy LAN Switch**.
  - Step 4 Enter data for the LAN switch. See Table 6-10 on page 6-10 for descriptions of the fields. Click **Forward**.
  - Step 5 Click **Finish**.  
A LAN switch icon appears on the right pane of the Map Viewer window.
- 

## Deploying a Cisco MGX 8260

---

- Step 1 Open the Map Viewer window.
  - Step 2 Click to select a Site icon from the left panel of the Map Viewer window.
  - Step 3 Right-click the **Site** icon and select **Deployment**, then **Deploy MGX8260**.
  - Step 4 Enter data for the Cisco Media Gateway. See Table 6-10 on page 6-10 for descriptions of the fields. Click **Forward**.
  - Step 5 Click **Finish**.  
A Cisco Media Gateway icon appears on the right pane of the Map Viewer window.
- 

## Deploying a Billing and Measurements Server (BAMS)

---

- Step 1 Open the Map Viewer window.
  - Step 2 Click to select a Site icon from the left panel of the Map Viewer window.
  - Step 3 Right-click the **Site** icon and select **Deployment**, then **Deploy Billing and Measurement Server**.
  - Step 4 Enter data for the BAMS server. See Table 6-10 for descriptions of the fields. Click **Forward**.
  - Step 5 Click **Finish**.  
An icon appears on the right pane of the Map Viewer window.
-



## Using Polling to Monitor Network Performance

---

### Introduction to Performance Monitoring

An important component of efficient network management is the ability to receive performance information on a large network of many devices to provide an overall view of the your network's functioning. You can then pro-actively manage your network elements by analyzing the performance data.

CMNM lets you monitor the performance statistics gathered from network elements managed by CEMF. CMNM collects performance information from the Cisco MGC node, allowing you to monitor the health and performance of the network. You can display the performance information. You can also view performance data associated with a given object and graph that data over time. CMNM collects performance information from all of the components of the Cisco MGC node. You can configure the objects being polled and the frequency of the polling.

Cisco MGC allows you to specify how long performance data should be kept in the database. You can also specify rollup-rules and other actions that should be taken on performance data after a set length of time.

The Performance Manager is opened from the Network Maps, Event Browser, or Object Manager by selecting **Performance Manager** from the pop-up menu available on a selected object. A screen similar to Figure 7-1 is displayed.

*Figure 7-1 Performance Manager Screen*



A selected object or group of objects has a number of different attributes. You can choose to monitor an area of the network, for example, the performance statistics of a particular attribute. This information could then be used to evaluate the performance of specific equipment and assess the requirements for upgrades or software downloads.

Performance statistics also provide a summary view of the performance of network elements. These statistics help you determine the degree to which the network is meeting assigned service levels. You are able to drive down to the chassis level from the network level in a simple manner if you want to view individual chassis statistics.

CMNM Performance Manager can present data in two ways:

- **Raw**—This is performance data in its most detailed format (not summarized). History storage criteria defines which attributes are to be monitored on specified objects. When these objects are polled, the retrieved data is stored by CEMF and can be viewed using the Performance Manager. This data is raw data. History storage criteria may also specify summary intervals and rules to be applied to the raw data. The resultant data is summarized data.
- **Summarized**—This gives derived summaries of raw data. This is an approach which displays the data at a level appropriate to the task in hand; for example, you may decide to view data summarized in hourly or daily intervals according to requirements.

Performance data has the potential to overwhelm. For example, you may wish to view the Errored Packets for a device over a six-month interval. If the data was displayed in a table or graph at the rate at which it was sampled, this could be tens of thousands of values. In these circumstances, it is preferable to view summaries of the data. For example, if data was originally received at intervals of 5 minutes, the



ability to view it summarized in hourly, daily, or weekly intervals would be an excellent way of managing the network. History storage criteria can be used to specify these summary intervals and the rules which are used to generate the summaries for the history storage criteria's objects and attributes.

Hourly summaries are generated on the hour, daily summaries are generated at midnight, and weekly summaries are generated at midnight on Sundays (that is, the end of Sundays). For example, if polling starts at 9:30 and hourly summaries are to be generated, the first full hour's worth of data is between 10:00 and 11:00. So at 11:00, the first hourly summary is generated, and given a timestamp of 10:00. The same pattern is followed for all summaries (daily, weekly, or user-defined). This pattern standardizes summary intervals so that all attributes' summaries have the same timestamps.

**Note**

---

Data generated between 9:30 and 10:00 is ignored in the above example, because an hourly summary for 9:00 to 10:00 would be misleading as it would have been generated using only half the usual number of values.

---

In some cases, an object may fail to be polled; for example, if communication to the object is lost. This is referred to as a missed poll, and all missed polls are indicated on Performance Manager graphs and charts.

Performance Manager graphs and charts also indicate when an attribute started and stopped being polled due to history storage criteria being added, edited, or removed. You are therefore able to see when polling on an attribute started, the attribute's values while it was being polled (and any missed polls), and finally when the attribute stopped being polled.

A Performance Manager can be opened for each network element you wish to monitor. To view up-to-date information on the Performance Manager, click **Refresh** and the selected data is displayed.

## How Performance Data Is Collected

Depending on the type of device, performance data is collected in different ways.

- Performance data for the active Cisco MGC host is collected by retrieving flat files at user-defined intervals.
- CMNM collects performance data from the Cisco SLT and LAN switch using the standard SNMP mechanisms.

## Performance Data Collected for the Active Cisco MGC Host

Collection of performance data from the active Cisco MGC host is different from the other Cisco MGC node devices. CMNM does not use SNMP to collect this data. Rather, the Cisco MGC host software writes out performance data files at a predefined time interval. The actual data written out is defined by you in the Cisco MGC host configuration file `measCats.dat`.

Periodically CMNM transfers (using FTP) these performance files from the active Cisco MGC host, parses them, and loads the performance data directly into the CEMF database. Note that no data is ever collected from a Cisco MGC host in standby mode.

**Figure 7-2 Cisco MGC Host Performance Collection**

CMNM does not predefine which performance statistics are collected from the Cisco MGC host. You must configure the Cisco MGC host software to collect performance data, and CMNM simply processes whatever data is available.

CMNM always polls the active Cisco MGC host for performance data. In the event of a failover, CMNM automatically starts polling the new active Cisco MGC host (that is, the former standby host). All existing performance data is maintained.

CMNM collects only the performance measurement data that the Cisco MGC host generates. However, CMNM provides the ability to filter out specific performance measurements. This is accomplished by editing the Cisco MGC host performance filter file located in *install directory/config/hostController/perfMeasFilters*.

This file contains a list of collected Cisco MGC host measurements and allows for the filtering of these measurements by both measurement name and component name. Individual measurements can be turned off by commenting out the measurement line (with #) or by simply removing the measurement line.

This file is first read at CMNM startup and upon receipt of configuration change traps from the Cisco MGC host.

## Common Performance Data Collected for the Cisco SLT and LAN Switch

The performance counters collected for each Cisco SLT and LAN switch are described in Table 7-1.

**Table 7-1 Cisco SLT and LAN Switch Performance Counters**

| Counter                | Description                                             |
|------------------------|---------------------------------------------------------|
| RFC1213-MIB.tcpMaxConn | Total number of TCP connections the entity can support. |

Table 7-1 Cisco SLT and LAN Switch Performance Counters

|                             |                                                                                                                                                                                                                                                             |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RFC1213-MIB.tcpActiveOpens  | Number of times TCP <sup>1</sup> connections have made a direct transition to the SYN-SENT state from the CLOSED state.                                                                                                                                     |
| RFC1213-MIB.tcpPassiveOpens | Number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.                                                                                                                                                  |
| RFC1213-MIB.tcpAttemptFails | Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state. |
| RFC1213-MIB.tcpEstabResets  | Number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.                                                                                                                |
| RFC1213-MIB.tcpCurrEstab    | Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.                                                                                                                                                                  |
| RFC1213-MIB.tcpInSegs       | Total number of segments received, including those received in error.                                                                                                                                                                                       |
| RFC1213-MIB.tcpOutSegs      | Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.                                                                                                                             |
| RFC1213-MIB.tcpRetransSegs  | Total number of segments retransmitted—that is, the number of TCP segments transmitted containing one or more previously transmitted octets.                                                                                                                |
| RFC1213-MIB.tcpInErrs       | Total number of segments received in error (for example, bad TCP checksums).                                                                                                                                                                                |
| RFC1213-MIB.tcpOutRsts      | Number of TCP segments sent containing the RST flag.                                                                                                                                                                                                        |
| RFC1213-MIB.udpInDatagrams  | Total number of UDP <sup>2</sup> datagrams delivered to UDP users.                                                                                                                                                                                          |
| RFC1213-MIB.udpNoPorts      | Total number of received UDP datagrams for which there was no application at the destination port.                                                                                                                                                          |
| RFC1213-MIB.udpInErrors     | Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.                                                                                                                     |
| RFC1213-MIB.udpOutDatagrams | Total number of UDP datagrams sent from this entity.                                                                                                                                                                                                        |

1. Transmission Control Protocol

2. User Datagram Protocol

## Performance Data Collected for the Cisco SLT Network Interfaces

The performance counters collected for each network interface on the Cisco SLT are described in Table 7-2.

**Table 7-2 Cisco SLT Ethernet and TDM Interface Performance Counters**

| Counter            | Description                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------|
| IF-MIB.ifInErrors  | Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. |
| IF-MIB.ifInOctets  | Total number of octets received on the interface, including framing characters.                                    |
| IF-MIB.ifOutErrors | Number of outbound packets that could not be transmitted because of errors.                                        |
| IF-MIB.ifOutOctets | Total number of octets transmitted out of the interface, including framing characters.                             |

The counters described in Table 7-3 are collected for each TDM interface to the SS7 network.

**Table 7-3 Cisco SLT TDM Interface Performance Counters**

| Counter                     | Description                                                                                |
|-----------------------------|--------------------------------------------------------------------------------------------|
| RFC1406-MIB.dsx1CurrentESs  | Number of errored seconds encountered by a DS1 interface in the current interval.          |
| RFC1406-MIB.dsx1CurrentSEsS | Number of severely errored seconds encountered by a DS1 interface in the current interval. |

## Performance Data Collected for the LAN Switch Network Interfaces

The performance counters collected for each network interface on the LAN switch are described in Table 7-4.

**Table 7-4 LAN Switch Interface Performance Counters**

| Counter            | Description                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------|
| IF-MIB.ifInErrors  | Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. |
| IF-MIB.ifInOctets  | Total number of octets received on the interface, including framing characters.                                    |
| IF-MIB.ifOutErrors | Number of outbound packets that could not be transmitted because of errors.                                        |
| IF-MIB.ifOutOctets | Total number of octets transmitted out of the interface, including framing characters.                             |

## Opening the Performance Manager

The Performance Manager can be accessed from pop-up menus on selected objects in the following applications:

- Network Maps
- Event Browser
- Object Manager

To open Performance Manager:

- 
- Step 1** Open the appropriate window to display a relevant object.
  - Step 2** Place the cursor over the object.
  - Step 3** Press and hold the right mouse button.
  - Step 4** Move the cursor until the **Tools** option is highlighted, then highlight the **Performance Manager** option, as shown in Figure 7-3.

**Figure 7-3** *Map Viewer Screen—Tools->Performance Manager Option*



- Step 5** Release the right mouse button.  
You see the Performance Manager screen shown in Figure 7-4.
-

*Figure 7-4 Performance Manager Screen*



From the Performance Manager screen you can:

- Identify all monitored attributes on a selected managed object.
- Identify all time periods configured for sampling each monitored attribute.
- Identify all summary methods configured for selected monitored attributes and selected summary periods.
- View historical performance data over a requested period of time (in tabular or graphical format).
- Print performance data to a printer or file.

## Setting Polling Frequencies

You can set the polling frequency for the various types of devices. While you can specify a separate polling frequency for the Cisco SLTs, the LAN switches, and the Cisco MGC hosts, you cannot set a separate polling frequency for an individual device.

### Changing Collection Defaults

CMNM predefines which performance statistics are collected and simply processes whatever data is available. However, the Cisco MGC host allows you to change these defaults by editing the Cisco MGC host filter file `perfMeasFilters`. Use the following commands:

```
install directory/config/hostController
perfMeasFilters
```

Measurements can be turned on or off by commenting out the line with # or by deleting the line.

## Changing Polling Frequency

You can define the polling frequency for the various devices, but you should not set the CMNM polling frequency to be less than the Cisco MGC host polling frequency. However, you can increase the CMNM polling frequency so that not all of the Cisco MGC host performance files are processed. For example, you can set Cisco MGC host performance data collection to only once a day.

To configure the polling frequency:

- 
- Step 1 Select the site icon on the Map Viewer.
  - Step 2 Right-click to display the pull-down menu, select **Tools**, then **Open Polling Frequencies** as shown in Figure 7-5.

**Figure 7-5** Map Viewer Screen—Tools>Polling Open Polling Frequencies Option



You see the screen in Figure 7-6.

*Figure 7-6 Polling Frequencies Screen*



- Step 3** Select a polling frequency from the menu. To change from minutes to hours, select from the pull-down menu, as shown in Figure 7-7.



*Figure 7-7 Polling Frequencies Screen—Frequency Pull-down Menu*



**Step 4** To save the polling frequencies you just set, click the **Save** icon as shown in Figure 7-8.

*Figure 7-8 Save Polling Frequencies Screen*



---

## Starting Polling On a Device

By default, performance data is not collected for any object. When an object is first deployed in CEMF, it is in the normal state; no performance polling is done. To enable performance polling, you must transition the object into the polling state. This is done using the dialogs posted from the object. CMNM allows you to transition either a single object or a group of objects between the normal and polling states.










## Understanding the Different Polling States of a Device

When an object is polling, its icon is augmented with a small annotation. Each LAN switch, Cisco SLT, and common Cisco MGC host object has this icon when polling. In addition, the Cisco MGC node object has the polling icon if any of its children are doing polling. In this way, the states of the Cisco MGC subobjects are reflected up to the Cisco MGC node object.

CMNM uses many different indicators to indicate the logical state of a device. On the right side of the Map Viewer, the icon representing each device is shown. For some states, a small symbol is placed near the top of the icon to indicate a logical state. In addition, cross-hatching is used to indicate state information.

Table 7-5 shows the different logical states.

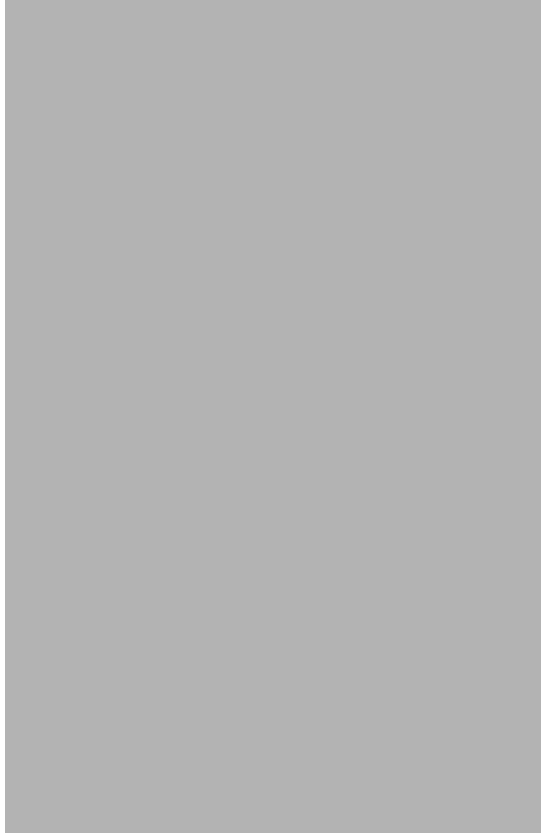
**Table 7-5 State Symbols**

| State Symbol                                                                        | Description                                                                                                                             |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
|    | Indicates that the object is in the process of discovering. The icon also has a hatch pattern.                                          |
|    | Indicates that the object is terminating or is out-of-service. Icon also has a hatch pattern.                                           |
|   | Indicates that the object is performing polling.                                                                                        |
|  | Indicates that the device is not SNMP reachable. This may be because the device is off the network or its SNMP agent is not responding. |
|  | Indicates that some major service or software process on the device has failed. The icon also has a hatch pattern.                      |
|  | Indicates that the device is off-duty or administratively down.                                                                         |
|  | Indicates that the device is providing service (active).                                                                                |
|  | Indicates that the device is running in warm standby mode (standby).                                                                    |
|  | A hatch-pattern (without any corresponding state symbol) is used to indicate that the device is not being managed (decommissioned).     |

To place a device into a polling state so that data can be collected (this example uses the Cisco SLT, but the procedure is the same for each device):

- 
- Step 1** Click the network or device, right-click to display the pull-down menu, then select **Open SLT States** as shown in Figure 7-9.

*Figure 7-9 Map Viewer Screen—Open SLT States Option*



You see the screen in Figure 7-10.

*Figure 7-10 SLT States Screen*

**Step 2** Click **Start Polling**.

You see the screen in Figure 7-11.

*Figure 7-11 Polling Configuration Prompt*

**Step 3** Click **Yes** to proceed.

To stop polling at anytime during the process, click **Stop Polling**, as shown in Figure 7-12.



**Note**

---

Starting and stopping polling on the Cisco MGX 8260, Cisco SLTs, and LAN switch also starts or stops polling for each interface on the chassis.

---

*Figure 7-12 Stop Polling Screen*



**Note**

---

When polling is taking place, a sheet with an arrow pointed up appears just above the network or object icon. Figure 7-13 shows the 2600a-Ethernet-1 and 2600a-Serial-8 in polling states.

---

*Figure 7-13 Map Viewer Screen—2600a in Polling State*



## Polling On Demand

While the active Cisco MGC host is being polled, you can also poll other devices on demand by clicking **Poll Now**.

## Action Report

An action report is presented when polling is complete, as shown in Figure 7-14.

*Figure 7-14 Action Report Screen*

## Decommissioning and Rediscovering Devices

You can commission or decommission devices such as the Cisco SLT, LAN switch, Cisco MGX 8260, BAMS, and Cisco MGC host. On the States screen, there are two buttons: one to decommission the device and the other to commission it. There is also a Rediscover button. See Figure 7-10.

Decommissioning a device prevents it from being presence polled or performance polled. A device in the decommissioned state still processes traps, but a presence poll alarm is cleared. Commissioning it brings it back on the network so that it starts presence polling.

Rediscover performs subrack discovery on the device and synchronizes all of the network interfaces and IP addresses.

## Viewing Performance Data

CMNM generates simple graphs of performance data (single counter, single object). These screens show the performance data in tabular, near real-time format for SS7, SS7 Link, SS7 Link Set, Voice Traffic, and Interface Utilization measurements. The performance counters associated with these measurements include, but are not limited to:

- Calls cancelled because of CCS congestion
- Number of transmitted IAM messages
- Received answer signaling
- Number of received IAM messages
- Number of transmitted CCS answer signals
- Number of attempts to transmit IAM messages
- Number of MSUs transmitted and received
- Duration of Level 1, 2, and 3 congestion

- Link availability

To view performance data, you need to select:

- Attributes for which performance data is to be displayed
- Time period over which the performance data is gathered
- Format to be used to display the results



**Note**

Before you can view performance data, you must first start performance monitoring on a device or network and wait until polling is complete.

**Step 1** Open the Performance Manager. The window shows the name of the selected object.

**Step 2** From the Monitored Attributes list, select the attribute to be monitored.



**Note**

You can select multiple attributes in a list by holding down the **Shift** key and selecting attributes in the list. You can select multiple individual attributes by holding down the **Ctrl** key and clicking individual items. The information for all selected attributes is shown in the Table Display. Only the first selected attribute is shown in the Line Chart or Bar Chart.

**Step 3** In the Start Date data entry boxes, enter the date the view of the performance statistics has to start from. The format is *mm/dd/yyyy*.

**Step 4** You set a start time and an end time using 24-hour notation. The times are inclusive. In the Start Time data entry boxes, enter the time the view of the performance statistics has to start on the Start Date.

**Step 5** To set the End Date you have two options:

In the End Date data entry boxes, enter the date the view of the performance statistics has to stop at. The format must be *mm/dd/yyyy* or select the **Now** check box to view the data from the selected start date to the current time. By selecting this option, you do not have to update the End Date and End Time fields.



**Note**

Now is the current time and remains current.

**Step 6** To set the End Time you have two options:

In the End Time data entry boxes, enter the time the view of the performance statistics has to stop on the End Date or select the **Now** check box to view the data from the selected start date to the current time. By selecting this option, you do not have to update the End Date and End Time fields.

**Step 7** From the Interval pull-down menu, select the summary interval to be used. This varies according to the attribute selected. The summary interval is the period of time over which the rule is applied. This pull-down menu always contains the option to select **raw**. This displays the data in raw format, which is performance data in its most detailed format (not summarized).



**Note**

When raw is selected, the Bar Chart view is not available and the Summary Rule option is grayed out.

**Step 8** From the Rule pull-down menu, select the summary rule to be used. This gives you the option to summarize data to a lower granularity as follows:

- Total—Totals all values gathered in the summary period
- Average—Takes the average of all values gathered in the summary period
- Min—Presents the lowest value received over the summary period
- Max—Presents the highest value received over the summary period
- LogicalOR—Displays either 1 or 0. This is typically used for status flags. Some attributes may have only two potential values (such as, true or false; yes or no; 1 or 0). When summaries are generated from values such as these, and the logical OR rule is used, the summarized value is 1 if any value in the summary interval is 1. If all values in the summary interval are 0, then the summarized value is 0.



**Note** The Summary Rule option is not available when the option to view raw data is selected.



**Note** The default summary rule is one day (24 hours).

**Step 9** Click **Refresh**.



**Note** The Refresh button is blue when it is available for selection. It is grayed out when not available. The Refresh button is available for selection when Now is selected, or when any criteria has changed and you have moved the cursor away from the changed value by clicking the **Tab** key or by using the mouse.



**Note** SNMP data (that is, data collected from the Cisco SLT and LAN switch) is refreshed in near real-time. When data is collected from the active Cisco MGC host, you can manually collect and display the current performance data by clicking **Refresh**. Refresh simply refreshes the Data view to display the latest data collected during polling. To update the data, you must start polling again.

By default, a line chart of the performance information, to date, is displayed. You can view performance information in the following formats:

- Line Chart, refer to Figure 7-15
- Table Display, refer to Figure 7-16

The performance information displayed corresponds to the attributes' raw values. If a summary period is selected, the information is displayed according to the Summary Rule. No summary period is associated with raw data.



**Note** In some circumstances, an object may fail to be polled. All missed polls are indicated on graphs and charts by yellow points that show the last valid value collected. A missed poll affects the summary data, and the data should not be relied upon.

CMNM graphs and charts also indicate when an attribute started and stopped being polled due to history storage criteria being added, edited, or removed. Start and end polling events are shown in charts and tables:



- The start polling events point is shown in green.
- The end polling events point is shown in red.



---

**Note** A Polling Events key is displayed.

---

**Figure 7-15** *Sample Line Chart Screen*



**Figure 7-16** *Sample Table Display Screen*



## Viewing Raw Data

You can view raw data as it is received without any summarization. History storage criteria define which attributes are to be monitored on specified objects. When these objects are polled, the retrieved data is stored by CEMF and can be viewed using the Performance Manager. This data is raw data. History storage criteria may also optionally specify summary intervals and rules to be applied to the raw data. The resultant data is summarized data.



**Note** The Summary Rule option and the Bar Chart view are not available when the option to view raw data is chosen.

- 
- Step 1** Launch the Performance Manager.
  - Step 2** Choose the desired attributes and set the dates and times, as described in the “Viewing Performance Data” section on page 7-16.
  - Step 3** From the Summary Interval pull-down menu, select **raw**.
  - Step 4** Click **Refresh**.

The new performance information displayed corresponds to the attributes value returned during the raw period.



**Note** The Refresh button is blue when it is available for selection. It is grayed out when not available. The Refresh button is available for selection when Now is selected or when any criteria has changed and you have moved the cursor away from the changed value by pressing the **Tab** key or by using the mouse.

## Viewing a Chart

You can zoom in, zoom out, and move around the displayed charts by using the keys and mouse buttons described in Table 7-6. Note that you must select a chart before invoking these actions.

**Table 7-6** Chart Viewing Actions

| Press                       | Action                                                                                                                                                    |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Shift and left mouse button | To select multiple attributes in a list.                                                                                                                  |
| Up arrow key                | Scrolls up the Table display.                                                                                                                             |
| Down arrow key              | Scrolls down the Table display.                                                                                                                           |
| Left mouse button           | Clicking and dragging with the left mouse button over an area zooms in on that section of the chart. You cannot zoom in on a chart that has a scroll bar. |
| Middle mouse button         | Takes the view back one zoom level after zooming in using the left mouse button.                                                                          |

## Viewing Points and Values on a Line Chart

You can choose to annotate a line chart with color-coded points that represent the polling status. You can also show the values associated with each point.

- 
- Step 1** From the View menu, select **Points**. This annotates the line chart with points, which visually indicate the points that are presented in tabular form in the Table Display. A point is colored-coded to show polling status as follows:
- Black—Poll
  - Red—Stopped polling
  - Green—Started polling
  - Yellow—Missed poll
- Step 2** From the View menu, select **Values**. This option shows the values associated with each point, which are presented in tabular form in the Table Display.

The values are shown on each chart until the item is deselected in the View menu.

---

## Viewing a Performance Log

Performance data is saved in a log. To view data from past pollings:

- 
- Step 1** Using the instructions in the “Viewing Performance Data” section on page 7-16, select the following to define the data you want to view:
- Start time and date
  - End time and date (select **Now** for current data)
  - Summary interval
  - Summary rule
- Step 2** Click **Refresh**.
- 

## Setting How Performance Data Is Archived

CMNM allows you to specify how long performance data should be kept in the database. You can also specify roll-up rules and other actions that should be taken on performance data after a set length of time.

CEMF manages a database of performance data values, and ensures the database does not grow indefinitely. This is achieved by purging data that is deemed to be old. Several rules are used to determine what data should be purged based on the concept of samples. A sample is either a collection of raw data, or a collection of data that has been summarized using one summary rule for one summary interval.

The attributeHistoryServer.ini file, described in Table 7-7, controls the behavior of the performance purging mechanism:

```
minValueCount = 50
maxValueCount = 1000
minRawDataAge = 60
```

**Table 7-7** *attributeHistoryServer.ini* file Attributes

| Parameter     | Description                                                                                                                                                                                                                                                                                                                                                    |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| minValueCount | Specifies the minimum number of values to be kept for each sample. Data is never removed from a sample if doing so would result in that sample having fewer than this number of values. This value is set to 50 on a standard CEMF installation.                                                                                                               |
| minRawDataAge | Specifies the minimum age of raw data (in seconds) that must be kept. Raw data younger than this age is never removed. This value is set to 60 on a standard CEMF installation. For example, if the system has just received 100 changes to an attribute in the 40 seconds preceding a purge, then the last 100 values would be kept and not just the last 50. |
| maxValueCount | Specifies the maximum number of values to be kept for each sample. Whenever this number of values is reached for a sample, values are removed until either of the first two settings would be breached if any more were removed. This value is set to 1000 on a standard CEMF installation.                                                                    |

In some cases, these three settings may conflict with history-storage-criteria summary intervals. For example, if the history storage criteria specifies that only daily summaries are to be generated, but the purging criteria specify that one full day's worth of raw data is never available, then the daily summaries could not be generated if the purge settings were followed. In such cases, data is not purged until summaries that depend on that data have been generated.

These values can be modified using the historyAdmin utility. However these values have a significant effect on database size and performance. As such, care must be taken when changing these parameters, because the settings have a direct association with overall disk requirements.



**Note**

For information on configuring how alarms are stored and deleted, see the "Setting How Long Alarms Are Stored" section on page 8-41.

## Printing a Performance File

You can print performance statistics from the Performance Manager, either as a chart or as a table. A chart prints out the information that can be seen in the window. A table prints out all of the performance statistics in a plain text format.

The output is printed by the default printer setup on your network.

- 
- Step 1** Open the Performance Manager and select the desired performance statistics.
- Step 2** From the **File** menu, select **Print**. Choose either **As Chart** or **As Table**.
-



## Managing Traps and Events

---

### Introduction to Fault Management

One of the most important aspects of network management is the ability to identify events on the system and to take action to resolve them quickly and efficiently. For example, there may be a power supply fault in a chassis that would require an engineer to be sent out to rectify the fault. This fault is critical to the running of the network and would need prompt attention.

In CMNM, when a condition (fault) occurs on a managed object in the network, the system is notified immediately. This notification is shown as an event or alarm and can be viewed with the CEMF Event Browser. The Event Browser is opened from the CEMF Launchpad. A screen similar to Figure 8-1 is displayed.

*Figure 8-1 Event Browser Screen*



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 that faults can be attended to from the screen that shows the event.



**Note**

---

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

---

You can have more than one Event Browser session open at any one time. Each Event Browser session can have different queries specified. All users can see any event. In the Event Browser window, you can acknowledge that a particular event is one that you are going to deal with, and all other users then see that the event is being handled. When the event is cleared, it is shown in the Event Browser window, so other users know that the event requires no further attention.

When an event is received, it is shown as active and unacknowledged (the two indicators are shown as grey). At this stage, no one has taken responsibility to deal with it. You may not want to view all events on the system, so a query can be set up using the CEMF Query Editor to view specific events.

# How CEMF Models Events

A CEMF event represents a notification from a managed entity that a certain condition has just occurred. These events usually represent error conditions on managed elements.

Each event is associated with the object for which it provides notification. Therefore, an object can have a number of events related to itself at any one time.

## Event Information

The default information stored against all CEMF events includes:

- The object on which the event was raised
- The time the event was raised
- The severity of the event
- A description of the event
- The state of the event.

Descriptions of event state and severity are given below.

## Event State

The event state indicates whether the event is acknowledged or unacknowledged and active or cleared.

When a new event is received by the system, its state is active/unacknowledged. You may acknowledge the event, which indicates to other users that the event is being handled. Once the event has been dealt with, you may clear the event. When you cannot clear an event due to an existing problem, it can be returned to the unacknowledged state and subsequently acknowledged or cleared by another user.

When an event is in the unacknowledged or acknowledged state, it is counted as being active, and therefore, it is still affecting the state of the object upon which it was raised.

**Figure 8-2** *State Diagram for Events*



After events are cleared, they continue to be stored within the system for a configurable amount of time to maintain an event history for an element. These events can be viewed and manipulated in the same way as any other event.

## Colors used to Indicate Severity

Each event has a severity, indicating the importance of the event, and is identified with a corresponding color as shown in Table 8-1.

**Table 8-1** Colors Used to Indicate Severity

|  | Color  | Severity of Event |
|--|--------|-------------------|
|  | Red    | Critical          |
|  | Orange | Major             |
|  | Yellow | Minor             |
|  | Cyan   | Warning           |
|  | Green  | Normal            |
|  | White  | Informational     |

## Source Domain

The source domain identifies where an event was generated. In CEMF, the source domain can be one of the following:

- SNMP—Event was generated by the managed network
- Internal—Event is generally generated by CEMF

## Management Domain

This is the management domain of SNMP trap information. The SNMP MIB specific information typically defines the equipment type generating a trap.

## Event Propagation

In order to make the identification of potential problems easy, CEMF propagates the alarm state of objects upwards through each object view.

In real terms, this means that if an object receives an event, then not only does it change color to reflect its new state, but all parent objects within a view, also change color, to reflect the most severe alarm on any of the children. The example in the following diagram shows a typical physical view of the network. The line cards are contained within the chassis, the chassis within a bay, the bay within a site, and so on.

If a minor alarm was received on Port B, then it, and all of the objects up to the region, turn yellow to indicate a potential minor problem, as illustrated in Figure 8-3.



**Figure 8-3 Example Minor Event Propagation**



If a critical alarm was then received on Port A, then it, and all of the objects up to the region, turn red to indicate a potential critical problem, as illustrated in Figure 8-4.

**Figure 8-4 Example Critical Event Propagation**



If the critical alarm is then cleared, the icons return to yellow.

## How CMNM Manages Faults

CMNM provides fault management of the Cisco MGC node, including the Cisco MGC host, the Cisco SLT, and the LAN switch. Traps generated by these elements are displayed within the CEMF system. When an alarm is received for an object, a pop-up balloon on Map Viewer shows the number and severity of the alarms for that object. The balloon color indicates the severity of the most severe alarms. The fault management features of the Cisco MGC allow you to view, acknowledge, and clear alarms for a given object.

CMNM handles numerous connectivity traps. CMNM defines the necessary trap mappings and containment trees, allowing CMNM to delegate all traps relating to the connectivity network to the nodes that represent it. You can display these alarms in the Event Browser.

When the Cisco MGC host detects a problem with one of its logical connections, it generates a trap. CMNM receives these traps and maps them to the object that represents that logical connection. For example, if CMNM receives a trap that the link to a media gateway is down, CMNM maps that trap to the object that represents the media gateway link and displays an alarm icon on the Map Viewer.

CMNM maps the incoming traps to alarms. However, not all traps are mapped to alarms. CMNM filters out duplicate traps from a network element. It also filters out traps from network elements that report a problem, and then reports within a few seconds (up to 6) when the problem is resolved. That is, the Cisco MGC automatically clears existing alarms when a network element reports that an alarm condition is no longer present. This reduces the number of unnecessary alarms displayed in the Event Browser. You cannot configure when an alarm should be automatically cleared.

## Presence Polling

CMNM periodically polls each managed object (the Cisco MGC host, Cisco SLT, Cisco MGX 8260, LAN switch, and BAMS) to ensure that the device is still reachable using SNMP. If the device is not reachable, it is indicated by annotation on the map display and an alarm is generated. In addition the object is placed into the CEMF errored state.

After the object loses connectivity, CEMF continues to poll the object until it can be reached. Once connectivity is re-established, the alarm is cleared and the annotation on Map Viewer is removed. In addition the object is returned to the CEMF normal state.

CMNM also displays the status of the Cisco MGC host connectivity network. This includes the logical connections from the active Cisco MGC host to the:

- Interfaces (Ethernet, TDM)
- STPs
- Point codes (SS7 Routes)
- Remote MGCs
- TCAP nodes
- Cisco Media Gateways

The logical connections from the active Cisco MGC host are shown as subnodes under the common Cisco MGC host object. If the standby Cisco MGC host is not processing calls, only the network connectivity of the active Cisco MGC host is shown.

## How Traps Are Managed for Network Devices

The following sections outline the southbound traps that are handled from the network elements. CMNM does not handle every possible trap that can be generated from each of the network elements, only those traps that are used for management of the devices.

### Cisco SLT Traps

*Table 8-2 Cisco SLT Traps*

| Trap      | MIB        |
|-----------|------------|
| coldStart | SNMPv2-MIB |
| warmStart | SNMPv2-MIB |
| linkUp    | IF-MIB     |

**Table 8-2 Cisco SLT Traps**

|                       |                            |
|-----------------------|----------------------------|
| linkDown              | IF-MIB                     |
| authenticationFailure | SNMPv2-MIB                 |
| syslogAlarm           | CISCO-SYSLOG-MIB           |
| configChange          | CISCO-CONFIG-MAN-MIB-V1SMI |

## LAN Switch 5500 Traps

**Table 8-3 LAN Switch Traps**

| Trap                  | MIB                        |
|-----------------------|----------------------------|
| coldStart             | SNMPv2-MIB                 |
| warmStart             | SNMPv2-MIB                 |
| linkUp                | IF-MIB                     |
| linkDown              | IF-MIB                     |
| authenticationFailure | SNMPv2-MIB                 |
| configChange          | CISCO-CONFIG-MAN-MIB-V1SMI |
| switchModuleUp        | CISCO-STACK-MIB            |
| switchModuleDown      | CISCO-STACK-MIB            |

## Catalyst 2900XL Traps

**Table 8-4 2900XL Traps**

| Trap                  | MIB              |
|-----------------------|------------------|
| coldStart             | SNMPv2-MIB       |
| warmStart             | SNMPv2-MIB       |
| linkUp                | IF-MIB           |
| linkDown              | IF-MIB           |
| authenticationFailure | SNMPv2-MIB       |
| syslogAlarm           | CISCO-SYSLOG-MIB |
| configChange          | CISCO-STACK-MIB  |

## Catalyst 2900 Traps

*Table 8-5 2900 Traps*

| Trap                  | MIB             |
|-----------------------|-----------------|
| coldStart             | SNMPv2-MIB      |
| warmStart             | SNMPv2-MIB      |
| linkUp                | IF-MIB          |
| linkDown              | IF-MIB          |
| authenticationFailure | SNMPv2-MIB      |
| authenticationFailure | SNMPv2-MIB      |
| configChange          | CISCO-STACK-MIB |
| switchModuleUp        | CISCO-STACK-MIB |
| switchModuleDown      | CISCO-STACK-MIB |

## Cisco MGC Host Traps

CMNM handles the traps in Table 8-6 from the Cisco MGC hosts.

*Table 8-6 Cisco MGC Host Traps*

| Trap             | MIB                 |
|------------------|---------------------|
| qualityOfService | CISCO-TRANSPATH-MIB |
| processingError  | CISCO-TRANSPATH-MIB |
| equipmentError   | CISCO-TRANSPATH-MIB |
| environmentError | CISCO-TRANSPATH-MIB |
| commAlarm        | CISCO-TRANSPATH-MIB |

## Cisco MGX 8260 Traps

*Table 8-7 Cisco MGX 8260 Traps*

| Trap                  | MIB          |
|-----------------------|--------------|
| coldStart             | SNMPv2-MIB   |
| warmStart             | SNMPv2-MIB   |
| linkUp                | IF-MIB       |
| linkDown              | IF-MIB       |
| authenticationFailure | SNMPv2-MIB   |
| shelfMajorAlarm       | mms1600_trap |
| shelfMinorAlarm       | mms1600_trap |
| shelfAlarmClear       | mms1600_trap |

*Table 8-7 Cisco MGX 8260 Traps*

| Trap                 | MIB          |
|----------------------|--------------|
| shelfSecurityAlert   | mms1600_trap |
| shelfColdStart       | mms1600_trap |
| shelfHistoryChg      | mms1600_trap |
| cardInserted         | mms1600_trap |
| cardRemoved          | mms1600_trap |
| cardFailed           | mms1600_trap |
| cardCoreSwitched     | mms1600_trap |
| cardServiceSwitched  | mms1600_trap |
| cardMajorAlarm       | mms1600_trap |
| cardMinorAlarm       | mms1600_trap |
| cardAlarmCleared     | mms1600_trap |
| cardActive           | mms1600_trap |
| cardCoreRedFailed    | mms1600_trap |
| cardSmRedFailed      | mms1600_trap |
| cardMsmMajorAlarm    | mms1600_trap |
| cardMismatched       | mms1600_trap |
| cardCfgCleared       | mms1600_trap |
| cardInStdbby         | mms1600_trap |
| cardBackInserted     | mms1600_trap |
| cardBackRemoved      | mms1600_trap |
| dsx1LineAdded        | mms1600_trap |
| dsx1LineDeleted      | mms1600_trap |
| dsx1LineModified     | mms1600_trap |
| dsx1MajorAlarm       | mms1600_trap |
| dsx1MinorAlarm       | mms1600_trap |
| dsx1AlarmClear       | mms1600_trap |
| dsx1PerfMajorAlarm   | mms1600_trap |
| dsx1PerfMinorAlarm   | mms1600_trap |
| dsx1PerfAlarmCleared | mms1600_trap |
| dsx1UpdateThreshold  | mms1600_trap |
| dsx1PayloadLoopup    | mms1600_trap |
| dsx1LineLoopup       | mms1600_trap |
| dsx1OtherLoopup      | mms1600_trap |
| dsx1LineLoopDown     | mms1600_trap |
| dsx1LineBertOn       | mms1600_trap |
| dsx1LineBertOff      | mms1600_trap |

Table 8-7 Cisco MGX 8260 Traps

| Trap                  | MIB          |
|-----------------------|--------------|
| dsx3LineAdded         | mms1600_trap |
| dsx3LineDeleted       | mms1600_trap |
| dsx3LineModified      | mms1600_trap |
| dsx3MajorAlarm        | mms1600_trap |
| dsx3MinorAlarm        | mms1600_trap |
| dsx3AlarmClear        | mms1600_trap |
| dsx3PerfMajorAlarm    | mms1600_trap |
| dsx3PerfMinorAlarm    | mms1600_trap |
| dsx3PerfAlarmCleared  | mms1600_trap |
| dsx3UpdateThreshold   | mms1600_trap |
| dsx3PayloadLoopup     | mms1600_trap |
| dsx3LineLoopup        | mms1600_trap |
| dsx3OtherLoopup       | mms1600_trap |
| dsx3LineLoopDown      | mms1600_trap |
| etherLineAdded        | mms1600_trap |
| etherLinedeleted      | mms1600_trap |
| etherLineConfigChange | mms1600_trap |
| etherLineActive       | mms1600_trap |
| etherLineInActive     | mms1600_trap |
| etherLineFailed       | mms1600_trap |
| etherLineAlarmCleared | mms1600_trap |
| voicePortAdded        | mms1600_trap |
| voicePortDeleted      | mms1600_trap |
| voicePortDeleted      | mms1600_trap |
| voicePortModified     | mms1600_trap |
| emmMajorAlarm         | mms1600_trap |
| emmMinorAlarm         | mms1600_trap |
| emmAlarmClear         | mms1600_trap |
| clockMajorAlarm       | mms1600_trap |
| clockMinorAlarm       | mms1600_trap |
| clockAlarmCleared     | mms1600_trap |
| clockSwitched         | mms1600_trap |
| dmcM13MapAdded        | mms1600_trap |
| dmcM13MapDeleted      | mms1600_trap |
| dmcM13MapModified     | mms1600_trap |

Table 8-7 Cisco MGX 8260 Traps

| Trap          | MIB          |
|---------------|--------------|
| dspMinorAlarm | mms1600_trap |
| dspMajorAlarm | mms1600_trap |

## Trap Receipt Not Guaranteed

CMNM does not provide any guarantee that it received a trap from the southbound systems or network elements. CMNM does not perform any negotiation with the network elements to detect or recover lost traps. However, you can perform presence polling to display trap data that may have been lost.

## Forwarding Traps to Other Systems

CMNM provides forwarding of traps generated by each component of the Cisco MGC node (the Cisco MGC host, Ciso SLT, and LAN switch) to northbound systems.



### Note

If you plan to configure CMNM to forward traps to northbound systems, you should only configure SNMP Version 1 traps on network devices. CMNM only forwards SNMP Version 1 traps to northbound systems. For more information on configuring SNMP on network devices, see Chapter 3, “Configuring Network Devices for Management.”

Traps are forwarded to the northbound systems using standard SNMP transport. To receive traps, northbound systems must register with CMNM. If the northbound system wants to receive standard SNMP traps, you must manually enter the IP address of the northbound system in CMNM. CMNM either provides a dialog where this information is entered or you must deploy an object that represents the northbound system.

To forward traps to another system:

- 
- Step 1** Select the site icon on the Map Viewer.
  - Step 2** Right-click to display the pull-down menu, select **Tools**, then **Open Trap Forwarding**.  
You see the screen in Figure 8-5.

*Figure 8-5 Trap Forwarding Screen*



- Step 3** Next to Trap Forwarding Address:, enter the IP address to which you want to forward traps and click **Add**.

You see the screen in Figure 8-6.

*Figure 8-6 Action Report Screen*



- Step 4** Click **Close**, then close the Trap Forwarding screen shown in Figure 8-5.
- Step 5** Select the site icon on the Map Viewer, right-click to display the pull-down menu, select **Tools**, then **Open Trap Forwarding**.
- You see the Trap Forwarding screen shown in Figure 8-5 with the IP address you specified added to the left pane.






---

**Note** To remove an IP address, from the Trap Forwarding screen select the IP address, select **Actions**, then **Remove**. You see a screen confirming your action. Click **OK**.

---

## Opening the Event Browser

The Event Browser application is launched using the  icon in the CEMF Launchpad screen. The Query Editor window is displayed.

Set your query (the Event Browser displays events that match the query criteria). For more information, see the “Filtering Events Using Queries” section on page 8-15.

From the pop-up menu available when you right-click one or more objects in the Map Viewer (the Event Browser displays only the events associated with the selected objects), or from other CEMF applications, select the **Event Browser** option.

## Overview of the Event Browser Screen

The main panel in the Event Browser window, shown in Figure 8-7, displays a list of events including:

- Object name (the managed device’s name)
- Time the event was raised
- Severity of the event (color-coded)
- 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 **Ack** to indicate to other users that the fault is being worked on. The button changes to the color of the severity, in this case, red. If for any reason you cannot clear the problem, this button can be deselected so the event can be reassigned. Click **Clear** when the fault has been rectified to indicate that the event requires no further attention.



---

**Note** The option to unacknowledge an event is available only to an administrator or to the user who acknowledged the event initially.

---

*Figure 8-7 Event Browser Screen*



Menus are available that provide you options for modifying the way the information is displayed. From the Edit menu, you can:

- Set up the Event State (Clear Events, Acknowledge, or Unacknowledge Events)
- Set up queries to specify the events you want to see
- Set up sort options to present the events in the order you want

From the View menu you have the following options to manage the way events are viewed on each object:

- Use Auto or Manual Update
- Set the Color Coding
- View the Event History window
- Refresh the Event Browser window
- Display the Full Object Name
- Select Full Name Options

The Full Event Description window allows you to view the status of a selected event. For more information, refer to the “Viewing a Full Description of an Event” section on page 8-28.

Clicking an event severity, name, time, or description selects that event. One or more events can be selected; this gives the opportunity to perform bulk operations. With one or more events selected, clicking the right mouse button displays a pop-up menu that shows the common services available on those events.

The Event Browser window also displays other information in the status bar:

- Progress bar (indicates that events are being added to the display)
- Current Update status (this can be auto or manual)
- Current query
- Current sort order, for example, sort by time
- Total number of events displayed (this number is shown in blue until it is acknowledged by the user by clicking the number)




---

**Note** The Event Browser can display a maximum of 10,000 entries. If there are more events on the system, this is indicated in the status bar.

---

In the Event Browser, you can use Print to save the contents of all or part of the browser to a file or to print a paper copy.

## Filtering Events Using Queries

The Event Browser monitors all events on all devices. To work efficiently, you may want to specify the objects on the network with which you are concerned. The Event Browser gives you the option to do this through queries that can be configured to match your requirements. With queries you can choose to include or exclude devices or criteria. For example, you could choose to monitor a particular device, specify a time period, and choose to look only at events that are warnings or are critical. You define a query so that the Event Browser displays only the events that meet the criteria you defined.




---


**Note** Any changes made to the queries are not stored after exiting the Event Browser.

---

## Opening the Query Editor

To define a query, click the  icon in the CEMF Launchpad window, or

in the Event Browser, select the **Edit** menu's **Query Setup** option, or

click the Query Filter icon  from the Toolbar.

The Query Editor window, similar to Figure 8-8, is displayed. The criteria that can be used to specify a query are available on individual tabs. Values or criteria can be selected on each tab. A dark gray tab is active (On); its query is used in the Event Browser. A light gray tab is inactive (Off); its query is not used.

*Figure 8-8 Query Editor Screen*

The Query Editor is split into the following tabbed sections (see the next section, “Setting Filtering Criteria,” for more information):

- Severity
- Time
- Event Status
- Source Domain
- Mgmt Domain
- User
- Event Class
- Object Scope
- Object Class
- Object Attribute Presence
- Object Attribute Value

The Event Browser is updated with events that match the query criteria. A progress bar indicates that CEMF is querying for events and the window is being updated. The total number of events displayed is shown in blue until you acknowledge it by clicking on the number.

## Setting Filtering Criteria

To set filtering (query) criteria:

- 
- Step 1** From the Query Editor screen, click the **Severity** tab.

You see the screen in Figure 8-9.

*Figure 8-9 Query Editor Screen—Severity Tab*



- Step 2** From the Available Values list, select the desired alarm level.
- Step 3** Click the right arrows to transfer the alarm level to the Selected Value list.
- Step 4** Click the **Time** tab.  
You see the screen in Figure 8-10.

*Figure 8-10 Query Editor Screen—Time Tab*



- Step 5** Select the time range and the date range for collecting the alarms.
- Step 6** Click the **Event Status** tab.

You see the screen in Figure 8-11.

**Figure 8-11 Query Editor Screen—Event Status Tab**



**Step 7** From the Available Values list, select the events and click the right arrows to transfer them to the Selected Values list.

**Step 8** Click the **Source Domain** tab.

You see the screen in Figure 8-12.

**Figure 8-12 Query Editor Screen—Source Domain Tab**



**Step 9** From the Available Values list, select Domain values and click the right arrows to transfer the values to the Selected Values list.

**Step 10** Click the **Mgmt Domain** tab.

You see the screen in Figure 8-13.

*Figure 8-13 Query Editor Screen—Mgmt Domain Tab*



- Step 11** From the Available Values list, select management domains and click the right arrows to transfer the values to the Selected Values list.
- Step 12** Click the arrows on the right side of the tabs to scroll to additional tabs.
- Step 13** Click the **User** tab.  
You see the screen in Figure 8-14.

*Figure 8-14 Query Editor Screen—User Tab*



- Step 14** From the Available Values list, select users and click the right arrows to transfer the values to the Selected Values list.
- Step 15** Click the **Event Class** tab.  
You see the screen in Figure 8-15.

*Figure 8-15 Query Editor Screen—Event Class Tab*



- Step 16** From the Available Values list, select event classes and click the right arrows to transfer the values to the Selected Values list.
- Step 17** Click the **Object Scope** tab to display all the events of a node and all its children.  
You see the screen in Figure 8-16.

*Figure 8-16 Query Editor Screen—Object Scope Tab*



- Step 18** Click **Add Scope**.  
You see the screen in Figure 8-17.



*Figure 8-17 View Scope Selector Screen*



- Step 19** In the View Scope selector, select the node.
- Step 20** Type the number of levels to view. This can be more than needed.
- Step 21** Click the diamond to the left of Descendants and click **Apply**.
- Step 22** On the Query Editor screen, click the **Object Classes** tab.  
You see the screen in Figure 8-18.

*Figure 8-18 Query Editor Screen—Object Class Tab*



- Step 23** From the Available Values list, select the desired object classes and click the right arrows to transfer the values to the Selected Values list.
- Step 24** Click the **Object Attribute Presence** tab. Click a pull-down menu under Object Type to select a value and click a pull-down menu under Attribute Name to select a value, as shown in Figure 8-19.

*Figure 8-19 Query Editor Screen—Object Attribute Presence Tab*



- Step 25** Click the **Object Attribute Value** tab. Click a pull-down menu under Object Type to select a value, click a pull-down menu under Attribute Name to select a value, and click a pull-down menu under Attribute Value to select a value, as shown in Figure 8-20.

Figure 8-20 Query Editor Screen—Object Attribute Value Tab



**Step 26** After all values are set, click **Apply** and close the Query Editor.

You see the following message:

Save Query Changes?

**Step 27** Click **Yes**.

The Event Browser begins collecting the data using the criteria you selected and displays it in the Event Browser window.



**Note**

---

Query changes are saved for the immediate session only. When you close the Event Browser, the query criteria is reset to the default.

---

## Modifying Filtering Criteria

You can change the alarm criteria displayed in the Event Browser at any time by launching the Query Editor and changing the values.

---

**Step 1** To change the criteria, from the Edit menu on the Event Browser, select **Query Setup**, as shown in Figure 8-21.

*Figure 8-21 Event Browser—Edit>Query Setup Option*

- Step 2** Set up the query by selecting values as described in the “Setting Filtering Criteria” section on page 8-16.
- Step 3** Close the Query Setup screen. The Event Browser displays the data.

## Sorting Events

Query Editor configuration allows you to specify the events you want to see. Sorting gives you options to change the order in which you view the events that match your query criteria.

### Setting Up Sort Options

From the Edit menu, select **Sorting Options**. A pull-down menu is displayed listing the available sorting options. An indicator shows which option is selected. Selecting an option causes the Event Browser display to change to show the appropriate information. The sort option selected is shown in the status bar. You can sort by:

- Time—Shows the most recent event first
- Event Class—Allows you to sort event classes
- Event State—If the query is set up to show all states, this option shows events in the following order:
  - Unacknowledged/Active
  - Acknowledged/Active
  - Cleared/Unacknowledged
  - Cleared/Acknowledged.
- Managed Object—Sorts by the name of the managed object on the network




---

**Note** Set the option to show full name before sorting by name.

---

- Severity— If the query was set up to show all severities, this option shows events in the following order:
  - Critical
  - Major
  - Minor
  - Warning
  - Normal

- Decommission
- Informational

## Managing Events

When the Event Browser shows a sorted list of events that match the query criteria set, you can start to manage those events. This is the place to acknowledge an event, which shows that you have taken responsibility for managing that event. If you cannot continue to manage an event, it can be unacknowledged and then becomes available to other users.



**Note**

---

The option to unacknowledge an event is available only to an administrator or to the user who acknowledged the event initially.

---


When the fault has been rectified and the event requires no further attention, clear the event. It is then removed from the Event Browser.

Three methods are available for managing events:

- Two indicators (Clear and Ack) are available to the left of the object name. Select or deselect the indicator associated with an event in the Event Browser window.
- Use the Edit menu.
- Right-click a selected event to display a pop-up menu of options available on that event.

Clicking an event severity, name, time, or description selects that event. One or more events can be selected; this gives you the opportunity to perform bulk operations.

## Managing an Event from the Window

- 
- Step 1** To clear the event, select the indicator associated with the event or select the object and click the **Clear Events** icon  on the Toolbar.

This displays the Events Clearing window. Enter the reason for clearing the event, then click **Apply** to save or click **Cancel** to exit the window without saving. The indicator changes to the new color of the severity of the event.

- Step 2** Select the **Ack** indicator to Acknowledge an event. The indicator changes to the color of the severity of the event. To Unacknowledge an event, select the **Ack** indicator, which is then shown as deselected.



**Note**

---

This option is available only to the user who acknowledged the event or to a user with administrative access.

---

## Managing an Event from the Menu Bar

From the Edit menu, you can select the **Edit Event State** option. A pull-down menu is displayed, which provides options to manage the events.

- **Clear Events**—Allows you to clear the event. When you select this option, the Events Clearing window is displayed. Enter a reason then click **Apply** to save the details or click **Cancel** to exit without saving.
- **Acknowledge Events**—Allows you to acknowledge an event.
- **Acknowledge Events with comment**—Allows you to record a reason for acknowledging an event. When you select this option, the Acknowledge Events window is displayed. Enter a reason then click **Apply** to save the details or click **Cancel** to exit without saving.
- **Unacknowledge Events**—Allows you to unacknowledge an event.




**Note**

This option is available only to the user who acknowledged the event or to a user with administrative access.

## Enabling Auto or Manual Update

Auto Update is the default state and allows you to view incoming events that are automatically updated in the window.

The status box displays the current update state; either Auto or Manual. If Auto Update is enabled, the status box displays Auto Update.

When the update state is Manual (Auto Update is disabled), you should refresh the window at regular intervals using the View menu's **Refresh** option or the Refresh icon  so that new events are displayed.

To enable auto update:

- Step 1** From the View menu, select **Enable Auto Update**. The message in the status box changes to Auto Update.



**Note**

If an indicator is displayed on the pull-down menu, to the left of Enable Auto Update, the Auto Update application is enabled.

To enable manual update:

- Step 1** From the View menu, deselect **Enable Auto Update**.



**Note**

The message in the status box changes to Manual Update.

## Setting How Events Are Color-Coded

Three color-coding options are available to you. The color you choose depends on the severity of the event. The options are as follows:

- **Full Color-Coding**—When this option is selected, the severity information displayed has text on a colored background.
- **Partial Color-Coding**—When this option is selected, the Severity column is colored. The color of the column depends on the severity of the event.
- **No Color-Coding**—When this option is selected, text only is displayed in the Severity column.

## Selecting the Type of Color Coding to Be Used

- 
- Step 1** From the View menu, select **Set Color Coding**.
- Step 2** From the menu that appears, select one of the options.
- The selected option is implemented immediately.
- 

## Viewing the Event History

Event history allows you to display any events that match the current query criteria and have had their state changed, either acknowledged, cleared, or unacknowledged. This is disabled by default. To view this information, select the View menu's **Event History** option.

To view the event history:

- 
- Step 1** Configure the event query (refer to the “Filtering Events Using Queries” section on page 8-15.)  
The Event Browser displays current events that match the criteria set in the query.
- Step 2** From the View menu, select **Event History**.  
The Event Browser now displays any events that meet that query and have been cleared.



**Note** By default, cleared events are stored by the system for seven days. Therefore, only events that match the current query and have had their state changed in the last seven days, are displayed when the Event History is enabled.


---

*Figure 8-22 Event History Enabled Screen*



## Refreshing the Event Window

Ensure that Manual Update is selected; this is shown as a current status message. You can then:

- From the View menu, select **Refresh**.
- Click the Refresh icon  on the Toolbar.

The window is refreshed.



### Note

---

You should refresh the window at regular intervals to show an up-to-date list of events.

---

## Viewing a Full Description of an Event

Double-clicking an event displays the Full Event Description window. This provides details of the event with Acknowledge and Clearing details.

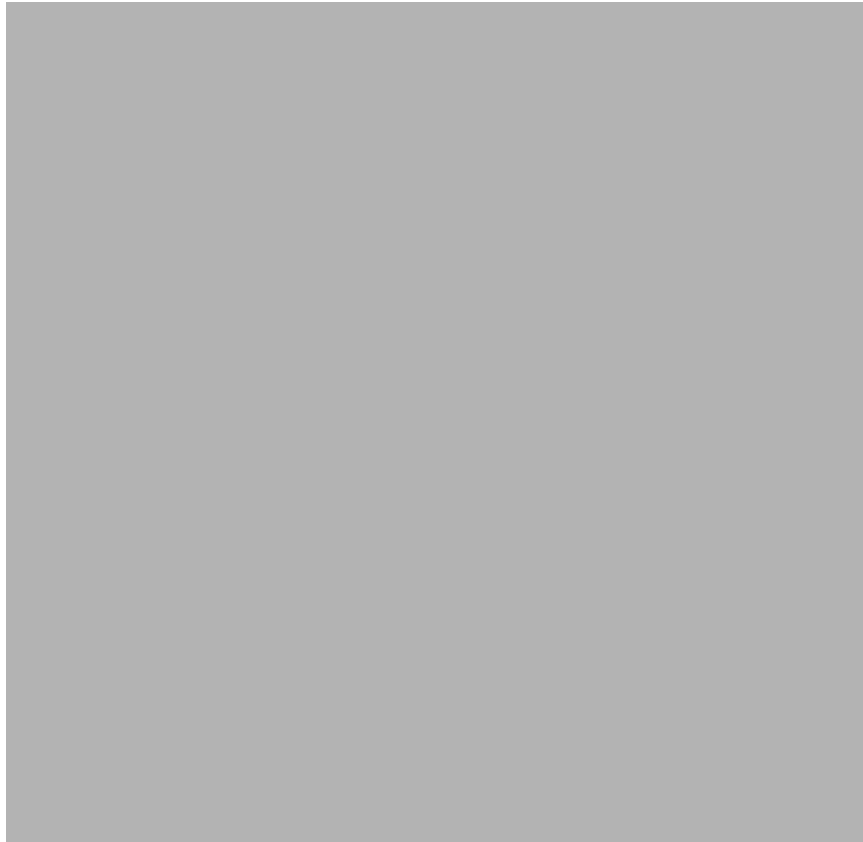
To view a full description of an event:



Place the cursor over the relevant event in the Event Browser, then double-click the left mouse button or select **Event Description**, then select **Event Information Dialog** from the pop-up menu available on a selected object.

A window similar to Figure 8-23 is displayed.

*Figure 8-23 Full Event Description Screen*



**Note**

---

If the event has not been cleared, the Event State displays Active and the Clearing Method, User Responsible for Clearing, Clearing Time and Date sections are disabled. The information displayed cannot be altered.

If an event has been cleared, you can view the method used to clear it by clicking **Clearing Event**.

---

The Full Event description window displays the following information:

- Object name—Name of the CEMF managed object the event was reported against
- Time and Date—The time and date the event was reported
- Severity—The severity of the reported event
- Source Domain—Indicates from which Communications domain the event was reported
- Management Domain—Indicates from which Management domain the event was reported
- Event Description—Provides a brief description of the reported event

- **Event State**—Indicates whether the event is active or cleared. If the event has been cleared, the **Clearing Method**, **User Responsible for Clearing**, and **Clearing Time and Date** sections become active.

## Acknowledge Details

- **Acknowledgement User**—Identifies the user who acknowledged the event
- **Acknowledgement Time and Date**—Identifies when the event was acknowledged

## Clearing Details

- **Clearing Method**—Indicates if the event was cleared by the network or by a user.
- **User Responsible for Clearing**—Displays the user name responsible for clearing the event.
- **Clearing Time and Date**—Indicates the time and date the event was cleared.
- **Reason for clearing**—The information that was entered in the Events Clearing window, which is completed when the Clear indicator is selected.

# Managing Cisco MGX 8260 Faults

You can view and manage faults on the Cisco MGX 8260 with the Web View tool. To use Web View:

- 
- Step 1** Select the Cisco MGC 8260 icon, right-click to display the pull-down menu, click **Tools**, then **Open Web Viewer**, as shown in Figure 8-24.

*Figure 8-24 Map Viewer Screen—Tools>Open Web Viewer Option*



**Step 2** When the Web Browser displays, type your user ID and password and click **Login**.

## Using the Cisco MGC Tool Bar

You can manage Cisco MGC host faults and performance from the MGC Toolbar.

---

**Step 1** Select the Cisco MGC common host, right-click to display the pull-down menu, select **Tools**, then select **Open MGC Toolbar**, as shown in Figure 8-25.

*Figure 8-25 Map Viewer Screen—Tools>Open MGC Toolbar Option*



You see the screen in Figure 8-26.

*Figure 8-26 MGC Toolbar*



From the MGC Toolbar you can click the following buttons:

- Alarm&Meas Viewer—View alarms on the Cisco MGC host.
- CDR Viewer—View call detail records (CDRs).
- CONFIG-LIB Viewer—Configure a library.
- Log Viewer—View a log file.
- Trace Viewer—View a trace file.
- Translation Verification—Verify a translation.
- File Options—View a configuration of the files.
- Close—Close the MGC Toolbar.

## Alarm and Measurements Viewer

**Step 1** On the MGC Toolbar, click **Alarm&Meas Viewer** to view alarms on the Cisco MGC host.

**Figure 8-27** MGC Toolbar—Alarm&Meas Viewer Option



You see the screen in Figure 8-28.

**Figure 8-28** Alarm&Meas Viewer Warning Screen



**Step 2** Click **Yes**.

You see the screen in Figure 8-29.

**Figure 8-29** Alarm & Measurement Viewer Screen—Meas Record View Tab



**Step 3** In the Select Component box, use the Comp Type and Complist pull-down menus to select values.

**Step 4** In the Select Category box, use the catType and measList pull-down menus to select values.

- Step 5** Select a file from the list on the right of the screen.
- Step 6** Click **Execute** to run the query.  
The results appear in the box at the bottom of the screen.
- Step 7** Click the **Alarm Record View** tab to display alarm records.  
You see the screen in Figure 8-30.

*Figure 8-30 Alarm & Measurement Viewer Screen—Alarm Record View Tab*



- Step 8** In the Select Component box, use the Comp Type and Complist pull-down menus to select values.
- Step 9** In the Select Category box, use the alarmCategory pull-down menu to select a value.
- Step 10** Select a file from the list on the right of the screen.
- Step 11** Click **Execute** to run the query.  
The results appear in the box at the bottom of the screen.
- 

## CDR Viewer

---

- Step 1** On the MGC Toolbar, click **CDR Viewer** to view CDR records.  
You see the screen in Figure 8-31.

*Figure 8-31 CDR Viewer Warning Screen*



- Step 2** Click **Yes** to proceed.  
You see the screen in Figure 8-32.

*Figure 8-32 CDR View Screen—Query Tab*



- Step 3** Select an action to perform.
- Step 4** Click the **Config** tab.  
You see the screen in Figure 8-33.

*Figure 8-33 CDR View Screen—Config Tab*



- Step 5** From the All Possible Message Types list, select the messages you want to filter and click **Transfer** to transfer them to the Selected filtering list.
- 

## CONFIG-LIB Viewer

---

- Step 1** On the MGC Toolbar, click **CONFIG-LIB Viewer** to configure a library.  
You see the screen in Figure 8-34.



*Figure 8-34 CONFIG-LIB Viewer Warning Screen*



- Step 2** Click **Yes** to continue.  
You see the screen in Figure 8-35.

*Figure 8-35 config-lib Screen*



- Step 3** Enter the number of the list item to be executed and press **Enter**.
- 

## Log Viewer

---

- Step 1** On the MGC Toolbar, click **Log Viewer** to view a log file.  
You see the screen in Figure 8-36.

*Figure 8-36 Log Viewer Warning Screen*



- Step 2** Click **Yes** to proceed.  
You see the screen in Figure 8-37.

*Figure 8-37 Log Viewer Screen*



- Step 3** Select categories and severities from the lists, then select a log file.
- Step 4** Select an action to execute.
- 

## Trace Viewer

---

- Step 1** On the MGC Toolbar, click **Trace Viewer** to view a trace file.  
You see the screen in Figure 8-38.

*Figure 8-38 Trace Viewer Warning Screen*



- Step 2** Click **Yes** to continue.  
You see the screen in Figure 8-39.

*Figure 8-39 Trace Files Screen*



- Step 3** Select a trace file to view and click **View**.
- 

## Translation Verification

---

- Step 1** On the MGC Toolbar, click **Translation Verification** to verify a translation.  
You see the screen in Figure 8-40.

*Figure 8-40 Translation Verification Warning Screen*



- Step 2** Click **Yes** to continue.  
You see the screen in Figure 8-41.

*Figure 8-41 Translation Verification Screen—DialPlan Translation Tab*



- Step 3 Type a four-digit dial plan number in the field provided.
  - Step 4 Click **Execute** to finish.
  - Step 5 Click **SaveInFile** to save the data in a file for later viewing.
  - Step 6 Click the **Config** tab to display related environmental variables.
  - Step 7 You see the screen in Figure 8-42.
- 

*Figure 8-42 Translation Verification Screen—Config Tab*



## File Options

---

- Step 1 On the MGC Toolbar, click **File Options** to view a configuration of the files.  
You see the screen in Figure 8-43.

*Figure 8-43 File Options Screen*

Step 2 Click a file, then click an action to execute it.

---

## Setting How Long Alarms Are Stored

All alarms are automatically stored in the CEMF database. Periodically CEMF purges the alarms from the database to free up room for new alarms.

The alarmDeleter utility controls the deletion of alarms. CEMF does not do any archiving of old alarms, but it can be configured to delete alarms of a specific age and state. Upon installation a cron job is set up to run the Alarm Deleter at midnight every night. At this time, the Deleter queries the alarm database, deleting alarms that meet the specified criteria. The alarmDelete.ini file, shown below, allows you to define these rules. The default is to delete cleared alarms that are seven days old.

```
[logger]
#include "loggercommon.include"
loggingName = alarmDeleter

[AlarmDeleter]
databaseName      = [[OSDBROOT]]/alarm.db
segmentDeletionInterval = 15
ageOfAlarmsInDays= 7
ageOfAlarmsInHours= 0
ageOfAlarmsInMinutes    = 0
deleteAllAlarms= 0

[Database]
#include "databaseCommon.include"
```

The variables used in defining the deletion rules are described in Table 8-8.

**Table 8-8 Alarm Deleter Attributes**

| Variable             | Description                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------------------|
| ageOfAlarmsInDays    | The age of the alarm, in days, before it is to be deleted.                                                         |
| ageOfAlarmsInHours   | The age of the alarm, in hours, before it is to be deleted.                                                        |
| ageOfAlarmsInMinutes | The age of the alarm, in minutes, before it is to be deleted.                                                      |
| deleteAllAlarms      | 0 = delete only cleared alarms that match criteria; 1 = delete both active and cleared alarms that match criteria. |



# Viewing Information About Network Devices

---

## Introduction

You can view the following information about network devices:

- Cisco MGC host accounts
- Cisco MGC host properties
- Cisco SLT accounts
- Cisco SLT properties
- LAN switch accounts
- LAN switch properties
- BAMS accounts
- BAMS properties
- Ethernet interface properties
- TDM interface properties
- Serial interface properties

## Viewing Accounts and Properties

For detailed information, you can view accounts and properties from the Map Viewer by clicking **View** on the CEMF Launchpad.

For a cross-reference of field names to attributes, see the “” section on page 9-28.



### Tips

---

For a description of each field name, slowly pass the cursor across the field name. A description of the field is displayed, as shown in Figure 9-1.

---

*Figure 9-1 Context Help*

## Viewing Cisco MGC Host Accounts

To view Cisco MGC host accounts:

- 
- Step 1 From the Map Viewer, select the MGC Host.
  - Step 2 Right-click to display the pull-down menu, then select **Open MGC Host Accounts**.  
You see the screen in Figure 9-2 with the account information for the selected Cisco MGC host.

*Figure 9-2 MGC Host Accounts Screen*

The status of the host system is displayed along with the account information for the selected host.

**Note**

If the account is locked (the lock icon is closed), you do not have permission to view this information.

---



## Viewing Cisco MGC Host Properties

To view Cisco MGC host properties:

- 
- Step 1** From the Map Viewer, select the MGC Host.
  - Step 2** Right-click to display the pull-down menu, then select **Open MGC Host Properties**.

You see the screen in Figure 9-3 with the properties of the Cisco MGC host displayed on the General tab.

*Figure 9-3 MGC Properties Screen—General Tab*



- Step 3** Click the **Host** tab to view the host configuration.  
You see the screen in Figure 9-4.

*Figure 9-4 MGC Properties Screen—Host Tab*



- Step 4** Click the **Network** tab to view the host and peer network addresses.  
You see the screen in Figure 9-5.

*Figure 9-5 MGC Properties Screen—Network IP Addresses Tab*



- Step 5** Click the **UNIX** tab to view the properties of the UNIX system.  
You see the screen in Figure 9-6.

Figure 9-6 MGC Properties Screen—UNIX Tab



## Viewing Cisco SLT Accounts

To view the accounts for the Cisco SLT:

- 
- Step 1** From the Map Viewer, select the Cisco SLT.
  - Step 2** Right-click to display the pull-down menu, then select **Open SLT Accounts**.



**Tips**

---

For a description of each field name, slowly pass the cursor across the field name. A description of the field is displayed, as shown in Figure 9-1.

---

You see the screen in Figure 9-7 with the account information for the selected Cisco SLT.

*Figure 9-7 SLT Accounts Screen*



## Viewing Cisco SLT Properties

To view the properties for the Cisco SLT:

- 
- Step 1** From the Map Viewer, select the Cisco SLT.
  - Step 2** Right-click to display the pull-down menu, then select **Open SLT Properties**.



**Tips**

---

For a description of each field name, slowly pass the cursor across the field name. A description of the field is displayed, as shown in Figure 9-1.

---

You see the screen in Figure 9-8 with the properties of the Cisco SLT displayed on the General tab.

*Figure 9-8 SLT Properties Screen—General Tab*



- Step 3** Click the **Details** tab to view the Transmission Control Protocol (TCP) connection states of the Cisco SLT and the transmission errors generated by the Cisco SLT.  
You see the screen in Figure 9-9.

*Figure 9-9 SLT Properties Screen—Details Tab*



- Step 4** Click the **Transmission** tab to view the TCP/UDP transmission statistics.  
You see the screen in Figure 9-10.

*Figure 9-10 SLT Properties Screen—Transmission Tab*



- Step 5** Click the **Memory** tab to view memory pool for the selected Cisco SLT.  
You see the screen in Figure 9-11.



Figure 9-11 SLT Properties Screen—Memory Tab



## Viewing LAN Switch Accounts

To view LAN switch accounts:

- 
- Step 1 From the Map Viewer, select the LAN.
  - Step 2 Right-click to display the pull-down menu, then select **Open Switch Accounts**.



**Tips** For a description of each field name, slowly pass the cursor across the field name. A description of the field is displayed, as shown in Figure 9-1.

---

You see the screen in Figure 9-12.

Figure 9-12 LAN Switch Accounts Screen



Step 3 Type your ID and password parameters in the fields provided.

---

## Viewing LAN Switch Properties

To view LAN switch properties:

---

Step 1 From the Map Viewer, select the LAN.

Step 2 Right-click to display the pull-down menu, then select **Open Switch Properties**.



**Tips**

For a description of each field name, slowly pass the cursor across the field name. A discription of the field is displayed, as shown in Figure 9-1.

---

You see the screen in Figure 9-13.

*Figure 9-13 LAN Switch Properties Screen—General tab*



**Step 3** Click the **Details** tab.

You see the screen in Figure 9-14 with the TCP connection states for the LAN switch and the transmission errors generated by the LAN switch.

*Figure 9-14 LAN Switch Properties Screen—Details Tab*



**Step 4** Click the **Transmission** tab.

You see the screen in Figure 9-15 with the TCP/UDP transmission statistics displayed.

*Figure 9-15 LAN Switch Properties Screen—Transmission Tab*



- Step 5** Click the **Memory** tab.
- Step 6** Select a memory pool supported by the LAN switch.  
You see the screen in Figure 9-16 with the details for the selected memory pool displayed.

Figure 9-16 LAN Switch Properties Screen—Memory Tab



## Viewing BAMS Accounts

To view BAMS accounts:

- 
- Step 1 From the Map Viewer, select the BAMS.
  - Step 2 Right-click to display the pull-down menu, then select **Open BAM Accounts**.



### Tips

---

For a description of each field name, slowly pass the cursor across the field name. A description of the field is displayed, as shown in Figure 9-1.

---

You see the screen in Figure 9-17 with the account information displayed for the selected BAMS.

*Figure 9-17 BAM Accounts Screen*



## Viewing BAMS Properties

To view BAMS properties:

- Step 1** From the Map Viewer, select the BAMS.
- Step 2** Right-click to display the pull-down menu, then select **Open BAM Properties**.  
You see the screen in Figure 9-18 with the properties of the selected BAMS displayed.

*Figure 9-18 BAM Properties Screen*



## Viewing Ethernet Interface Properties

To view Ethernet interface properties:

- 
- Step 1** From the Map Viewer, select the Ethernet interface.
- Step 2** Right-click to display the pull-down menu, then select **Open Ethernet Properties**.



**Tips**

---

For a description of each field name, slowly pass the cursor across the field name. A description of the field is displayed, as shown in Figure 9-1.

---

You see the screen in Figure 9-19 with the properties of the selected interface displayed on the General tab.

*Figure 9-19 Ethernet Properties Screen—General Tab*



- Step 3** Click the **Details** tab to view transmission details of the selected interface.
- You see the screen in Figure 9-20.



Figure 9-20 Ethernet Properties Screen—Details Tab



## Viewing TDM Interface Properties

To view TDM interface properties:

- 
- Step 1** From the Map Viewer, select the TDM.
- Step 2** Right-click to display the pull-down menu, then select **Open TDM Properties**.  
You see the screen in Figure 9-21 with the properties of the selected interface displayed on the General tab.



**Tips**

---

For a description of each field name, slowly pass the cursor across the field name. A description of the field is displayed, as shown in Figure 9-1.

---

*Figure 9-21 TDM Properties Screen—General Tab*



- Step 3** Click the **Details** tab to view the status and configuration of the selected TDM.  
You see the screen in Figure 9-22.

*Figure 9-22 TDM Properties Screen—Details Tab*



- Step 4** Click the **Transmission** tab to view transmission details of the selected TDM.  
You see the screen in Figure 9-23.

*Figure 9-23 TDM Properties Screen—Transmission Tab*



- Step 5** Click the **Current** tab to view the data errors for the current interval on the selected TDM.  
You see the screen in Figure 9-24.

*Figure 9-24 TDM Properties Screen—Current Tab*



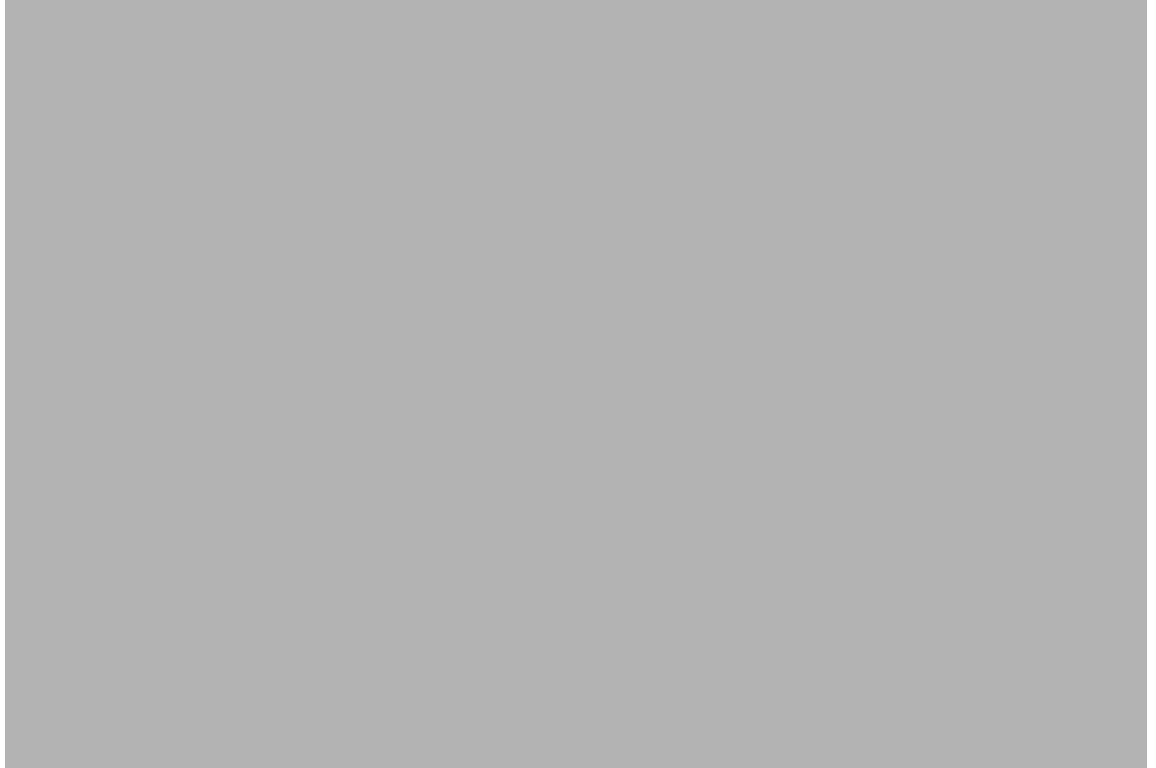
- Step 6** Click the **FarEnd Current** tab to view far end data errors for the current interval.  
You see the screen in Figure 9-25.

*Figure 9-25 TDM Properties Screen—FarEnd Current Tab*



- Step 7** Click the **Interval** tab to view data errors. You must first select the interval for the data errors. You see the screen in Figure 9-26.

*Figure 9-26 TDM Properties Screen—Interval Tab*



**Step 8** Click the **FarEnd Interval** tab to view far end data errors for the selected interval. You must first select an interval.

You see the screen in Figure 9-27.

Figure 9-27 Properties Screen—FarEnd Interface Tab



## Viewing Serial Interface Properties

To view Serial interface properties:

- 
- Step 1 From the Map Viewer, select the serial interface.
  - Step 2 Right-click to display the pull-down menu, then select **Open Serial Properties**.

You see the screen in Figure 9-28 with the properties of the selected interface displayed on the General tab.



### Tips

---

For a description of each field name, slowly pass the cursor across the field name. A description of the field is displayed, as shown in Figure 9-1.

---



*Figure 9-28 Serial Interface Properties Screen—General Tab*



**Step 3** Select the interface type from the pull-down menu as shown in Figure 9-29.

*Figure 9-29 Serial Interface Properties Screen—Interface Type Pull-down Menu*



**Step 4** Select **Admin Status**.

**Step 5** Select **Operational Status** as shown in Figure 9-30.

*Figure 9-30 Serial Interface Properties Screen—Operational Status Pull-down Menu*



**Step 6** Click the **Details** tab.

You see the screen in Figure 9-31 with the transmission details for the selected interface displayed.

*Figure 9-31 Serial Interface Properties Screen—Details Tab*



---

## Attributes for Fields in Accounts and Properties

Attributes for each field in the accounts and properties interface are listed in the following tables.

## Host Controller Attributes

*Table 9-1 hostController MIB Attributes*

| Field Name          | Attribute Name                                         | Description                                     |
|---------------------|--------------------------------------------------------|-------------------------------------------------|
| Platform State      | hostController:HostController-MIB.desiredPlatformState | Desired platform state                          |
| Hardware Model      | hostController:HostController-MIB.hardwareModel        | Sun Solaris hardware model                      |
| Host ID             | hostController:HostController-MIB.hostID               | Sun Solaris host ID                             |
| Host Name           | hostController:HostController-MIB.hostName             | Sun Solaris host name                           |
| Host Vendor         | hostController:HostController-MIB.hostVendor           | Cisco MGC host software vendor                  |
| Host Version        | hostController:HostController-MIB.hostVersion          | Cisco MGC host software version                 |
| Network Address     | hostController:HostController-MIB.ipNetworkAddr[1-4]   | Cisco MGC host network address                  |
| Peer Address        | hostController:HostController-MIB.ipPeerAddr[1-2]      | Failover peer address                           |
| Virtual Switch      | hostController:HostController-MIB.isVirtualSwitch      | True if Cisco MGC is acting as a virtual switch |
| Last Boot Time      | hostController:HostController-MIB.lastBootTime         | Time the host machine was last booted           |
| Login ID            | hostController:HostController-MIB.loginID              | Cisco MGC host login ID                         |
| OS Release          | hostController:HostController-MIB.osReleaseLevel       | Sun Solaris release level                       |
| OS Version          | hostController:HostController-MIB.osVersion            | Sun Solaris version                             |
| Host Login Password | hostController:HostController-MIB.password             | Cisco MGC host login password                   |
| Root Password       | hostController:HostController-MIB.rootPassword         | Sun Solaris root (super-user) password          |
| Transpath Directory | hostController:HostController-MIB.transpathHomeDir     | Home directory of call agent software           |

## IP Manageable Attributes

*Table 9-2 ip Manageable Attributes*

| Field Name | Attribute Name                   | Description              |
|------------|----------------------------------|--------------------------|
| IP Address | LocalDB: AMAF-MGMT-MIB.ipaddress | IP address of the device |

## SNMP Attributes

**Table 9-3** *SNMPv2-MIB.system Attributes*

| Field Name  | Attribute Name              | Description                                  |
|-------------|-----------------------------|----------------------------------------------|
| Contact     | SNMP:SNMPv2-MIB.sysContact  | Contact person for the device                |
| Description | SNMP:SNMPv2-MIB.sysDescr    | Description of the device                    |
| Location    | SNMP:SNMPv2-MIB.sysLocation | Physical location of the device              |
| Name        | SNMP:SNMPv2-MIB.sysName     | Administratively assigned name of the device |
| Up Time     | SNMP:SNMPv2-MIB.sysUpTime   | Length of the time the device has been up    |

## Interface Attributes

**Table 9-4** *IF-MIB.interfaces Attributes*

| Field Name         | Attribute Name            | Description                                                                                     |
|--------------------|---------------------------|-------------------------------------------------------------------------------------------------|
| Index              | LocalDB:IF-MIB.ifIndex    | Unique value for each interface.                                                                |
| Admin Status       | SNMP:IF-MIB.ifAdminStatus | Desired state of the interface. Values: 1 (up), 2 (down), 3 (testing)                           |
| Description        | SNMP:IF-MIB.ifDescr       | Textual string containing information about the interface.                                      |
| Errors             | SNMP:IF-MIB.ifInErrors    | Number of inbound packets containing errors preventing delivery to a higher-layer protocol.     |
| Octets             | SNMP:IF-MIB.ifInOctets    | Total number of octets received on the interface, including framing characters.                 |
| Last Change        | SNMP:IF-MIB.ifLastChange  | Value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable.     |
| Mtu                | SNMP:IF-MIB.ifMtu         | Size of the largest packet that can be sent and received on the interface, specified in octets. |
| Operational Status | SNMP:IF-MIB.ifOperStatus  | Current operational state of the interface. Values: 1 (up), 2 (down), 3 (testing)               |
| Out Errors         | SNMP:IF-MIB.ifOutErrors   | Number of outbound packets that could not be transmitted because of errors.                     |
| Out Octets         | SNMP:IF-MIB.ifOutOctets   | Total number of octets transmitted out of the interface, including framing characters.          |
| Physical Address   | SNMP:IF-MIB.ifPhysAddress | Interface's address at its protocol sublayer.                                                   |
| Speed              | SNMP:IF-MIB.ifSpeed       | Estimate of the interface's current bandwidth in bits per second.                               |
| Type               | SNMP:IF-MIB.ifType        | Type of the interface. Refer to SNMPv2-MIB for possible values.                                 |

## TCP Attributes

Table 9-5 TCP Attributes

| Field Name          | Attribute Name                   | Description                                                                                                                                                                                                                                                 |
|---------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active Opens        | SNMP:RFC1213-MIB.tcpActiveOpens  | Number of times Transmission Control Protocol (TCP) connections have made a direct transition to the SYN-SENT state from the CLOSED state.                                                                                                                  |
| Fail Attempts       | SNMP:RFC1213-MIB.tcpAttemptFails | Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state. |
| Current State       | SNMP:RFC1213-MIB.tcpCurrEstab    | Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.                                                                                                                                                                  |
| Resets              | SNMP:RFC1213-MIB.tcpEstabResets  | Number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.                                                                                                                |
| Errors              | SNMP:RFC1213-MIB.tcpInErrs       | Total number of segments received in error (for example, bad TCP checksums).                                                                                                                                                                                |
| Segments            | SNMP:RFC1213-MIB.tcpInSegs       | Total number of segments received, including those received in error.                                                                                                                                                                                       |
| Maximum Connections | SNMP:RFC1213-MIB.tcpMaxConn      | Total number of TCP connections the entity can support.                                                                                                                                                                                                     |
| RST                 | SNMP:RFC1213-MIB.tcpOutRsts      | Number of TCP segments sent containing the RST flag.                                                                                                                                                                                                        |
| Segments            | SNMP:RFC1213-MIB.tcpOutSegs      | Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.                                                                                                                             |
| Passive Opens       | SNMP:RFC1213-MIB.tcpPassiveOpens | Number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.                                                                                                                                                  |
| Retransmitted       | SNMP:RFC1213-MIB.tcpRetransSegs  | Total number of segments retransmitted; that is, the number of TCP segments transmitted containing one or more previously transmitted octets.                                                                                                               |

## UDP Attributes

Table 9-6 UDP Attributes

| Field Name          | Attribute Name                   | Description                                                                                                                             |
|---------------------|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Datagrams Delivered | SNMP:RFC1213-MIB.udpInDatagrams  | Total number of UDP datagrams delivered to UDP users.                                                                                   |
| Errors              | SNMP:RFC1213-MIB.udpInErrors     | Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port. |
| Ports               | SNMP:RFC1213-MIB.udpNoPorts      | Total number of received UDP datagrams for which there was no application at the destination port.                                      |
| Datagrams Sent      | SNMP:RFC1213-MIB.udpOutDatagrams | Total number of UDP datagrams sent from this entity.                                                                                    |

## Memory Pool Attributes

Table 9-7 ciscoMemoryPoolTable Attributes

| Field Name                | Attribute Name                                        | Description                             |
|---------------------------|-------------------------------------------------------|-----------------------------------------|
| Memory Pool Name          | SNMP:CISCO-MEMORY-POOL-MIB.ciscoMemoryPoolName        | Textual name assigned to memory pool    |
| Memory Pool Value         | SNMP:CISCO-MEMORY-POOL-MIB.ciscoMemoryPoolValid       | Indicates if memory pool is valid       |
| Bytes Used                | SNMP:CISCO-MEMORY-POOL-MIB.ciscoMemoryPoolUsed        | Number of bytes that are being used     |
| Bytes Free                | SNMP:CISCO-MEMORY-POOL-MIB.ciscoMemoryPoolFree        | Number of bytes free                    |
| Largest Number Free Bytes | SNMP:CISCO-MEMORY-POOL-MIB.ciscoMemoryPoolLargestFree | Largest number of contiguous bytes free |

## BAMS Chassis Attributes

Table 9-8 bamChassis Attributes

| Field Name     | Attribute Name                                  | Description                |
|----------------|-------------------------------------------------|----------------------------|
| Login ID       | mgcController:MgcController-MIB.bamLoginID      | Login ID                   |
| Login Password | mgcController:MgcController-MIB.bamPassword     | Login password             |
| Root Password  | mgcController:MgcController-MIB.bamRootPassword | Root (super-user) password |

## Cisco MGC TDM Attributes

Table 9-9 *mgcTDMIf Attributes*

| Field Name             | Attribute Name                              | Description                                                                                                                                                                                                                                   |
|------------------------|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Circuit Identifier     | SNMP:RFC1406-MIB.dsx1CircuitIdentifier      | Transmission vendor's circuit identifier                                                                                                                                                                                                      |
| Far End Time Elapsed   | SNMP:RFC1406-MIB.dsx1FarEndTimeElapsed      | Time elapsed from start of measurement period                                                                                                                                                                                                 |
| Time Elapsed           | SNMP:RFC1406-MIB.dsx1TimeElapsed            | Time elapsed from start of measurement period                                                                                                                                                                                                 |
| Data Link Value        | SNMP:RFC1406-MIB.dsx1Fdl                    | Use of the facilities data link. Values: 1 (other), 2 (dsx1Ansi-T1-403), 3 (dsx1Att-54016), 4 (dsx1Fdl-none)                                                                                                                                  |
| Line Coding Value      | SNMP:RFC1406-MIB.dsx1LineCoding             | Zero Coding Suppression used on the link. Values: 1 (dsx1JBZS), 2 (dsx1B8ZS), 3 (dsx1HDB3), 4 (dsx1ZBTSI), 5 (dsx1AMI), 6 (other)                                                                                                             |
| Line Status            | SNMP:RFC1406-MIB.dsx1LineStatus             | Status of the line                                                                                                                                                                                                                            |
| Line Type              | SNMP:RFC1406-MIB.dsx1LineType               | DS1 line type. Values: 1 (other), 2 (dsx1ESF), 3 (dsx1D4), 4 (dsx1E1), 5 (dsx1E1-CRC), 6 (dsx1E1-MF), 7 (dsx1E1-CRC-MF)                                                                                                                       |
| Loopback Configuration | SNMP:RFC1406-MIB.dsx1LoopbackConfig         | Loopback configuration of DS1 interface. Values: 1 (dsx1NoLoop), 2 (dsx1PayloadLoop), 3 (dsx1LineLoop), 4 (dsx1OtherLoop)                                                                                                                     |
| Send Code              | SNMP:RFC1406-MIB.dsx1SendCode               | Type of code sent across the DS1 interface. Values: 1 (dsx1SendNoCode), 2 (dsx1SendLineCode), 3 (dsx1SendPayloadCode), 4 (dsx1SendResetCode), 5 (dsx1SendQRS), 6 (dsx1Send511Pattern), 7 (dsx1Send3in24Pattern), 8 (dsx1SendOtherTestPattern) |
| Signaling Mode         | SNMP:RFC1406-MIB.dsx1SignalMode             | Signaling mode. Values: 1 (none), 2 (robbedBit), 3 (bitOriented), 4 (messageOriented)                                                                                                                                                         |
| Transmit Clock Source  | SNMP:RFC1406-MIB.dsx1TransmitClockSource    | Source of the transmit clock. Values: 1 (loopTiming), 2 (localTiming), 3 (throughTiming)                                                                                                                                                      |
| BESs                   | SNMP:RFC1406-MIB.dsx1TableBESs <sup>1</sup> | Number of bursty errored seconds                                                                                                                                                                                                              |
| CSSs                   | SNMP:RFC1406-MIB.dsx1TableCSSs              | Number of controlled slip seconds                                                                                                                                                                                                             |
| DMs                    | SNMP:RFC1406-MIB.dsx1TableDMs               | Number of degraded minutes                                                                                                                                                                                                                    |
| ESs                    | SNMP:RFC1406-MIB.dsx1TableESs               | Number of errored seconds                                                                                                                                                                                                                     |
| LCVs                   | SNMP:RFC1406-MIB.dsx1TableLCVs              | Number of line code violations                                                                                                                                                                                                                |

**Table 9-9** *mgcTDMIf Attributes*

|       |                                          |                                            |
|-------|------------------------------------------|--------------------------------------------|
| LESs  | SNMP:RFC1406-MIB.dsx1 <i>Table</i> LESs  | Number of line errored seconds             |
| PCVs  | SNMP:RFC1406-MIB.dsx1 <i>Table</i> PCVs  | Number of path coding violations           |
| SEFSs | SNMP:RFC1406-MIB.dsx1 <i>Table</i> SEFSs | Number of severely errored framing seconds |
| SESSs | SNMP:RFC1406-MIB.dsx1 <i>Table</i> SESSs | Number of severely errored seconds         |
| UASs  | SNMP:RFC1406-MIB.dsx1 <i>Table</i> UASs  | Number of unavailable seconds              |

1. *Table* refers to the RFC-1406 DSX1 table and is one of Current, FarEndCurrent, Interval, or FarEndInterval



---

## Numerics

- 2900 traps 8-8
- 2900XL traps 8-7

---

## A

- access 4-3
- access control 5-1
- access specifications 5-3
  - creating new 5-11
  - modifying 5-18
- accounts
  - attributes for 9-28
  - setting up 5-4
  - user 5-4
  - viewing 9-1
  - viewing BAMS 9-16
  - viewing Cisco MGC host 9-2
  - viewing Cisco SLT 9-6
  - viewing LAN switch 9-11
- adjacent point code 1-9, 1-11
- administrative password 5-21
- Alarm&Meas Viewer 8-32
- alarms
  - setting how long they are stored 8-41
- alternate configurations 6-2
- APC 1-9, 1-11
- attributes
  - BAMS chassis 9-32
  - host controller 9-29
  - interface 9-30
  - IP manageable 9-29
  - memory pool 9-32
  - MGC TDM 9-33
  - seed file 6-6
  - SNMP 9-30
  - TCP 9-31
  - UDP 9-32

- authenticationFailure 8-7
- average summary rule 7-18

---

## B

- BAF 1-1
- BAMS 1-1
  - chassis attributes 9-32
  - deploying 6-18
  - viewing accounts 9-16
  - viewing properties 9-17
- Bellcore Automatic Message Accounting Format (BAF) 1-1
- Billing and Measurements Server 1-1
  - deploying 6-18

---

## C

- C7 IP link 1-9
- c7iplnk 1-9
- Catalyst 2900 1-1
- Catalyst 5000 1-1
- Catalyst 5500 1-1
- CDR Viewer 8-32, 8-34
- CEMF
  - performance enhancements 2-6
- CEMF client 2-6
- CEMF concepts
  - CEMF network model 1-5
  - Element Manager 1-2
  - events 8-3
  - event state 8-3
  - management domain 8-4
  - object 1-5, 1-6
  - object type 1-6
  - object types & attributes 1-6
  - view 1-6
  - what is CEMF? 1-4
  - what is contained within CEMF? 1-4

- CEMF Launchpad
  - options menu 4-8
  - starting applications from 4-2
  - toolbar 4-8
- CISCO-CONFIG-MAN-MIB-V1SMI 8-7
- Cisco Media Gateway Controller 1-1
- CISCO-MEMORY-POOL-MIB 6-4
- ciscoMemoryPoolTable 6-4
- Cisco MGC 1-1
- Cisco MGC host 1-1
  - collecting data for active 7-3
  - deploying 6-17
  - inventory 6-4
  - traps 8-8
  - viewing accounts 9-2
  - viewing properties 9-3
- Cisco MGC Manager (CMM) 1-3
- Cisco MGC Manager (CMNM) 1-2
- Cisco MGC node 1-1
- Cisco MGC Toolbar 4-7
- Cisco MGX 8260 1-3
  - deploying 6-18
  - managing faults 8-30
  - traps 8-8
- Cisco SC 1-1
- Cisco SC2200 1-1
- Cisco Signaling Controller 1-1
- Cisco Signaling Link Terminal 1-1
- Cisco SLT 1-1
  - deploying 6-17
  - inventory 6-2
  - memory pool 6-4
  - performance data collected 7-4
  - traps 8-6
  - viewing accounts 9-6
  - viewing properties 9-7
- Cisco SLT network interfaces
  - collecting performance data for 7-5
- Cisco SS7 PRI Gateway Solution 1-2, 1-3
- CISCO-STACK-MIB 8-8
- CISCO-SYSLOG-MIB 8-7
- Cisco Tandem Offload Solution 1-2, 1-3
- CISCO-TRANSPATH-MIB 8-8
- CiscoView 1-2, 2-12, 2-13, 4-7
- Cisco Virtual Switch Controller 1-1
- Cisco VSC3000 1-1
- CiscoWorks 2000 2-12
- clearing details
  - clearing method 8-30
  - clearing time and date 8-30
  - reason for clearing 8-30
  - user responsible for clearing 8-30
- close window 4-9
- CMM 1-2, 4-7
- CMNM
  - how it models the Cisco MGC node 1-7
  - installing 2-1, 2-10
  - key features 1-2
  - overview 1-1
  - uninstalling 2-14
- CMNM session
  - quitting 4-4
- coldStart 8-6
- commAlarm 8-8
- configChange 8-7
- CONFIG-LIB Viewer 8-32, 8-36
- configuration
  - alternate 6-2
  - Cisco MGC 6-2
- connectivity network
  - containment hierarchy 1-10
- containment hierarchy 1-10
- containment view 1-7
- Cooked partitions 2-2, 2-3, 2-7
- create new objects
  - deployment 6-9
- Ctrl + 4-4

## D

data collection 7-3  
 data summaries 7-2  
 decommissioning devices 7-16  
 deploying  
     BAMS 6-18  
     Billing and Measurements Server 6-18  
     Cisco MGC host 6-17  
     Cisco MGX 8260 6-18  
     Cisco SLT 6-17  
     LAN switch 6-18  
     media gateway network 6-15  
     site 6-11  
 deploying a network  
     using a seed file 6-6  
 deployment 6-1  
     manual 6-1  
     seed file 6-1  
 deployment wizard 6-9  
     open from existing object 6-11  
 destination point code 1-11  
 device inventory 6-1  
 diagnostic tools 4-7  
 disable toolbar 4-8  
 discovery 4-3  
 DNS requirements 2-8  
 documentation  
     BAMS xiii  
     CEMF xiii  
     suite of xii  
 DPC 1-11  
 DPNSS 1-9

## E

edit alarm state  
     acknowledge alarms 8-26  
     acknowledge alarms with comment 8-26

    clear alarms 8-26  
     unacknowledge alarms 8-26  
 EISUP path 1-9  
 eisuppath 1-9  
 Element Manager 1-2  
 end date data entry box 7-17  
 end time data entry box  
     Performance Manager 7-17  
 enetif 1-9  
 environmentError 8-8  
 equipmentError 8-8  
 errored state 8-6  
 Ethernet interface 1-7, 1-9, 1-10  
     viewing properties 9-18  
 Event Browser  
     drop down menu options 8-14  
     event history 8-27  
     event history enabled 8-28  
     full color coding 8-27  
     full event description 8-28  
     full event description screen 8-29  
     launch 8-13  
     manage an event from the menu bar 8-26  
     manage an event from the window 8-25  
     managing events 8-25  
     manual update 8-26  
     no color coding 8-27  
     open the query editor 8-15  
     partial color coding 8-27  
     print 8-15  
     progress bar 8-16  
     refresh 8-28  
     screen information 8-15  
     select type of color coding 8-27  
     set color coding 8-27  
     view the event history 8-27  
 Event Browser screen 8-13  
 events 4-3  
     history 8-27

- how CEMF models 8-3
- managing 8-25
- modifying filtering criteria 8-23
- setting how they are color coded 8-27
- sorting 8-24
- states 8-3
- viewing event history 8-27

external node 1-9

extnode 1-9

---

## F

FAS path 1-9

faspath 1-9

fault management

- introduction 8-1

faults

- how CMNM manages 8-5
- managing Cisco MGX 8260 8-30

feature lists 5-1, 5-3

file menu

- close 4-9
- print 4-9

File Options 8-32, 8-40

forwarding traps 8-11

FTP 7-3

full event description

- Event Browser 8-28

full event description screen

- acknowledge details 8-30
- clearing details 8-30
- Event Browser 8-29
- event description 8-29
- event state 8-30
- management domain 8-29
- object name 8-29
- severity 8-29
- time and date 8-29

---

## G

graphs and charts 7-18

groups 4-3

---

## H

hard drive partitioning 2-2

hardware requirements 2-1

help 4-9

history storage criteria 7-3

host controller attributes 9-29

---

## I

IF-MIB 6-2, 8-6

IF-MIB.ifAdminStatus 6-3

IF-MIB.ifDescr 6-3

IF-MIB.ifIndex 6-2

IF-MIB.ifInErrors 6-3, 7-6

IF-MIB.ifInOctets 6-3, 7-6

IF-MIB.ifLastChange 6-3

IF-MIB.ifMtu 6-3

IF-MIB.ifOperStatus 6-3

IF-MIB.ifOutErrors 6-3, 7-6

IF-MIB.ifOutOctets 6-3, 7-6

IF-MIB.ifPhysAddress 6-3

IF-MIB.ifSpecific 6-3

IF-MIB.ifSpeed 6-3

IF-MIB.ifType 6-3

installing CMNM 2-1

interface attributes 9-30

interfaces 6-2

- Ethernet 1-7
- serial 1-7
- TDM 1-7

inventory

- Cisco MGC host 6-4
- Cisco SLT 6-2

- connectivity network 6-5
- LAN switch 6-2
- IP FAS path 1-9
- ipfaspath 1-9
- IP link 1-10
- iplnk 1-10
- IP manageable attributes 9-29
- ISDN-PRI 1-9

---

## L

- LAN switch 1-3
  - 5500 traps 8-7
  - deploying 6-18
  - memory pool 6-4
  - performance data collected 7-4
  - viewing accounts 9-11
  - viewing properties 9-12
- LAN switch inventory 6-2
- linkDown 8-7
- linkset 1-10
- linkUp 8-6
- lnkset 1-10
- logicalOR
  - summary rule 7-18
- login screen 4-2
- Log Viewer 8-32, 8-37

---

## M

- management domain 8-4
- managing events in Event Browser 8-25
- manual deployment 6-9
  - using templates 6-10
- max summary rule 7-18
- media gateway network
  - deploying 6-15
- memory pool
  - Cisco SLT 6-4

- LAN switch 6-4
- memory pool attributes 9-32
- MGCP path 1-10
- mgcppath 1-10
- MGC TDM attributes 9-33
- MGC Tool Bar 8-31
- min summary rule 7-18
- missed poll 7-3
- MML 1-11
- mms1600\_trap 8-9
- modifying
  - access specifications 5-18
  - user groups 5-17
  - users 5-16
- monitored attributes 7-17
- mouse
  - left button 4-4
  - middle button 4-4
  - right button 4-4
- multiple disk drives 2-2
- multiple Event Browser sessions 8-2

---

## N

- NAS path 1-10
- naspath 1-10
- navigating through CMNM 4-4
- navigation
  - Alt+ 4-5
  - Ctrl+ 4-5
- network devices, viewing information about 9-1
- network interface 1-7
- normal state 8-6
- northbound systems
  - forwarding traps to 8-11
- now checkbox
  - Performance Manager 7-17

## O

- object attributes 1-6
- object classes 1-6
- object group 5-3
- Object Group Manager 1-7
- object groups 1-7
- objects 1-5
- ObjectStore 2-4
- object types 1-6
- on demand polling 7-15
- open the query editor
  - Event Browser 8-15

## P

- password 4-2
  - changing administrative 5-21
- password requirements 6-1
- perfMeasFilters 7-8
- performance data
  - archiving 7-21
  - collected for Cisco MGC host 7-3
  - collected for Cisco SLT 7-4
  - collected for LAN switch 7-4
  - collected for LAN switch network interfaces 7-6
  - viewing 7-16
  - viewing logs 7-21
- performance enhancements 2-6
- Performance Manager
  - end date data entry box 7-17
  - end time data entry box 7-17
  - graphs and charts 7-3
  - history storage criteria 7-3
  - how data is collected 7-3
  - missed polls 7-3
  - now checkbox 7-17
  - opening 7-6
  - points, color coding 7-21

- refresh button 7-18
- sample line chart screen 7-19
- sample table display screen 7-19
- screen 7-8
- start date data entry box 7-17
- start polling events point 7-19
- start time data entry box 7-17
- stop polling events point 7-19
- summary interval 7-17
- summary rule 7-17
- viewing a chart 7-20
- view performance statistics 7-17
- view points and values on a line chart 7-21
- view raw data 7-20

## Performance Manager data

- raw 7-2
- summarized 7-2

## Performance Manager screen 7-8

## performance monitoring

- introduction 7-1

## performance statistics

- printing from Performance Manager 7-22

## permission level 5-3

## point code 1-10

## points color coding 7-21

## polling 7-1

- action report 7-15

- changing defaults 7-8

- decommissioning devices 7-16

- different states of a device 7-12

- on demand 7-15

- presence 8-6

- rediscovering devices 7-16

- setting frequencies 7-8

- starting on a device 7-11

- understanding state symbols 7-12

## POM DynamicReconfiguration 6-6

## pop up menu

- deployment 6-11

print 4-9  
 printing performance statistics 7-22  
 print view displayed in window 4-9  
 processingError 8-8  
 progress bar  
   Event Browser 8-16  
 propagation  
   event 8-4  
 properties  
   attributes for 9-28  
   viewing 9-1  
   viewing BAMS 9-17  
   viewing Cisco MGC host 9-3  
   viewing Cisco SLT 9-7  
   viewing Ethernet interface 9-18  
   viewing LAN switch 9-12  
   viewing serial interface 9-26  
   viewing TDM interface 9-19  
 ptcodes 1-10

## Q

---

Q.931 protocol 1-10  
 qualityOfService 8-8  
 Query Editor  
   modifying filtering criteria 8-23  
   screen 8-12, 8-16  
   set up sort options 8-24  
   sort options  
     object name 8-24  
     severity 8-24  
     time 8-24  
 quitting a CMNM session 4-4

## R

---

raw data  
   Performance Manager 7-2  
 Raw partitions 2-2, 2-4, 2-8

rediscovering devices 7-16  
 Reflection  
   configuring 2-14  
 refresh button 7-18  
 RFC1213-MIB.tcpActiveOpens 7-5  
 RFC1213-MIB.tcpAttemptFails 7-5  
 RFC1213-MIB.tcpCurrEstab 7-5  
 RFC1213-MIB.tcpEstabResets 7-5  
 RFC1213-MIB.tcpInErrs 7-5  
 RFC1213-MIB.tcpInSegs 7-5  
 RFC1213-MIB.tcpMaxConn 7-4  
 RFC1213-MIB.tcpOutRsts 7-5  
 RFC1213-MIB.tcpOutSegs 7-5  
 RFC1213-MIB.tcpPassiveOpens 7-5  
 RFC1213-MIB.tcpRetransSegs 7-5  
 RFC1213-MIB.udpInDatagrams 7-5  
 RFC1213-MIB.udpInErrors 7-5  
 RFC1213-MIB.udpNoPorts 7-5  
 RFC1213-MIB.udpOutDatagrams 7-5  
 RFC1406-MIB 6-3  
 RFC1406-MIB.dsx1CurrentESs 6-3  
 RFC1406-MIB.dsx1CurrentSEs 6-3  
 RFC1406-MIB.dsx1FarEndCurrentESs 6-4  
 RFC1406-MIB.dsx1FarEndCurrentSEs 6-4  
 RFC1406-MIB.dsx1FarEndIntervalESs 6-3  
 RFC1406-MIB.dsx1FarEndIntervalSEs 6-4  
 RFC1406-MIB.dsx1IfIndex 6-3  
 RFC1406-MIB.dsx1IntervalESs 6-3  
 RFC1406-MIB.dsx1IntervalSEs 6-3

## S

---

security 5-1  
 seed file  
   attributes 6-6  
   deploying a network using 6-6  
   selecting items 4-5  
   serial interface 1-7  
   viewing properties 9-26

Service Switching Points (SSPs) 1-9

severity

- colors used 8-4

sgcpath 1-10

SGCP path 1-10

shelfAlarmClear 8-8

shelfColdStart 8-9

shelfMajorAlarm 8-8

shelfMinorAlarm 8-8

shelfSecurityAlert 8-9

shortcut keys 4-5

show toolbar 4-8

Signaling Transfer Point (STP) 1-10

site

- deploying 6-11

SNMP 6-3, 7-3, 7-18, 8-4

SNMP attributes 9-30

SNMPv2-MIB 8-6

SNMPv2-MIB.sysContact 6-2

SNMPv2-MIB.sysDesc 6-2

SNMPv2-MIB.sysLocation 6-2

SNMPv2-MIB.sysName 6-2

SNMPv2-MIB.sysUpTime 6-2

software requirements 2-6

sorting events 8-24

sort options 8-24

source domain 8-4

SS7 network 1-9

SS7 path 1-10

ss7path 1-10

SS7 route 1-10

ss7route 1-10

ss7subsys 1-10

SS7 subsystem 1-10

Start Date data entry box

- Performance Manager 7-17

starting a CMNM session 4-1

start time data entry box

- Performance Manager 7-17

Status Dialog screen 4-8

status information

- viewing 4-7

STP 1-11

summarized data 7-2

summary interval 7-17

summary rule 7-17

- average 7-18
- logicalOR 7-18
- max 7-18
- min 7-18
- total 7-18

switchModuleDown 8-8

switchModuleUp 8-8

synchronization 6-5

sysinfo 6-5

syslogAlarm 8-7

---

## T

TCAP IP path 1-10

tcapipath 1-10

TCP attributes 9-31

tdmif 1-10

TDM interface 1-10, 6-3

- viewing properties 9-19

TDM link 1-10

telnet 4-7

Time Division Multiplexing (TDM) interfaces 1-7

toolbar 4-8

- disable 4-8
- enable 4-8, 4-9

total

- summary rule 7-18

Trace Viewer 8-32, 8-38

Translation Verification 8-32, 8-39

traps

- 2900 8-8
- 2900XL 8-7



Cisco MGC host 8-8  
 Cisco MGX 8260 8-8  
 Cisco SLT 8-6  
 forwarding to other systems 8-11  
 LAN switch 5500 8-7  
 receipt not guaranteed 8-11

---

## U

UDP attributes 9-32  
 user  
   modifying 5-16  
 user group 5-1, 5-3  
   creating 5-8  
   modifying 5-17  
 user name  
   CEMF login 4-2  
 user password  
   CEMF login 4-2

---

## V

view  
   containment 1-7  
   network 1-7  
   physical 1-7  
 viewer 4-3  
 viewing a chart 7-20  
 view points and values on a line chart 7-21  
 view raw data 7-20  
 view the event history 8-27  
 view up-to-date Performance Manager information 7-3  
 Voice Services Provisioning Tool 1-2, 1-3  
 VSC 1-1  
 VSPT 1-2, 4-7

---

## W

warmStart 8-6

Web Viewer 1-2, 1-4, 4-7  
 window refresh  
   Event Browser 8-28

---

## X

XDMCP connection 2-15  
 XECfgParm.dat  
   desiredPlatformState 6-4  
   homeDirRoot 6-4  
   IP\_Addr1, IP\_Addr2, IP\_Addr3, IP\_Addr4 6-4  
   ipAddrPeerA, ipAddrPeerB 6-4  
   maxNumLinks 6-5  
   maxNumMGCPLinks 6-5  
   maxNumPRIL3Links 6-5  
   product.vendor 6-5  
   product.version 6-5  
   SysVirtualSwitch 6-4  
 XTerm 4-7