



Cisco Media Gateway Controller Node Manager User Guide 1.5

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: 78-12214-01

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

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

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

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

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

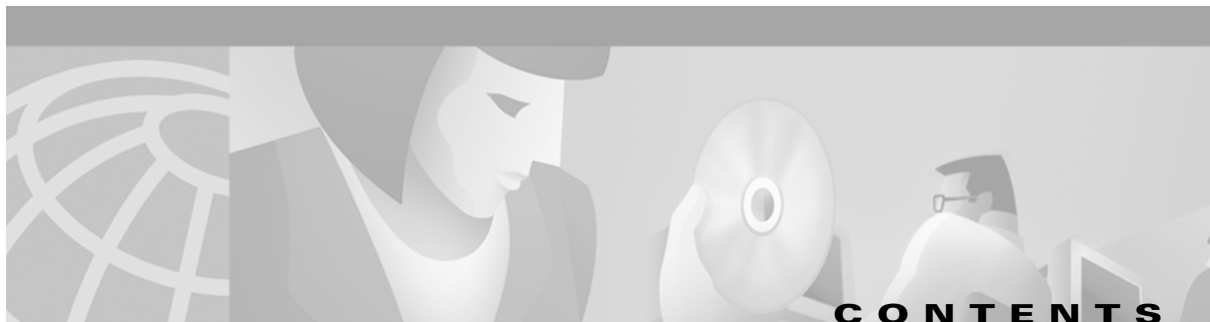
Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, Cisco Powered Network logo, Cisco Systems Networking Academy, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence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

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0010R)

Cisco Media Gateway Controller Node Manager User Guide 1.5

Copyright © <2000>, Cisco Systems, Inc.

All rights reserved.



Preface **xiii**

Document Objectives	xiii
Audience	xiii
Document Organization	xiii
Documentation Suite	xv
Cisco MGC Documentation	xv
Cisco Element Management Framework Documentation	xv
Billing and Measurements Server Documentation	xv
Document Conventions	xvi
Obtaining Documentation	xvii
World Wide Web	xvii
Documentation CD-ROM	xvii
Ordering Documentation	xvii
Documentation Feedback	xvii
Obtaining Technical Assistance	xviii
Cisco.com	xviii
Technical Assistance Center	xviii
Contacting TAC by Using the Cisco TAC Website	xviii
Contacting TAC by Telephone	xix

CHAPTER 1

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

Introduction	1-1
Terms Used in This Document	1-1
Overview of the Cisco MGC Node Architecture	1-2
Key Features of CMNM	1-2
Overview of CEMF	1-4
CEMF Components	1-4
How CEMF Models the Network	1-5
MGC Node View	1-7
Host View	1-8
SLT View	1-9
Switch View	1-10

- BAMS View **1-10**
- Physical View **1-11**
- Network View **1-11**
- How CMNM Models the Cisco MGC Node **1-12**
 - Cisco MGC Host Signaling Network **1-12**
 - Cisco MGC Host Signaling Objects **1-12**
 - Containment Hierarchy of the Signaling Network **1-14**
 - Cisco MGC Host Trunking Objects **1-15**
 - Containment Hierarchy of the Trunking Objects **1-15**
 - Cisco MGC Host Dial Plan Objects **1-16**
 - Containment Hierarchy of the Dial Plan Objects **1-17**
- Overview of Event Manager **1-18**
 - Thresholding Regimes **1-18**
 - Notification Profiles **1-19**
 - Event Groups **1-20**

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 **2-3**
 - Suggested Layout for Cooked Partitions (CEMF Default) **2-3**
 - Suggested Layout for Raw Partitions **2-4**
 - Configuring Raw File Systems in ObjectStore **2-5**
 - Suggested Layout for the CEMF Client **2-6**
- Software Requirements **2-6**
- Recommended Performance Enhancements for CEMF **2-7**
 - Performance Enhancements for Cooked Partitions **2-7**
 - Option 1 **2-7**
 - Option 2 **2-7**
 - Performance Enhancements for Raw Partitions **2-8**
 - Option 1 **2-8**
 - Option 2 **2-9**
- 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 Element Managers	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	2-15
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 (2611)	3-2
Configuring a LAN Switch (Catalyst 2900XL)	3-3
Configuring the LAN Switch (Catalyst 5500)	3-4
Configuring the Cisco MGX 8260	3-5
Configuring BAMS	3-5

CHAPTER 4**Getting Started with CMNM 4-1**

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
Ctrl +	4-5
Alt +	4-6
Selecting from Lists in CMNM	4-6

- Block Selecting Multiple Items by Clicking and the Shift Key 4-6
- Selecting Multiple Items by Clicking and the Ctrl Key 4-6
- Selecting All Items 4-6
- Deselecting All Items 4-7
- Viewing Status Information 4-7
- Using the Toolbar 4-7
 - Enabling the Toolbar 4-8
 - Disabling the Toolbar 4-8
 - Showing or Hiding Tooltips 4-8
 - Printing the View Displayed in the Window 4-8
 - Closing a Window 4-9
 - Accessing Help 4-9
- Moving Between Open Windows 4-9

CHAPTER 5

- Setting Up CMNM Security 5-1**
 - Introduction to CMNM Security 5-1
 - User Groups 5-1
 - Feature Lists 5-1
 - Access Specifications 5-3
 - 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
 - Deploying a Network Using a Seed File 6-1
 - Seed File Attributes 6-2
 - Physical Location Field 6-3
 - Specifying a Deployment Seed File 6-3

Manually Deploying a Site, Object, or Network	6-6
Deployment Attributes	6-7
Opening the Deployment Wizard	6-7
Deploying a Cisco MGC Node	6-8
Deploying a Cisco MGC Host	6-9
Deploying a Cisco SLT	6-10
Deploying a LAN Switch	6-10
Deploying a Cisco MGX 8260	6-11
Deploying a Billing and Measurements Server (BAMS)	6-11
Subrack Discovery	6-11
Cisco MGC Host and BAMS Discovery	6-12
CIAgent System Component Discovery	6-12
Cisco SLT Discovery	6-12
Cisco 2900XL Discovery	6-13
Catalyst 5500 Discovery	6-14
Cisco MGC Node Discovery	6-15
Synchronization	6-16
Managing Software Images and Configurations	6-16
TFTP Server	6-17
Uploading and Downloading Cisco SLT and LAN Switch Images and Configurations	6-17
Uploading and Downloading Cisco MGC Host and BAMS Images and Configurations	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
Common Performance Data Collected for Several Devices	7-3
Performance Data Collected for the Cisco MGC Hosts	7-5
Performance Data Collected for BAMS	7-5
Performance Data Collected for the Cisco SLT	7-6
Performance Data Collected for the LAN Switch	7-6
Performance Data Collected for Network Interfaces	7-7
Performance Data Collected for TDM Interfaces	7-7
Performance Data Collected for the Cisco 2900XL LAN Switch Port	7-8
Performance Data Collected for the CIAgent System Components	7-8
Fixed Disk	7-8
Processor	7-9

- RAM 7-9
- Virtual Memory 7-9
- Cisco MGC Host Configuration Performance Counters 7-9
 - Measurement Filters 7-10
- Opening the Performance Manager 7-10
- Setting Polling Frequencies 7-12
 - Understanding the Different Polling States of a Device 7-13
 - Changing Collection Defaults 7-14
 - Setting Different Polling Frequencies 7-14
 - Starting Polling On a Device 7-17
 - Decommissioning, Rediscovering, and Rebooting Devices 7-20
- Viewing Performance Data 7-23
 - Viewing Raw Data 7-27
 - Viewing a Chart 7-27
 - Viewing Points and Values on a Line Chart 7-28
 - Viewing a Performance Log 7-28
- Setting How Performance Data Is Archived 7-28
- Exporting Performance Data 7-29
- Printing a Performance File 7-30

CHAPTER 8

Managing Traps and Events 8-1

- Introduction to Fault Management 8-1
- How CEMF Models Events 8-2
 - Event Information 8-3
 - Event State 8-3
 - Colors used to Indicate Severity 8-3
 - Source Domain 8-4
 - Management Domain 8-4
 - Event Propagation 8-4
- How CMNM Manages Faults 8-5
- Presence/Status Polling 8-6
 - How CMNM Manages Multiple IP Addresses for Presence Polling 8-6
 - Trap Proxies 8-7
 - IP Address Failover 8-7
 - Status Polling 8-8
 - Polling Frequency 8-9

Manual SNMP Query	8-9
How Traps Are Managed for Network Devices	8-10
BAMS Alarms	8-10
Cisco SLT Alarms	8-10
Catalyst LAN Switch Alarms	8-11
Catalyst 5500 Alarms	8-11
Catalyst 2900XL Alarms	8-12
Catalyst 2900 Alarms	8-12
Cisco MGC Host Alarms	8-13
MGC Host and BAMS Resource Alarms	8-13
Cisco MGX 8260 Alarms	8-14
8-17	
Trap Receipt Not Guaranteed	8-17
How Traps Are Cleared Using Correlation Files	8-17
Cisco MGC Host Clear Correlation	8-17
Cisco SLT Clear Correlation	8-17
LAN Switch Clear Correlation	8-18
CIAgent Clear Correlation	8-19
Forwarding Traps to Other Systems	8-19
Opening the Event Browser	8-21
Overview of the Event Browser Screen	8-21
Filtering Events Using Queries	8-23
Opening the Query Editor	8-23
Setting Filtering Criteria	8-24
Modifying Filtering Criteria	8-31
Sorting Events	8-32
Setting Up Sort Options	8-32
Managing Events	8-33
Managing an Event from the Window	8-33
Managing an Event from the Menu Bar	8-34
Enabling Auto or Manual Update	8-34
Setting How Events Are Color-Coded	8-35
Selecting the Type of Color Coding to Be Used	8-35
Viewing the Event History	8-35
Refreshing the Event Window	8-36

- Viewing a Full Description of an Event **8-36**
 - Acknowledge Details **8-38**
 - Clearing Details **8-38**
- Managing Cisco MGX 8260 Faults **8-38**
- Using the Cisco MGC Tool Bar **8-39**
 - Alarm and Measurements Viewer **8-40**
 - CDR Viewer **8-42**
 - CONFIG-LIB Viewer **8-44**
 - Log Viewer **8-45**
 - Trace Viewer **8-46**
 - Translation Verification **8-47**
 - File Options **8-48**
- Setting How Long Alarms Are Stored **8-49**

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 MGC Host File Systems **9-8**
 - Viewing Cisco SLT Accounts **9-11**
 - Viewing Cisco SLT Properties **9-13**
 - Viewing LAN Switch Accounts **9-18**
 - Viewing LAN Switch Properties **9-20**
 - Viewing BAMS Accounts **9-25**
 - Viewing BAMS Properties **9-27**
 - Viewing BAMS File Systems **9-33**
 - Viewing CI-Agent Device Information **9-36**
 - Viewing Ethernet Interface Properties **9-40**
 - Viewing TDM Interface Properties **9-42**
 - Viewing Serial Interface Properties **9-44**
- Using Diagnostic Tools **9-48**
 - MGC Host Status Check **9-49**
 - Configuration Audit **9-50**
 - Processes and Alarms **9-50**
 - File System Monitor **9-50**

Identifying Where You Can Launch Features in CMNM 9-51

APPENDIX A**BAMS, Cisco MGC, and CMNM Messages A-1**

Looking Up BAMS and Cisco MGC Messages A-1

Cisco MGC Host Messages A-2

BAMS Messages A-2

CMNM Internal Messages A-3

Solving Deployment and Discovery Errors A-6

 Changing Password or Community Strings A-6

 Changing IP Address A-6

 Rediscovering a Device After a Problem A-6

INDEX



Preface

Document Objectives

This user 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.
Appendix A	BAMS, Cisco MGC, and CMNM Messages	This appendix supplements the information in Chapter 8. It provides references to documentation explaining BAMS and Cisco MGC alarm messages and it describes CMNM's own internal alarms.

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 8 Installation and Configuration Guide*
- *Cisco Media Gateway Controller Software Release 8 Provisioning Guide*
- *Cisco Media Gateway Controller Software Release 8 Reference Guide*
- *Cisco Media Gateway Controller Software Release 8 Operations, Maintenance, and Troubleshooting Guide*
- *Release Notes for Cisco Media Gateway Controller Software Release 8*
- *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 Administration 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:

boldface font	Commands and keywords are in boldface .
<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 <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font .
<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

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

World Wide Web

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

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered CCO users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

<http://www.cisco.com>

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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



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 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 2-12 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.

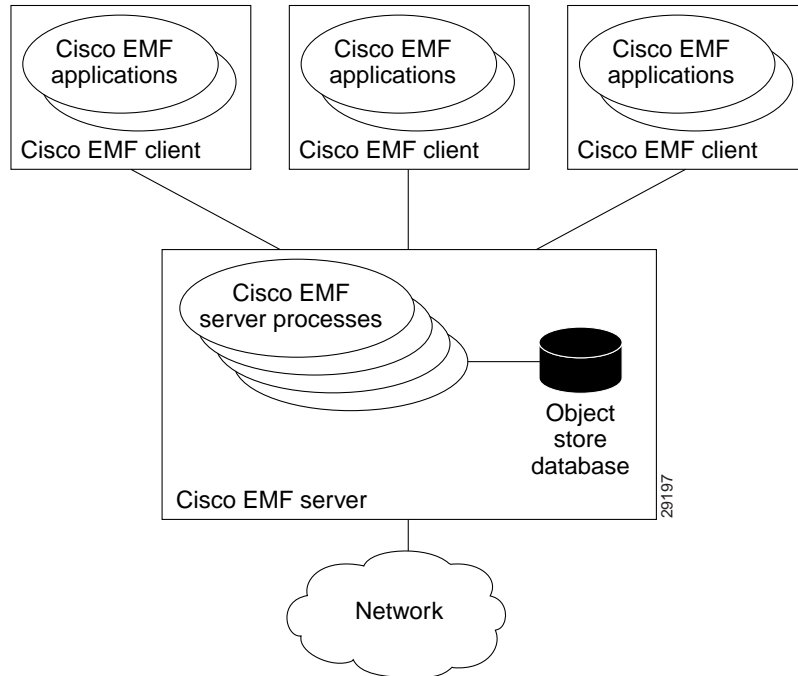
CEMF has been designed to overcome the limitations of traditional enterprise network management solutions, particularly in the broadband access market, and also in other network management applications where the aforementioned characteristics are important. CEMF is used to quickly develop and deploy 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 Viewer browser.

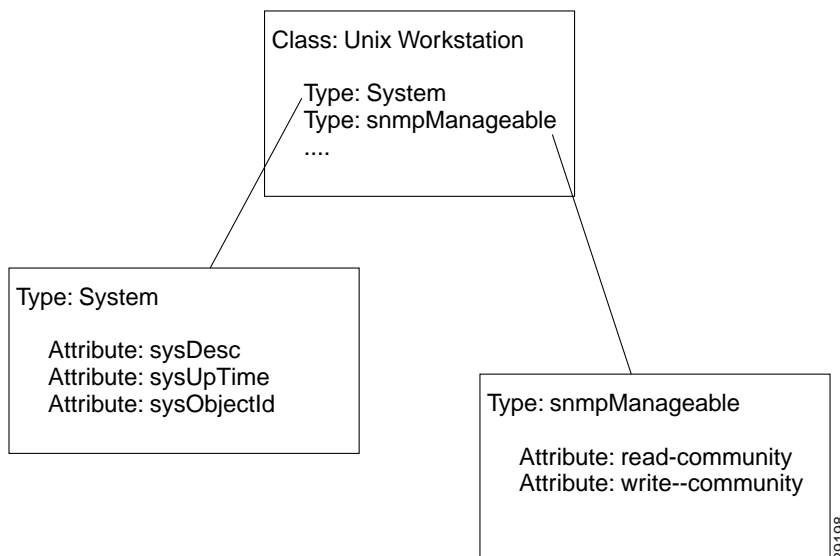
The use of classes also allows powerful queries to be carried out based upon the kind of object. Examples of this type of query could be: show all events in the system from cable modems or create a group of router objects.

- 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 UNIX Workstation 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. CMNM views are summarized in Table 1-1.

Table 1-1 CMNM Views

View	Description
MGC-Node-View	Displays all of the Cisco MGC nodes in the network along with their logical children (Cisco SLTs, switches, Cisco MGC hosts, and so on). This view also includes all of the signaling, dial plan, and trunking components of the Cisco MGC node. For more information, see the “MGC Node View” section on page 1-7.
Host-View	Presents all of the Cisco MGC host devices in the network. For more information, see the “Host View” section on page 1-8.
SLT-View	Presents all of the Cisco SLT devices in the network. This view also contains all of the interfaces on each Cisco SLT. For more information, see the “SLT View” section on page 1-9.
Switch-View	Presents all of the LAN switch devices in the network. This view also shows all of the interfaces on each LAN switch. For more information, see the “Switch View” section on page 1-10.
BAMS-View	Presents all of the BAMS in the network. For more information, see the “BAMS View” section on page 1-10.
Physical	Displays all of the Cisco MGC network devices, grouped by physical location (buildings, sites, regions, and so on). For more information, see the “Physical View” section on page 1-11.
Network	Displays all IP devices within their relative networks and subnets. This is a standard CEMF View. For more information, see the “Network View” section on page 1-11.

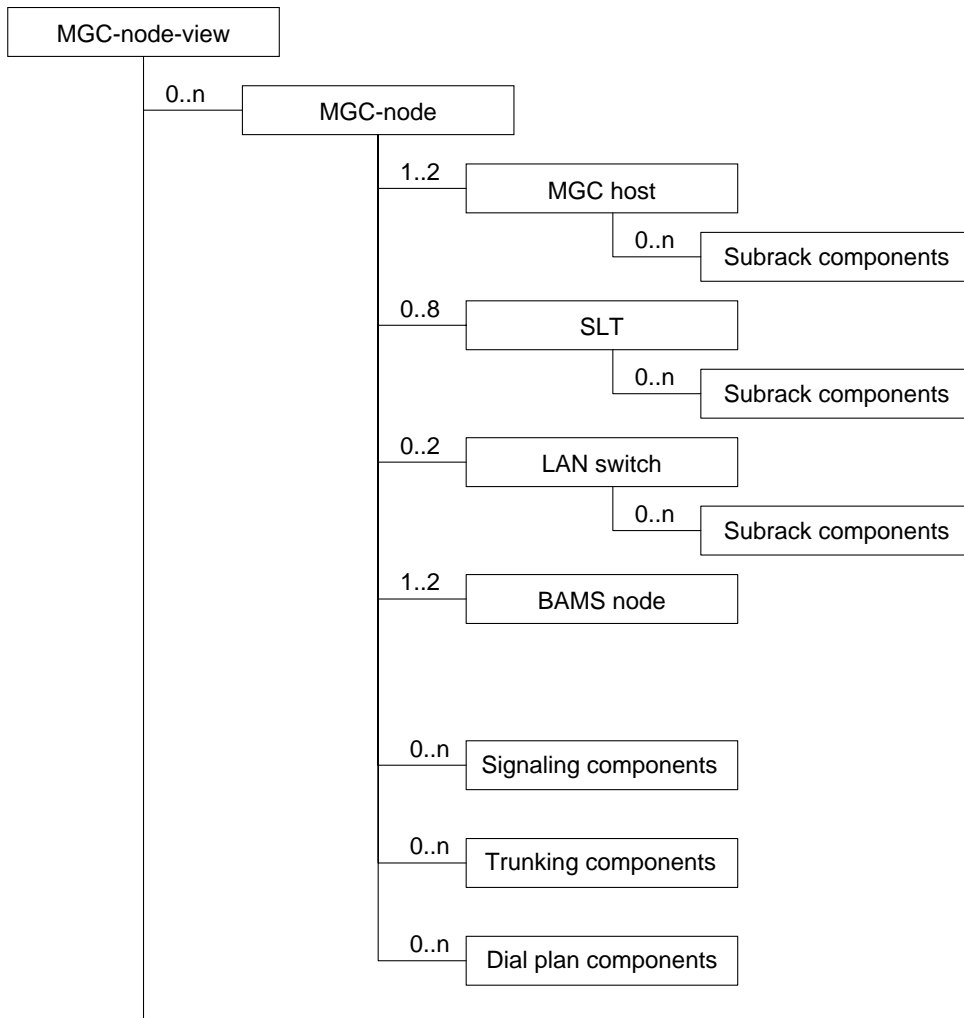
- Object groups—An object group is simply a collection of objects that are related in some way. They may all be the same type of equipment or all belong to the same customer.

Object groups can be built either manually or by building a query. Object groups are accessible through the Object Group Manager application.

MGC Node View

The MGC-Node-View displays all of the Cisco MGC node elements in the network. For each Cisco MGC node, all of the logical components of the node are displayed, as illustrated in Figure 1-3.

Figure 1-3 MGC Node View

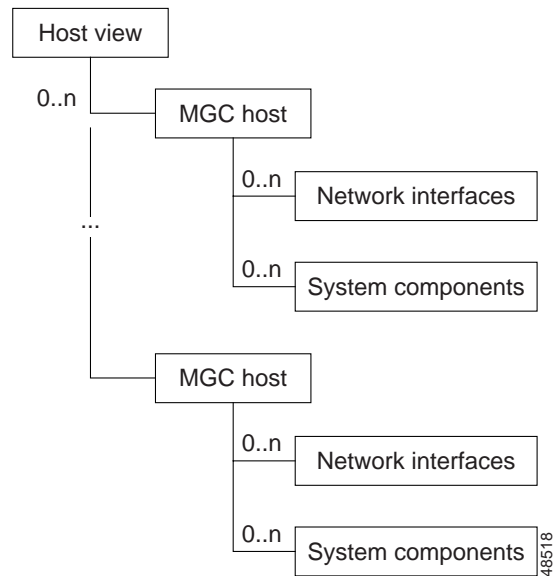


Each Cisco MGC node is represented with its logical child elements. These child elements include the Cisco MGC hosts, BAMS, Cisco SLTs, and LAN switches, and each device's network interfaces. Depending on the configuration, there can be up to two Cisco MGC host devices (active/standby pair), two BAMS (active/standby pair), eight Cisco SLTs, and two LAN switches.

In addition to the physical devices, the logical configuration of the active Cisco MGC host is also displayed. This logical configuration includes the signaling, trunking, and dial plan information from the active Cisco MGC host. For more information, see the “How CMNM Models the Cisco MGC Node” section on page 1-12.

Host View

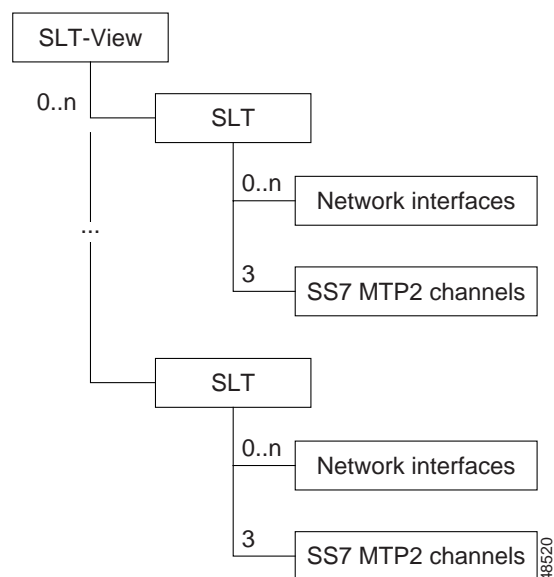
The Host-View displays all of the Cisco MGC host devices along with their associated interfaces, as illustrated in Figure 1-4.

Figure 1-4 Host View

Each Cisco MGC host in the network is displayed along with its network interfaces and system components. This view is used to collect all Cisco MGC hosts in a single location where services can be launched.

SLT View

The SLT-View displays all of the Cisco SLT devices in the network along with their associated interfaces, as illustrated in Figure 1-5.

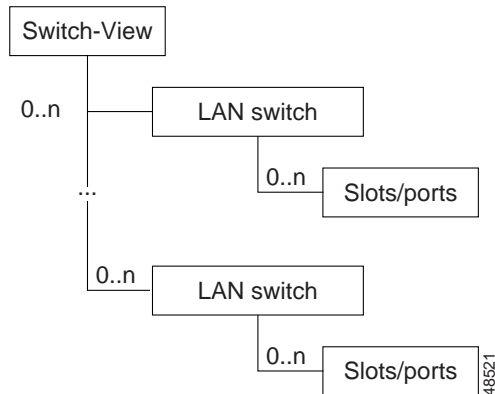
Figure 1-5 SLT View

This view is used to collect all Cisco SLTs in a single location. From this view the user can monitor faults or launch Cisco SLT-specific services.

Switch View

The Switch-View displays all of the LAN Switches in the network. In addition, the slots and ports on the LAN switches are displayed, as illustrated in Figure 1-6.

Figure 1-6 LAN Switch View

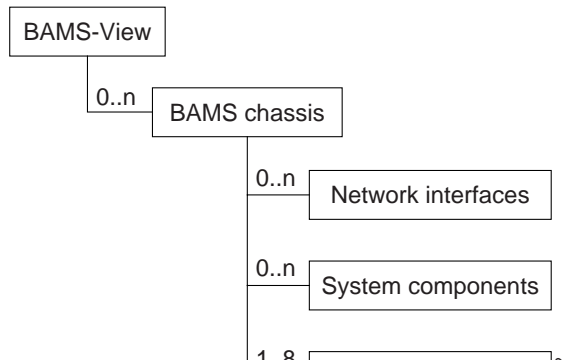


This view is used to collect all LAN switches in a single location for viewing faults or launching services.

BAMS View

The BAMS-View displays all of the BAMS in the network. For each BAMS, the network interfaces of the BAMS are displayed. In addition, each Cisco MGC host that is communicating with the BAMS is shown, as illustrated in Figure 1-7.

Figure 1-7 BAMS View



Each BAMS in the network is displayed along with its network interfaces and system components. This view is used to collect all BAMS in a single location where services can be launched.

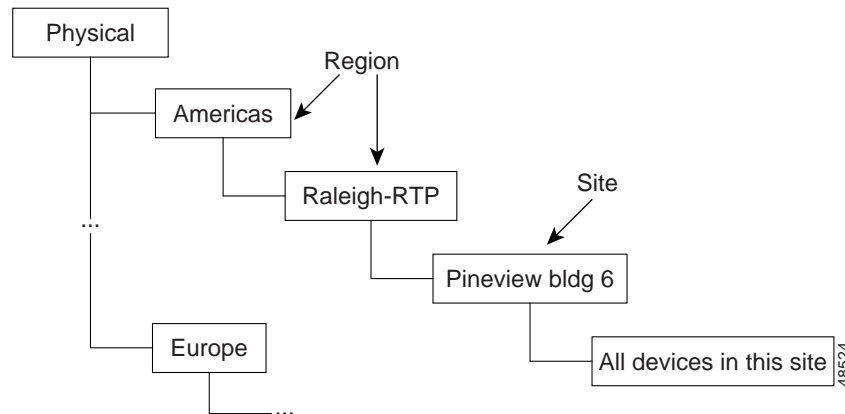
Physical View

The Physical view is used to model the physical interconnections between devices. Because of the nature of the Cisco MGC node, the relation between devices is more of a logical connection than a physical one. Since the logical connections are already represented in the other containment trees, CMNM uses the Physical view to represent the physical location of devices. In this view, the operator is free to set up different types of grouping based on the physical layout of the network.

Users can create sites and regions to represent the physical locations of devices in their network. When Cisco MGC node devices are deployed, users can specify the physical location of these devices in one of the pre-defined regions or sites. In this way, the Physical view can be used to quickly see which network elements are colocated. In the same way, network operations center (NOC) operators can easily see where personnel should be dispatched in the event of a device failure.

An example of the Physical view is shown in Figure 1-8.

Figure 1-8 Physical View



During deployment the administrator dictates which devices are placed in each region or site. Note that CMNM does not represent any relationships between objects in each site (this is done by the other views). Rather, each device is shown at a single level of hierarchy in the region or site. Also note that only physical devices are shown in this view. Because the Cisco MGC node is not a “physical” device, it is not present in this view.

Network View

The Network view groups all IP-enabled devices in containers based on their subnet address. This view is a standard CEMF view and is not controlled or managed any way by CMNM. The idea behind the Network view is to see all of the devices on a particular subnet. In practice, this view is not used very often.

How CMNM Models the Cisco MGC Node

This section provides information about how CMNM models:

- Cisco MGC host signaling network
- Cisco MGC host trunking objects
- Cisco MGC host dial plan objects

Cisco MGC Host Signaling Network

CMNM displays the status of the Cisco MGC host signaling 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 objects 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 signaling network is updated to reflect the current configuration and network status of the active Cisco MGC host.

CMNM monitors the status of the signaling 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.

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 Signaling Objects

The Cisco MGC host software defines over 20 different types of network signaling 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 signaling 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 signaling network in CMNM are described in Table 1-2.

Table 1-2 Classes Representing Signaling 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 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.
iplnk	IP link	IP connection between a Cisco MGC 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/adapter 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 Signaling Network

When CMNM retrieves the current configuration from the active Cisco MGC host, it establishes the containment hierarchy of the signaling network. A hierarchical model example is shown in Figure 1-9.

Figure 1-9 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

Cisco MGC Host Trunking Objects

As with signaling components, CMNM also models all of trunk groups on the active Cisco MGC host. CMNM also makes trunk information available to northbound systems. Trunks represent the physical bearer channels, while trunk groups provide a higher-level grouping of trunks.

Trunk group components are stored in a separate logical folder, the Trunking Components folder. This object is used to group the trunking components and avoid a cluttered display. When the Cisco MGC host is using switched trunks, each trunk group is shown in the folder. When the Cisco MGC host does not have any trunk groups, the folder is empty.

CMNM defines a class to represent each type of trunking component. The attributes associated with each class typically match the attributes in the MML command use to provision the component.

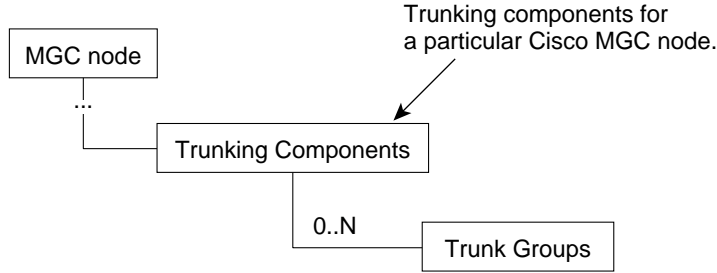
The classes used to represent the trunking objects in CMNM are described in Table 1-3.

Table 1-3 Classes Representing Trunking Objects

MML Type	Description
nailedtrnk	Nailed trunk component.
switchtrnk	Switched trunk component.
trnkgrp	Trunk group component.

Containment Hierarchy of the Trunking Objects

When CMNM retrieves the current configuration from the active Cisco MGC host, it establishes the containment hierarchy of the trunking objects. A hierarchical model example is shown in Figure 1-10.

Figure 1-10 Hierarchical Model Example of Trunking Objects

Trunks are accessible via an action

48511

Cisco MGC Host Dial Plan Objects

CMNM models the dial plan components on the active Cisco MGC host. The dial plan allows the Cisco MGC to perform pre-analysis, calling (A) number analysis, called (B) number analysis, and cause analysis. The routing components of the dial plan are used to identify the path for bearer traffic from the Cisco MGC host to its adjacent switch.

As with trunking components, dial plan components are stored in a separate folder.

CMNM defines a class to represent each type of dial plan component. The attributes associated with each class typically match the attributes in the MML command used to provision the component.

The classes used to represent the dial plan objects in CMNM are described in Table 1-4.

Table 1-4 Classes Representing Dial Plan Objects

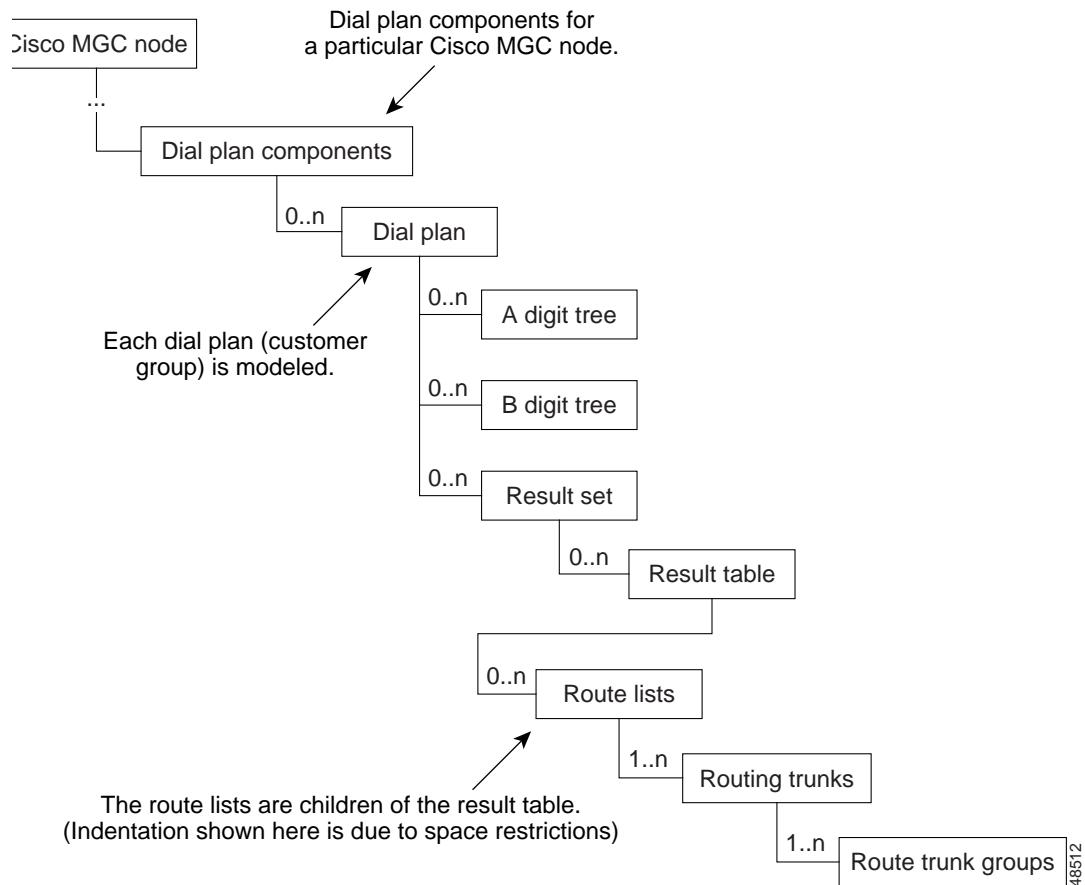
MML Type	Description
ablack	Calling number not to be processed
adigtree	Entries for each calling (A) number
awhite	Calling number to be processed
bblack	Called numbers not to be processed
bdigtree	Entries for each called (B) number
bwhite	Called numbers to be processed
carriertbl	Carrier selection table (8.x only)
cause	Cause analysis
dialplan	Represents an MML dialplan
digmodstring	String of numbers to apply to an A or B-number
location	Type of network that originates call
noa	Nature of address
npi	Numbering plan indicator
porttbl	Ported number table (8.x only)

Table 1-4 Classes Representing Dial Plan Objects

MML Type	Description
resultset	Result set table
resulttable	Result of number analysis
rtlist	Route list
rttrnk	Routing trunk
rttrnkgrp	Routing trunk group
service	User-defined services for screening
termtbl	Number termination table (8.x only)

Containment Hierarchy of the Dial Plan Objects

When CMNM retrieves the current configuration from the active Cisco MGC host, it establishes the containment hierarchy of the dial plan objects. A hierarchical model example is shown in Figure 1-9.

Figure 1-11 Hierarchical Model Example of Dial Plan Objects

Overview of Event Manager

There are three component parts to the Event Manager :

- Thresholding Regimes
- Notification Profiles
- Event Groups

The following sections provide an overview of these components.



Note For detailed information on using Notify, Thresholds, and Event Groups, see the *Cisco Element Management Framework User Guide, Version 3.1*.

Thresholding Regimes

Thresholding is the ability to configure the management system to actively monitor the network and notify the operator when some aspect of the network performance has deviated from preset criteria.

Normally an operator would wish to apply some standard set of criteria to an entire set of objects as part of a management policy. An example policy might be:

```
Poll all routers every 15 minutes and check if their CPU utilization is higher than 80%.
If it is higher than this, then raise a warning alarm on the routers that breach this
condition.
```

If the operator then decided that the polling rate should be ten minutes or that the threshold should be 70 percent, then they would not wish to have to apply this individually to, say, 5000 routers.

This is the reason for thresholding regimes. A regime is set up with the management policy to be applied and then this regime is applied to a group or groups of objects. If the policy is to be changed, then by simply changing the one central regime, the new policy will be applied to all objects within the group.

Once a threshold has been breached, the operator will want the system to notify the user or to perhaps carry out a sequence of actions. The specification of the actions to carry out is called a notification profile.

A thresholding regime has a set of trigger conditions and the set of object groups to which these trigger conditions are to be applied.

Each trigger condition is, in turn, made up of the following components :

- Expression to be checked; for example, CPU > 80%
- Frequency that the expression should be checked; for example, every 15 minutes
- Notifications profile to run when expression is satisfied

Notification Profiles

Notification profiles consist of a series of notifications that should be carried out as a result of the profile being triggered. There are a number of different types of notification available. These are:

- **Beep Once**—Produces a single beep
- **Raise Window**—Brings all windows containing the icon representing the controlling object to the front of the window stack

- **Flash Icon**—Causes the controlling object’s icon to flash in each open window that contains it
- **Beep Continuously**—Produces a continuous beep
- **Popup Dialog**—Opens a window containing a defined message
- **Play Sound**—Plays a user-defined sound
- **Run Script**—Causes a user-defined script to run
- **Raise Event**—Generates a Cisco EMF event

All of these notifications, such as run script or raise event, can be given a time delay. This allows a simple form of escalation process to be implemented. For example:

- When notification profile is triggered, raise a minor event; if the notification profile has not been reset within 30 minutes, then raise a major alarm.

Once a notification profile is triggered a “running instance” of this profile is created. This is a copy of the profile that is taken to keep track of the current status of notifications that are active. Notification profiles can be viewed as templates that are used at trigger time to create an active running version. A user can view the state of any running notification profiles currently on an object.

Event Groups

A typical telecommunications network can generate a large volume of events. Only a small proportion of these events may be affect service or require immediate attention. Other events will still be of interest but require less urgency. In order to provide effective network management, an operator must be able to quickly identify the critical issues from the “background noise” of events.

The operator may also want to categorize the handling of these events based upon geographical location or based upon the technical knowledge of certain users.

The purpose of Event Groups is to allow the operator to easily subdivide the stream of events into manageable groups based upon user-defined filtering criteria.

This filtering can be performed by a variety of criteria such as event severity, event state, class of network element affected by the event, and so on.

For display purposes, users can then arrange these event groups onto scoreboards. Each scoreboard shows a summary box for each group, which allows the user to see the state of a group at a glance.

Having multiple scoreboards allows multiple users to keep track of different sets of events easily without being distracted by events that are of no interest to them.

In a similar way to thresholding regimes, event groups can also be configured to run notification profiles that carry out a series of actions when certain trigger conditions are satisfied. With event groups there are three possible trigger conditions:

- Invoke notification profiles when first event enters the group
- Invoke notification profiles when first event on an object enters the group
- Invoke notification profiles when any event enters the group



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 3.1 and latest patches (Patch 1 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 for the Cisco VSC 3000 and Table 2-2 for the Cisco SC2200.

Table 2-1 Hardware Requirements for CMNM Host Machine—VSC3000

	Small Network 1-3 Operators 1-5 Nodes 1 trap / sec	Medium Network 4-6 Operators 6-10 Nodes 2 traps / sec		Large Network 7-10 Operators 11-20 Nodes 4 traps / sec	
Configuration	1 machine	Application server	Management server	Application server	Management server
RAM (GB)	2	2	2	2	4
Swap (GB)	2	1	2	1	2
Disk drives (9 GB minimum)	4	1	4	1	8
CPU (MHz)	2 x 440	2 x 440	2 x 440	4 x 440	2 x 440

Table 2-2 Hardware Requirements for CMNM Host Machine—SC2200

	Small Network 1-3 Operators 1-5 Nodes 1 trap / sec	Medium Network 4-6 Operators 6-10 Nodes 2 traps / sec		Large Network 7-10 Operators 11-20 Nodes 4 traps / sec	
Configuration	1 machine	Application server	Management server	Application server	Management server
RAM (GB)	2	2	2	2	4
Swap (GB)	2	1	2	1	2
Disk drives (9 GB minimum)	4	1	4	1	8
CPU (MHz)	2 x 440	2 x 440	2 x 440	4 x 440	2 x 440

**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 and Table 2-2.

**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 files 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 2-3 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 2-4 Drive 2

Mount Point	Size
<swap>	2.0 GB
/opt	Remainder

Table 2-5 Drive 3

Mount Point	Size
/opt/CSCOcemf/db	Remainder

Table 2-6 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 2-7 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 2-8 Drive 2

Mount Point	Size
<swap>	2.0 GB
/opt	Remainder

Table 2-9 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 `rdsk` 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/rdsk/c2t9d0s0
Partition1: PARTITION /dev/rdsk/c2t10d0s0
```

```
Partition2: PARTITION /dev/rdsk/c2t12d0s0
Partition3: PARTITION /dev/rdsk/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 2-10 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 2-11.

Table 2-11 External Software Versions

External Software	Version
CEMF	3.1
Cisco MGC host software	Latest version of 7.4.10(B)/8.1(1.2)
Cisco SLT IOS SS7 image	12.0.7 XR
LAN switch code	5.4(4)

Table 2-11 External Software Versions

Voice Services Provisioning Tool	1.5
BAMS	2.63

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 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 2-3.

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.

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 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 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 2-3.

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:
- 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** 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 host name 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 2-12. 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 **./installCSCOcmmn**.
-

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 CSCOcmmn
```
- The following message should appear:
- ```
application CSCOcmmn    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 2-12.

Table 2-12 Element Managers

mgxEM	Element Manager for Cisco MGX 8260 media gateway devices
mgcEM	Common Element Manager for Cisco MGC node devices
hostEM	Element Manager for Cisco MGC host signaling, trunking, and dial plan components

- 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 Tool Versions
```

Name	Version	Patch Level	Build Num	Build Type
CSCOcmm	1.5	00	102300	REL
CSCOcmcv	5.1	00	092600	
CSCOcemfm	3.1	none		

```
CSCOcmm Element Manager Versions
```

Name	Version	Patch Level	Build Num	Build Type
hostEMm	1.5	00	102300	REL
mgcEMm	1.5	00	102300	REL
mgxEMm	1.5	00	102300	REL

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 2-13.

Table 2-13 CiscoView Packages List

CiscoView Packages	Version
Cat2900 XL	1.1
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 2-13 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.nmim.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 "CSCOcmmn" 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:
- a. Click **Connect**.
  - b. Select the appropriate XDMCP computer. If you do not know which computer to select, contact your system administrator.
- For Direct method:
- a. In the Host Name field, enter the host name of an XDMCP computer.
  - b. 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 to 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 (2611)
- LAN switch (Catalyst 2900XL and Catalyst 5500)
- Cisco MGX 8260
- BAMS

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 /etc/srconf/agt**.
- 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** Add the following line after the existing `snmpNotifyEntry` lines:
- ```
snmpNotifyEntry 32 rambler trap nonVolatile
```




---

**Note** The second field on the line (32 in the example) must be a value that is unique in the `snmpNotifyEntry` section.

---

**Step 7** Add the following line after the existing `snmpTargetAddrEntry` lines:

```
snmpTargetAddrEntry 34 snmpUDPDomain 10.1.1.1:0 100 3 rambler \
v2cExampleParams nonVolatile 255.255.255.255:0
```




---

**Note** The second field on the line (34 in the example) must be a value that is unique in the `TargetAddrEntry` section.

---

**Step 8** Save the changes you made to the `snmpd.cnf` file.

**Step 9** Determine the process ID. 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 10** Terminate and restart the SNMP daemon. Enter the command:

```
kill -9 SNMP-daemon-process-ID
```




---

**Note** The SNMP daemon restarts automatically after termination.

---

## Configuring a Cisco SLT (2611)

To configure a Cisco SLT (a Cisco 2611 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 private 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 2k by entering the command:
- ```
snmp-server packetsize 2048
```
- 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 `2900x1` 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 2900x1 prompt.

**Step 5** Enter the command **configure terminal**.

You see the 2900x1 (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.

a. To configure the LAN switch to send all types of traps, enter the command:

```
snmp-server enable traps
```

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):

```
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 2k by entering the command:

```
snmp-server packet-size 2048
```

**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.
- To configure the LAN switch to send all types of traps, enter the command:

```
set snmp trap enable
```
 - 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 2.6x for network management:

- Step 1** Access the BAMS server by entering the command:

```
telnet BAMS-server-IP-address or CiscoBAMS-server-IP-address???
```
- Step 2** Type **su - root** to become the root user.
- Step 3** Type **cd /etc/srconf/agt**.
- 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 BAMS. The entry should be:

```
sysName BAMS-server-hostname
```

Step 6 Add the following line after the existing snmpNotifyEntry lines:

```
snmpNotifyEntry 32 rambler trap nonVolatile
```



Note The second field on the line (32 in the example) must be a value that is unique in the snmpNotifyEntry section.

Step 7 Add the following line after the existing snmpTargetAddrEntry lines:

```
snmpTargetAddrEntry 34 snmpUDPDomain 10.1.1.1:0 100 3 rambler \
v2cExampleParams nonVolatile 255.255.255.255:0
```



Note The second field on the line (34 in the example) must be a value that is unique in the TargetAddrEntry section.

Step 8 Save the changes you made to the snmpd.cnf file. Save the changes you made to the snmpd.cnf file.

Step 9 Determine the process ID. 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/BAMS/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 10 Terminate the SNMP daemon. Enter the command:

```
kill -9 SNMP-daemon-process-ID
```



Note The SNMP daemon restarts automatically after termination.



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.
- **Notify**—You can create notification profiles that consist of a series of notifications that should be carried out as a result of the profile being triggered.
- **Thresholds**—You can configure the management system to actively monitor the network and notify the operator when some aspect of the network performance has deviated from preset criteria.

- Event Grps—Event Groups allow the operator to easily subdivide the stream of events into manageable groups based upon user-defined filtering criteria.



Note For information on using Notify, Thresholds, and Event Groups, see the *Cisco Element Management Framework User Guide*, Version 3.1.

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
Ctrl + Q	Quit
Ctrl + W	Close
Ctrl + P	Print
Ctrl + S	Save
Ctrl + N	New
Ctrl + O	Open

Table 4-2 Edit Menu Short Cut Keys

Key Sequence	File Menu Function
Ctrl + Z	Undo
Ctrl + X	Cut
Ctrl + C	Copy
Ctrl + V	Paste
Ctrl + A	Select all
Ctrl + D	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 that 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.
-

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 that 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 that 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 pull-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

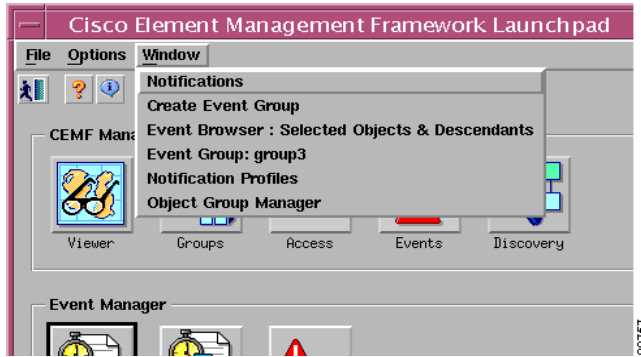


Select **Enable Tooltips** to display text associated with icons as the cursor passes over them.

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 Pull-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.

Table 5-1 Feature Lists in CMNM

Feature List	Permissions ¹	Description
AccessManagement	RWA	Set up users, user groups, assign passwords, and define access params.
AutoDiscovery	RW	Launch the auto-discovery services
Change Password	RWA	Change passwords
Deployment	RW	Deploy sites, regions, and network (generic object deployment)
EventGroupEditFeatureList	RW	Create and edit event groups
EventGroupViewFeatureList	R	View existing event groups
Events-View	R	Launch the event browser in read-only mode
Events-Clear_Acknowledge	RW	Allow user to clear and acknowledge events
GenericConfigApplication	RWA	Launch the object configuration utility
Help	R	Launch online help
Host-Dialplan-Properties	R	View properties of Cisco MGC host dial plan components
Host-Signaling-Performance	RW	View performance statistics for signaling components
Host-Signaling-Properties	R	View properties of Cisco MGC host signaling components
Host-Trunking-Properties	R	View properties of Cisco MGC host trunking components
Launchpad	R	Use the CEMF launchpad (start a CEMF session)
MGC-Node-Accounts	RWA	Change the passwords, login IDs, and SNMP community strings
MGC-Node-Diagnostics	RW	Run diagnostic tools on Cisco MGC node components
MGC-Node-Filesystems	RW	View file system information on BAMS and Cisco MGC host devices
MGC-Node-Properties	R	View properties of Cisco MGC node components
MGC-Node-Provisioning	RW	Deploy all Cisco MGC node components (either manually or via a seed file)
MGC-Node-States	RW	Change the states of Cisco MGC node components
MGC-Node-Tools	RW	Launch Cisco MGC node component tools
MGC-Node-Transfer	RWA	Performance configuration and image upload and download
MGC-Node-Trap-Forwarding	RWA	Configure trap forwarding destinations
MGX-Accounts	RWA	Change the passwords, IDs, and SNMP info for Cisco MGX 8260 components
MGX-Properties	R	View properties of Cisco MGX 8260 components
MGX-Provisioning	RW	Deploy Cisco MGX 8260 components
MGX-States	RW	Change the states of Cisco MGX 8260 components

Table 5-1 Feature Lists in CMNM

Feature List	Permissions ¹	Description
MGX-Tools	RW	Launch Cisco MGX 8260 component tools
MGX-Trap-Forwarding	RWA	Configure trap forwarding destinations
NotificationEditFeatureList	RW	Create and edit notification profiles
NotificationViewFeatureList	R	View existing notification profiles
ObjectGroups-Edit	RW	Create and edit object groups
ObjectGroups-View	R	View existing object groups
Performance Management	RW	Open the Performance Manager utility
ThresholderEditFeatureList	RW	Allow user to define and edit thresholds
ThresholderViewFeatureList	R	Allow user to view existing thresholds
Viewer-Edit	RW	Use the map viewer in read-write mode
Viewer-View	R	Use the map viewer in read-only mode

1. Use this column to determine the permissions you want to assign to various types of users. For more information, see the “Creating Typical Types of Users” section on page 5-16.

**Note**

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

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 that 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 nonadministrative 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)

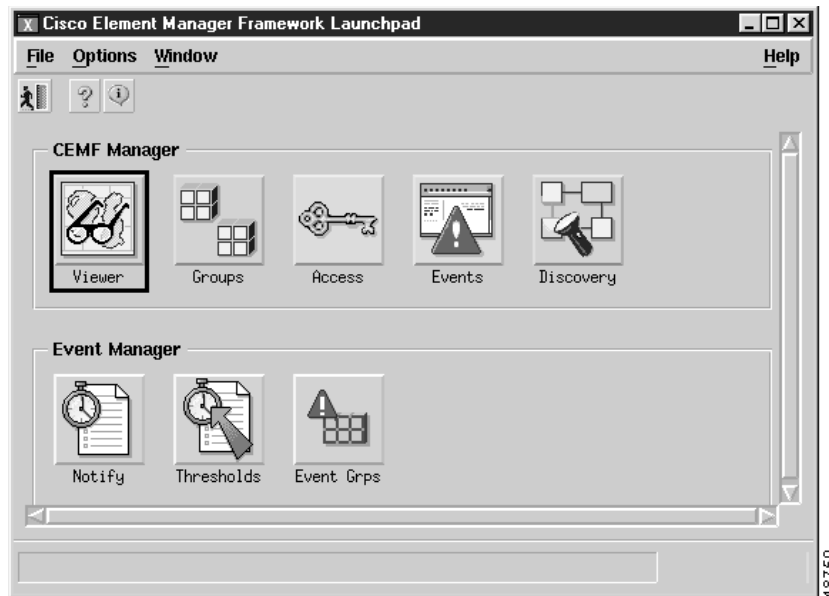
Setting Up New Accounts

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.

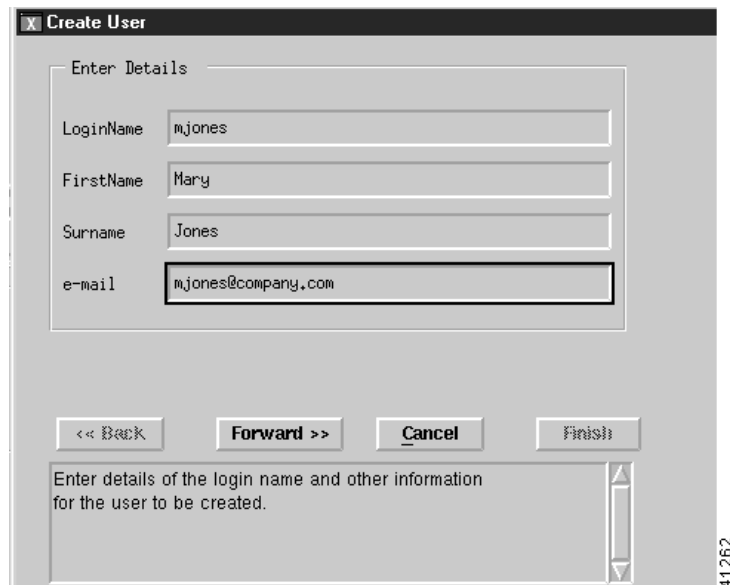
- Step 2** From the Access Manager screen, select **Edit**, **Create**, then **User** as shown in Figure 5-2.

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



You see the screen in Figure 5-3.

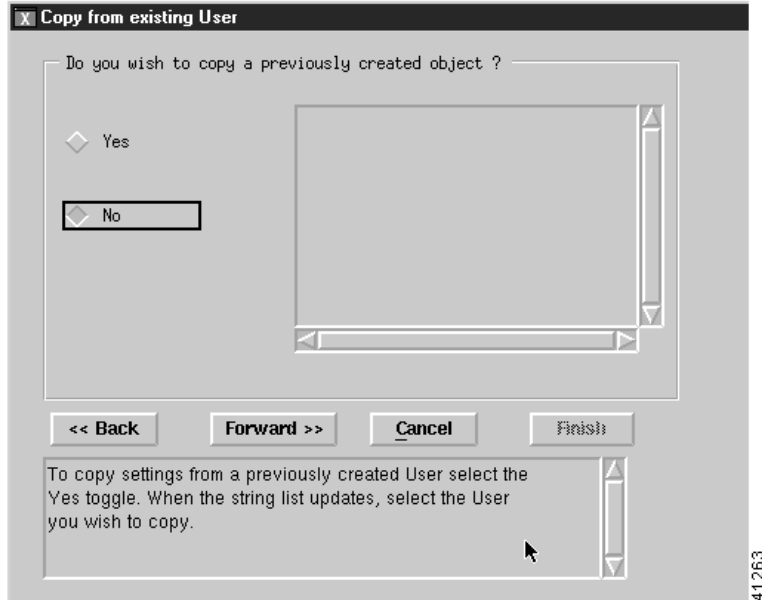
Figure 5-3 Create User Screen



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

You see the screen in Figure 5-4.

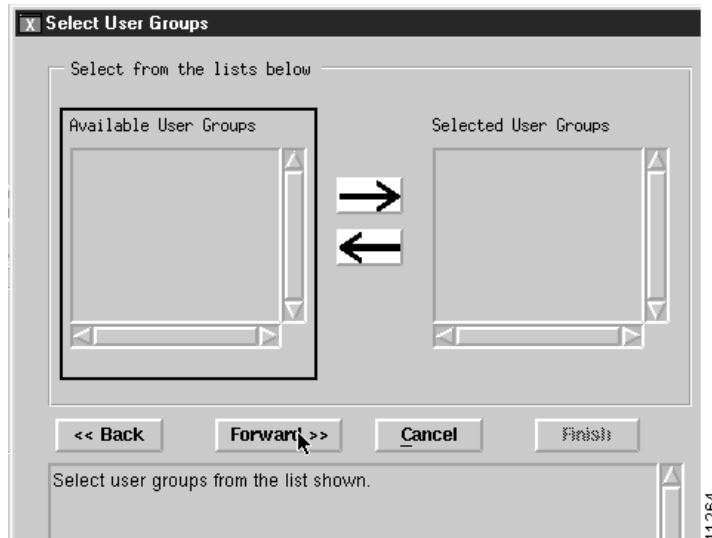
Figure 5-4 Copy from existing User Screen



- 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 Selected 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 “Creating User Groups” section on page 5-8.

You see the screen in Figure 5-6.

Figure 5-6 User Password Entry Screen

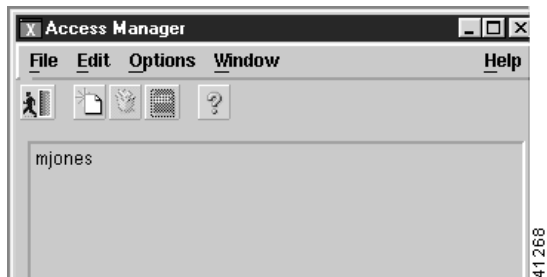
- Step 6** Enter a password for the user and confirm it. Passwords must contain 8 to 32 alphanumeric characters and at least one punctuation character such as `_`, `%`, `()`, or `^`. Click **Forward**.

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

To divide users into groups by creating user groups:

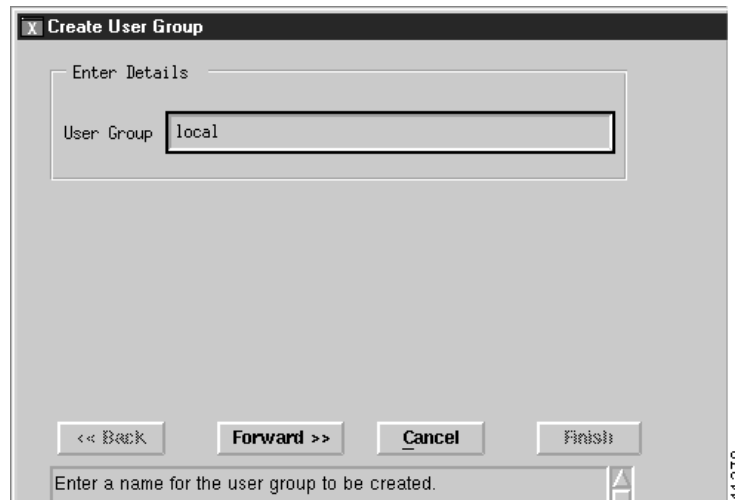
- Step 1** From the Access Manager screen, select **Edit**, **Create**, then **User Group** as shown in Figure 5-9.

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



You see the screen in Figure 5-10.

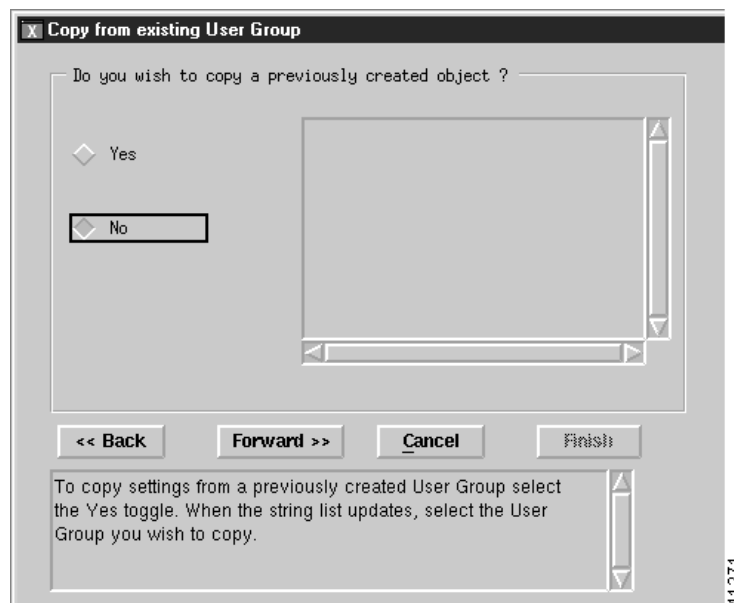
Figure 5-10 Create User Group Screen



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.

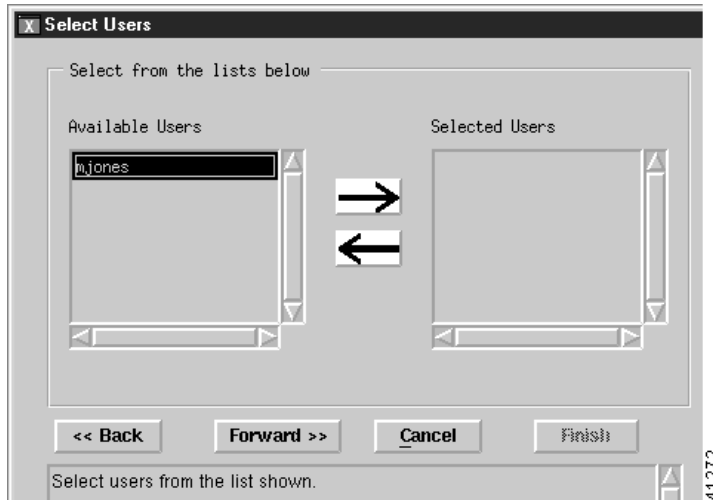
Figure 5-11 Copy from existing User Group Screen



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.

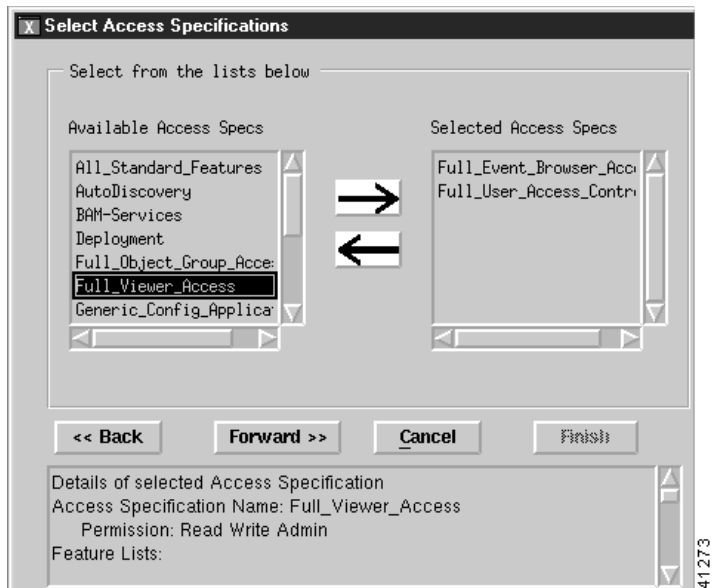
Figure 5-12 Select Users Screen



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 Specs list. When you are finished, click **Forward**.

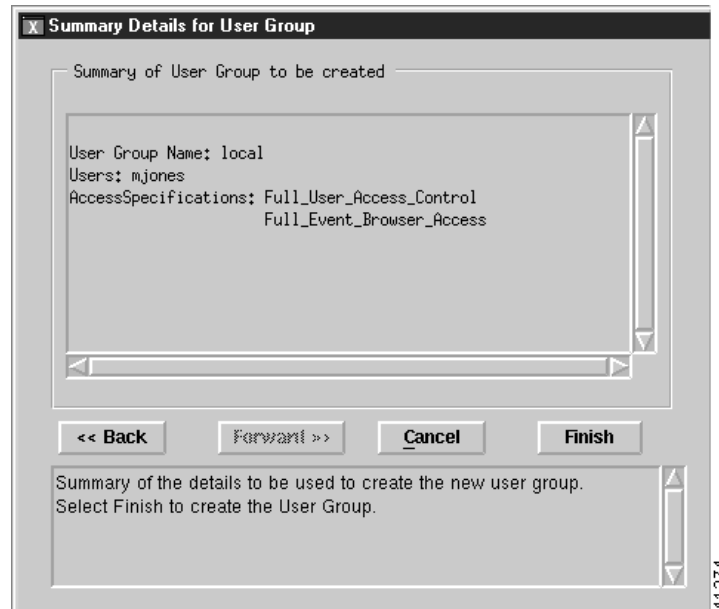

Caution

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.

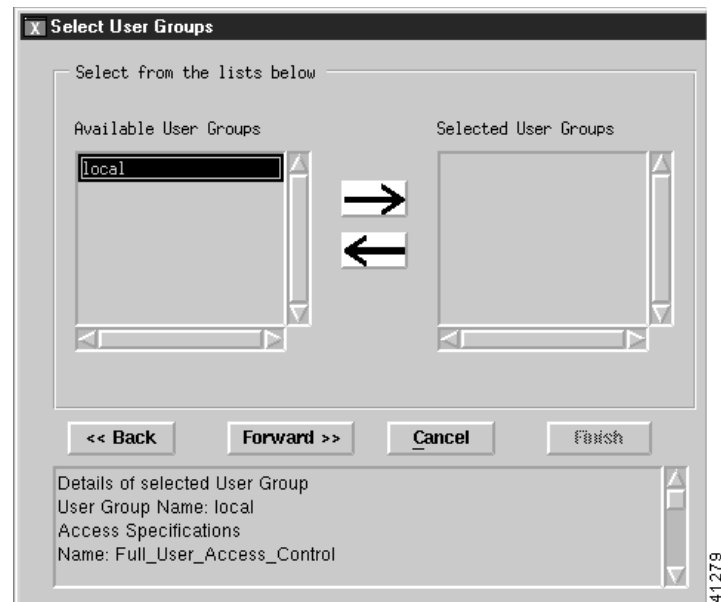
Figure 5-18 Select Permission Screen



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

You see the screen in Figure 5-19.

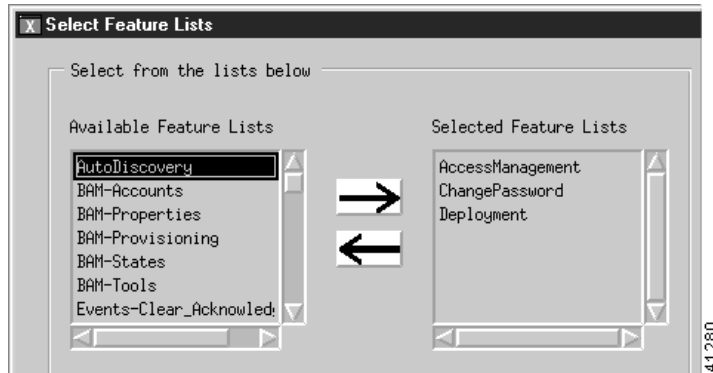
Figure 5-19 Select User Groups Screen



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.

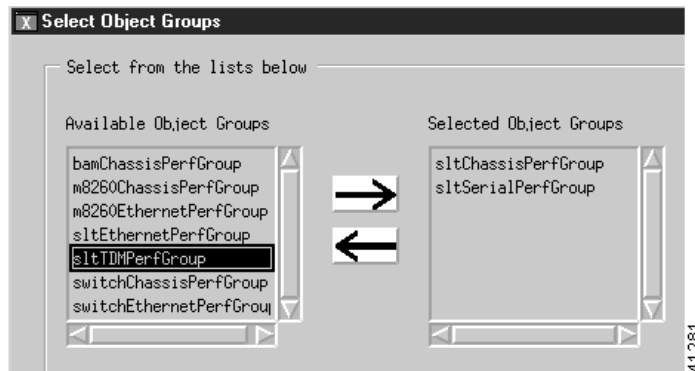
Figure 5-20 Select Feature Lists Screen



Step 6 Select each feature you want for the new access specification and click the right arrow to move each to the Selected Feature Lists. 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. The administrator should have all the features labeled with the permissions R, RW, and RWA in Table 5-1.
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 features labeled with the permissions R and RW in Table 5-1.</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 the user 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 features labeled with the permission R in Table 5-1.</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 the user to the group you just created.</p>

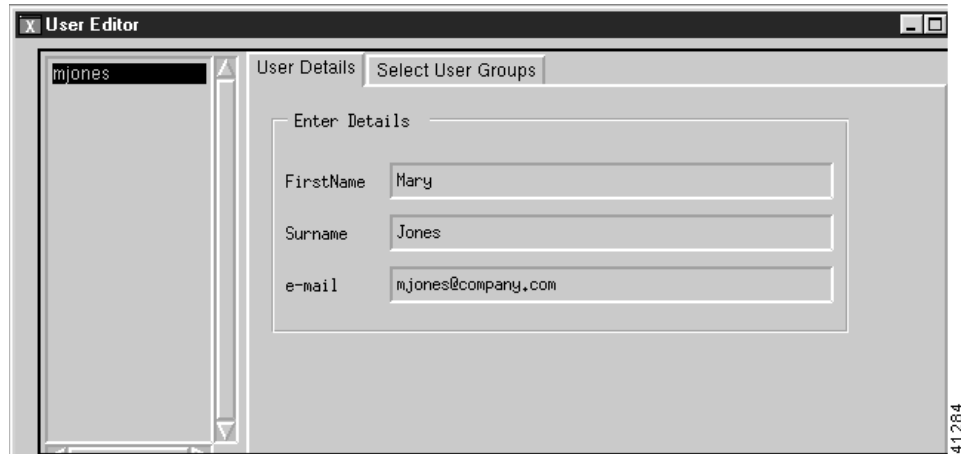
Modifying Users

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



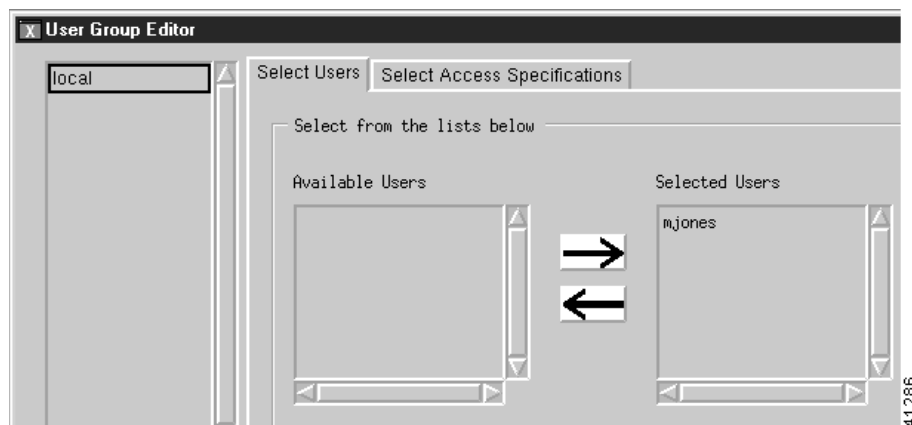
- Step 2** Select a user from the list and change any information in the fields. To change the user groups that the user belongs to, click the **Select User Groups** tab and make any changes.
- Step 3** Click **Apply**. To cancel changes, click **Revert**.

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.

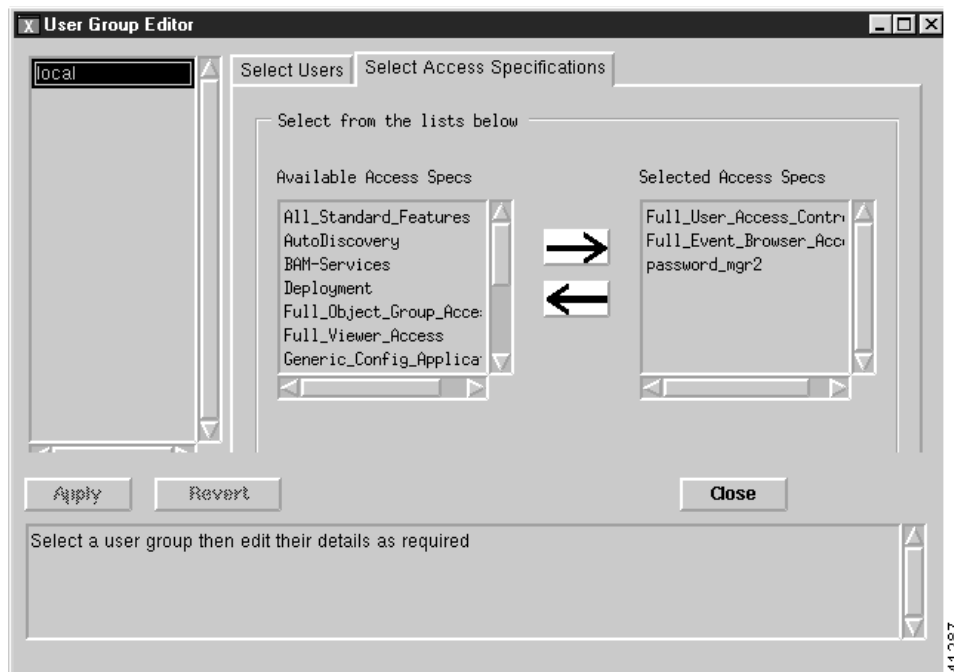
Figure 5-24 User Group Editor Screen—Select Users Tab



- 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



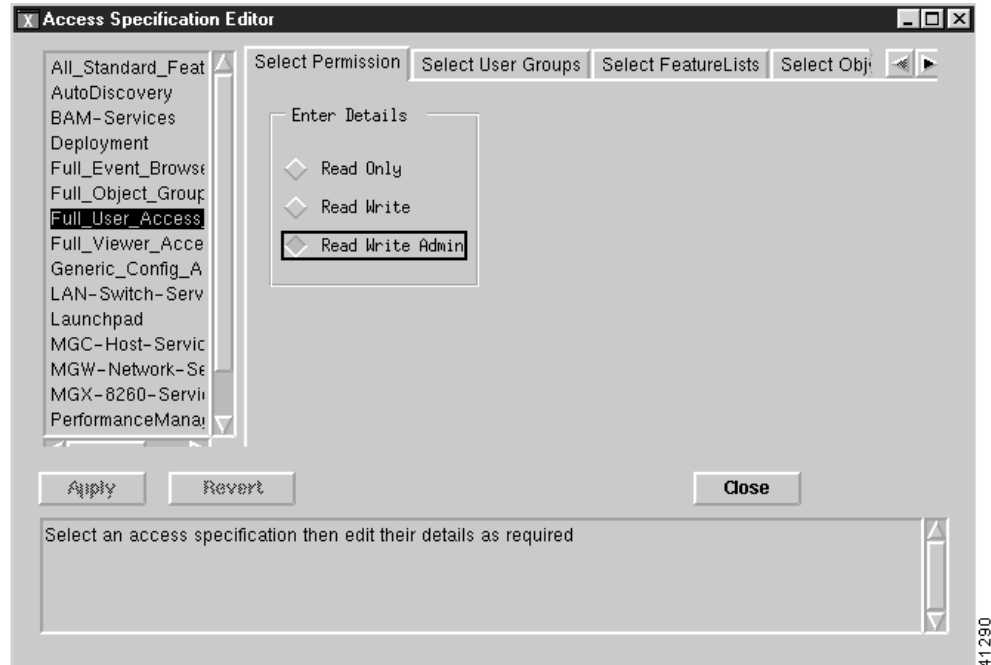
- Step 4** Select access specifications and click the arrows to add or remove access specifications from the group.
- Step 5** Click **Apply**. To cancel changes, click **Revert**.

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.

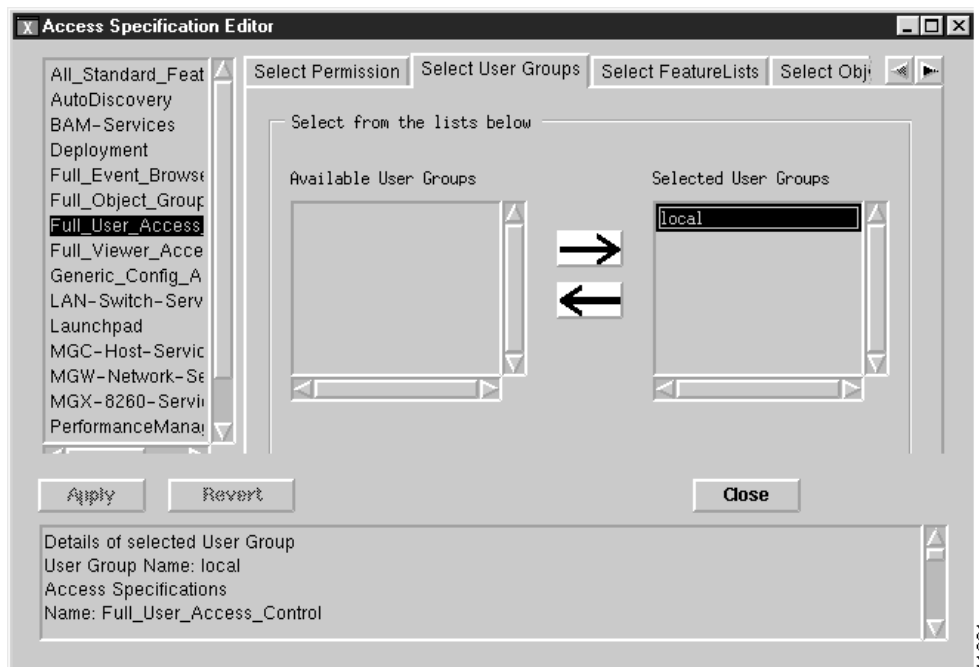
Figure 5-26 Access Specification Editor Screen—Select Permission Tab



41290

- 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.

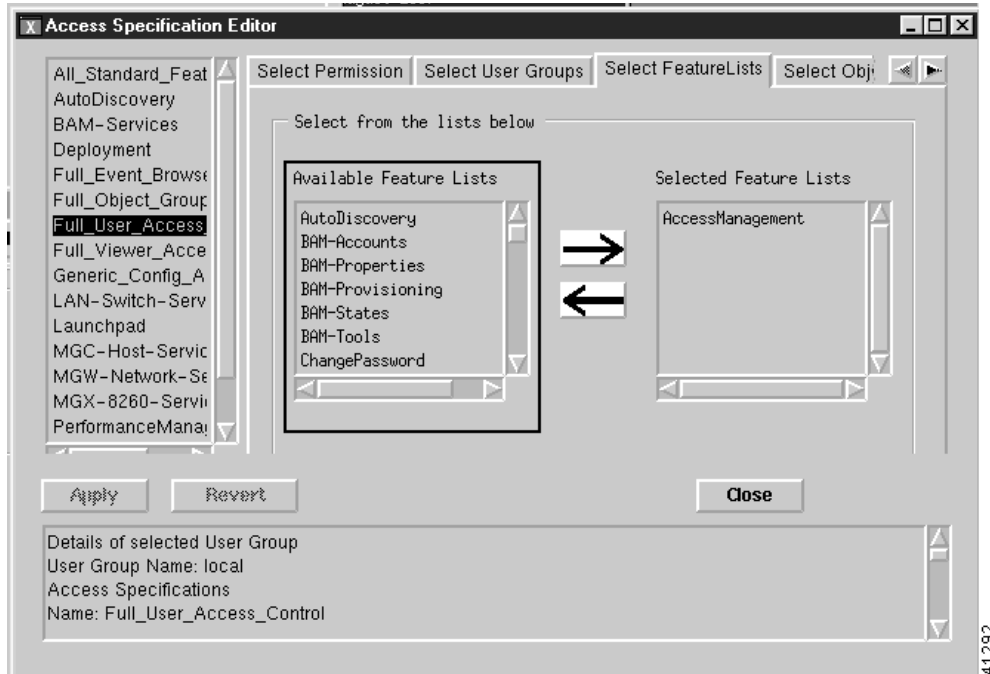
Figure 5-27 Access Specification Editor Screen—Select User Groups Tab



41291

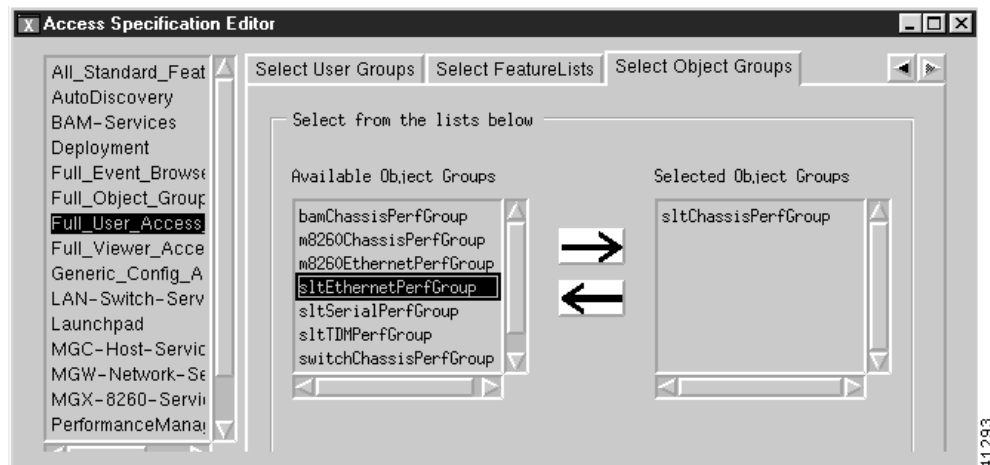
- Step 6** Select user groups and click the arrows to add or remove users groups from the access specification.
- Step 7** Click the **Select Feature Lists** tab.
You see the screen in Figure 5-28.

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.

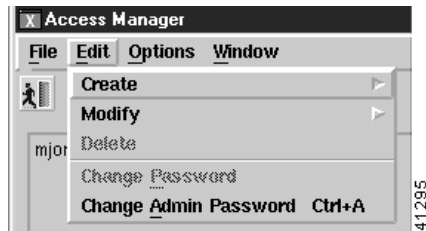
Step 12 When you are finished, click **Apply**. To discard changes, click **Revert**. Click **Close**.

Changing the Administrative Password

To change the administrative password:

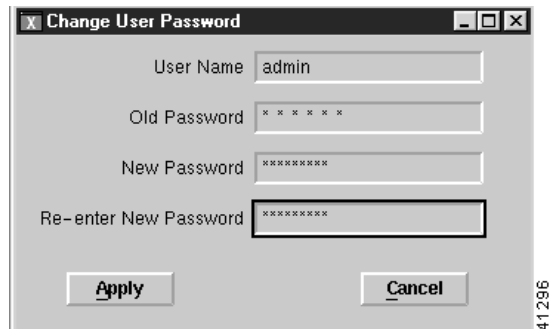
Step 1 From the Access Manager screen, select **Edit**, then **Change Admin Password**, as shown in Figure 5-30.

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.

You can also manage software images and configurations on the Cisco MGC node devices. For more information, see the “Managing Software Images and Configurations” section on page 6-16.

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 will 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.

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.

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 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
- The physical location of the device

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

Example 6-1 Sample Seed File

```
MGC (name=mgc1, location=Raleigh) {
  HOST (ip=191.34.44.2, login=transpath)# Hosts
  HOST (ip=191.34.44.3, password=lab)
  2600 (ip=191.34.44.4, name=joe, read=public, location=SanJose)
  2600 (ip=191.34.44.5, name=bob)
  2900XL (ip=191.34.44.6)# LAN Switch
  5500 (ip=181.33.44.7, write=private)
}
BAMS (ip=181.33.44.8, name=bambam, location=Chicago)
BAMS (ip=181.33.44.9, name=pebbles, location=St-Louis)
MGC (name=mgc2) {
  HOST (ip=191.44.55.78, read=public, write=private)
  2600 (ip=191.44.55.80)# SLTs
  2600 (ip=191.44.55.81, location=Boston)
  # Switches
  2900XL (ip=191.44.55.82, name=tex, location=Boston)
  5500 (ip=191.44.55.83)
}
```

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 6-1.

Table 6-1 Seed File Attributes

Attribute	Device Types	Required	Description
name	All	Only on Cisco MGC node and BAMS	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 log in to the device

Table 6-1 Seed File Attributes

rootPassword	Cisco MGC host, BAMS	No	Root (super-user) password for the device
enablePassword	Cisco 2611, 2900XL, 5500	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
location	All	No	Physical location of the device

Each Cisco MGC node can have, at most, one active host. You can define a maximum of two hosts per Cisco MGC node, 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 MGC-Node-View node or other type of CEMF object. 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.

Physical Location Field

When a device is deployed, it is placed into the Physical containment tree based on the physical location of the devices. That is, all devices in Chicago are placed under a region or site object named Chicago. When generating the seed file, you use the location attribute to specify where in the Physical containment tree each device should be deployed.

If you do not specify a physical location (the location attribute is optional), the objects are deployed in the same location as its logical parent. Otherwise, the object is deployed in a site named Default. If you specify a physical location, the devices are deployed under that object accordingly. If the specified location does not exist, CMNM automatically deploys a region object with the specified location name.

Cisco MGC node objects are not physical devices and, as such, are not deployed into the Physical containment tree. However, the seed file lets you specify a location for Cisco MGC nodes. This is done so dependent children of the Cisco MGC node can, by default, be placed in the specified location. For example, assume that you specify that a Cisco MGC node is in the site Cincinnati. All of its children that do not specifically specify a location are, by default, placed in the Cincinnati site.

Specifying a Deployment Seed File

To deploy a network using a seed file:

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

**Note**

Only one Cisco MGC node can be deployed at a time. Each requires a separate seed file.

You see the screen in Figure 6-1.

Figure 6-1 Deploy Network Screen—Seed File Tab

	MGC Host	SLT	LAN Switch	BAMS
Login ID:	mgcusr			accc
Password:				
Enable Password:				
Read Community:	*****	*****	*****	*****
Write Community:	*****	*****	*****	*****

- Step 3** Enter a filename in the seed file Filename field.
- 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.
- Step 5** To enter advanced information, click the **Advanced** tab.
- You see the screen in Figure 6-2.

Figure 6-2 Deploy Network Screen—Advanced Tab

Step 6 You can enter SNMP configuration parameters. You can also export the current configuration as a seed file or an inventory file.

An inventory file contains a description of all of the devices in the Cisco MGC network, including:

- IP address
- Hardware type
- Operating system and software versions

The inventory file lists all of the Cisco MGC node devices in the network. For each Cisco MGC node device, information about each sub-device in the node is listed. For example:

```
MGC (name=node1) {
HOST(name=host1,ip=1.2.3.4,os=Solaris 2.6,...)
2600(name=slt1,ip=3.4.5.6,os=IOS 12.3,image=boot3.1b,...)
5500(name=sw1,ip=2.3.4.5,os=CATOS 5.3,image=rboot3,...)
BAM(name=bam1,ip=5.6.4.3,os=Solaris 2.6,...)
}
MGC (name=node2) {
...
}
```

The attributes exported for the various device types are shown in Table 6-2.

Table 6-2 Inventory Export Attributes

Attribute	Types	Description
name	All	Name of the object in the CEMF display
ip	All except Cisco MGC	IP address of the device
os	All except Cisco MGC	Operating system name and version
boot	Cisco SLT/LAN switch	Name of the OS boot image
hostID	Cisco MGC host/BAMS	Solaris host ID
hostName	Cisco MGC host/BAMS	Name of the host

Step 7 When you are finished, click the **Seed File** tab to return to the screen in Figure 6-1 and click **Deploy**. You see the screen in Figure 6-3.

Figure 6-3 Deploy Confirmation Prompt

Step 8 Click **Yes**.
The network is deployed.

Manually Deploying a Site, Object, or Network

The deployment wizard is the graphical user interface (GUI) 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 6-3 describes deployment attributes.

Table 6-3 *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 node	Yes	IP address of the network element
Login	Cisco MGC host, Cisco SLT, LAN switch, BAMS	Yes for Cisco MGC host	Login ID for the device
Password	Cisco MGC host, Cisco SLT, LAN switch, BAMS	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, BAMS	Yes	IOS/Catalyst enable password
Read Community	All except Cisco MGC node	Yes	SNMP read-community string
Write community	All except Cisco MGC node	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 Cisco MGC Node

To deploy a Cisco MGC node:

-
- Step 1** Open the Map Viewer window.
 - Step 2** Click to select a MGC-Node-View icon from the left panel of the Map Viewer window.
 - Step 3** Right-click the **MGC-Node-View** icon, select **Deployment**, then **Deploy MGC Node**, as shown in Figure 6-5.

Figure 6-5 *Map Viewer Screen—Deployment>Deploy MGC Node Option*



You see the screen in Figure 6-6.

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



Step 4 Enter the name of the Cisco MGC node (no spaces). Click **Forward**.

You see a screen that summarizes the deployment you have created and allows you to commit or reject the deployment.

Step 5 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 6 Deploy Cisco MGC hosts by following the instructions in the “Deploying a Cisco MGC Host” section on page 6-10.

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

Deploying a Cisco MGC Host

- Step 1** Open the Map Viewer window.
- Step 2** Expand the MGC-Node-View icon and click to select a Cisco MGC node icon from the left panel of the Map Viewer window.
- Step 3** Right-click the **MGC node** icon and select **Deployment**, then **Deploy MGC Node Component**.
- Step 4** Click **Deploy an MGC Host** and click **Forward**.
- Step 5** Enter data for the host. See Table 6-3 on page 6-7 for descriptions of the fields. Click **Forward**.
- Step 6** Select a relationship and click **Forward**.
- 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** Expand the MGC-Node-View icon and click to select a Cisco MGC node icon from the left panel of the Map Viewer window.
- Step 3** Right-click the **MGC node** icon and select **Deployment**, then **Deploy MGC Node Component**.
- Step 4** Click **Deploy an SLT** and click **Forward**.
- Step 5** Enter data for the Cisco SLT. See Table 6-3 on page 6-7 for descriptions of the fields. Click **Forward**.
- Step 6** Select a relationship and click **Forward**.
- Step 7** 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** Expand the MGC-Node-View icon and click to select a Cisco MGC node icon from the left panel of the Map Viewer window.
- Step 3** Right-click the **MGC node** icon and select **Deployment**, then **Deploy MGC Node Component**.
- Step 4** Click **Deploy a 2900 XL Switch** or **Deploy a Catalyst 5500 Switch** and click **Forward**.
- Step 5** Enter data for the LAN switch. See Table 6-3 on page 6-7 for descriptions of the fields. Click **Forward**.
- Step 6** Select a relationship and click **Forward**.
- Step 7** 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 MGC-8260-View icon from the left panel of the Map Viewer window.
- Step 3** Right-click the **MGC-8260-View** icon and select **Deployment**, then **Deploy MGX 8260**.
- Step 4** Enter data for the media gateway. See Table 6-3 on page 6-7 for descriptions of the fields. Click **Forward**.
- Step 5** Select a relationship and click **Forward**.
- Step 6** Click **Finish**.

A 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 BAMS-View icon from the left panel of the Map Viewer window.
- Step 3** Right-click the **BAMS-View** icon and select **Deployment**, then **Deploy BAMS**.
- Step 4** Enter data for the BAMS server. See Table 6-3 on page 6-7 for descriptions of the fields. Click **Forward**.
- Step 5** Select a relationship and click **Forward**.
- Step 6** Click **Finish**.

An icon appears on the right pane of the Map Viewer window.

Subrack Discovery

When a Cisco SLT, LAN switch, Cisco MGC host, or BAMS is deployed, its subrack components are queried and deployed. The types of subrack components, as well as their relationships, differ based on the type of device.

CMNM performs the subrack discovery of various types of devices. When a device is deployed, CMNM checks the OID of the device. If possible, CMNM performs custom subrack discovery based on the device type. Otherwise, a generic discovery mechanism is used.

The various subrack discovery mechanisms are described in the following sections.



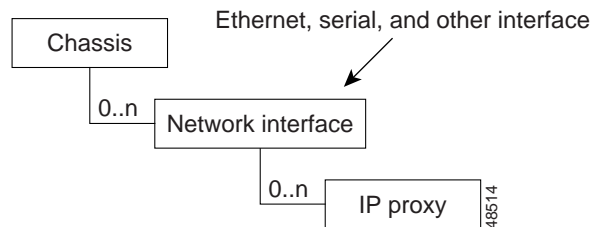
Note

CMNM automatically discovers each device at an interval you may specify and keeps track of the time that each device was last discovered. When the specified interval has elapsed, CMNM automatically rediscovers the device.

Cisco MGC Host and BAMS Discovery

The Cisco MGC host and BAMS discovery mechanism processes the ifTable of the device and deploys an object to represent each (supported) interface. BAMS also uses the CIAgent system component discovery mechanism. In addition, an object representing each (non-loopback) IP address is deployed as a child of its corresponding interface as shown in Figure 6-7.

Figure 6-7 Cisco MGC Host and BAMS Discovery



This subrack discovery mechanism is used for the Cisco MGC host, BAMS, and any unknown or unsupported device that is deployed.

CIAgent System Component Discovery

For devices that support the CIAgent SNMP Agent (Cisco MGC host and BAMS), components are deployed that represent logical components of the UNIX system, as shown in Table 6-4

Table 6-4 Components Deployed

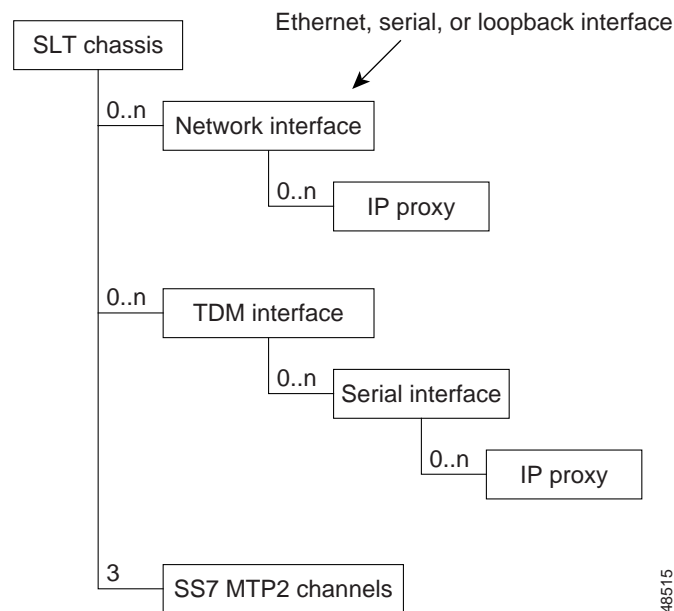
Component Type	Description
RAM	Physical RAM in the UNIX machine
virtualmem	Virtual memory storage
Fixed disk	Local (non-ncs mounted) disk drive
Processor	Processor (CPU)

Cisco SLT Discovery

The Cisco 2611 series auto-discovery mechanism expands slightly on the Cisco MGC host and BAMS discovery mechanism. First, all TDM (DS1) interfaces are deployed. Second, in a non-V.35 configuration, serial interfaces are placed under their dependent TDM interface. IP address objects are deployed under their corresponding interface.

CMNM also models the three SS7 MTP2 channels on each Cisco SLT. From these channels, you can view current SS7 MTP2 statistics.

Figure 6-8 Cisco SLT Chassis Discovery



Cisco 2900XL Discovery

CMNM models ports and modules (slots) on the Cisco 2900XL series devices. The Cisco 2900 XL has 24 ports built into the chassis. In addition the Cisco 2900XL has two slots into which different cards can be installed.

During auto-discovery, CMNM retrieves the tables shown in Table 6-5.

Table 6-5 Cisco 2900XL Discovery Tables

Table	Description
CISCO-C2900-MIB.c2900ModuleTable	Contains all of the module (slot) information
CISCO-C2900-MIB.c2900PortTable	Defines all of the ports on the chassis
SNMPv2-MIB.ifTable	Defines all of the interfaces on the chassis
RFC1213-MIB.ipAddrTable	Lists all of the IP address on a port
CISCO-VTP-MIB.vtpVlanTable	Lists all VLANs on the chassis

Each entry in the `c2900ModuleTable` is modeled as a `switch2900XLSlot` object. The attribute `SNMP:CISCO-C2900-MIB.c2900ModuleIndex` serves as an index into the table.

Each entry in the `c2900PortTable` is modeled as a `switch2900XLPort` object. In the CMNM object model, it is placed under its dependent slot. The `c2900PortTable` is indexed by two attributes, the module index and the port index. The module index indicates on which slot the port resides. Module index zero indicates that the ports are dependent on the chassis, and not on a slot. The attribute `c2900PortIfIndex` is used to correlate the `c2900PortTable` to the `ifTable`.

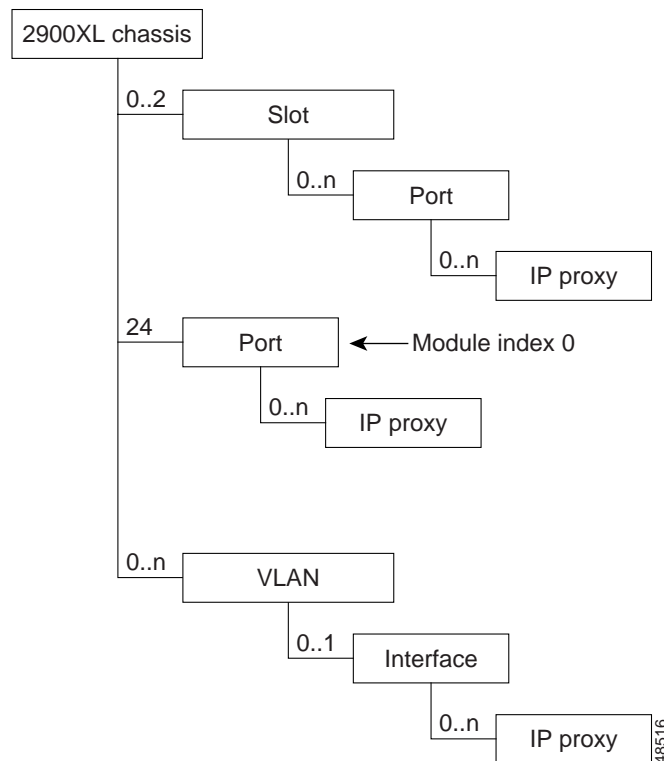
Each entry in the `vtpVLANTable` is modeled as a `switch2900XLVLAN`. In addition, each interface associated with the VLAN is displayed as children of its corresponding VLAN. In order to correlate interfaces from the `ifTable` to their corresponding VLANs in the `vtpVLANTable`, CMNM uses the description of the `ifTable` entry, which is of the form:

VLAN x

where x is the index of the corresponding entry in the `vtpVlanTable`.

The Cisco 2900XL subrack component appears as shown in Figure 6-9.

Figure 6-9 Cisco 2900XL Chassis Discovery



Catalyst 5500 Discovery

CMNM models slots, VLANs, and ports on the Catalyst 5500 series devices. During auto-discovery, CMNM retrieves the tables shown in Table 6-6.

Table 6-6 Catalyst 5500 Discovery Tables

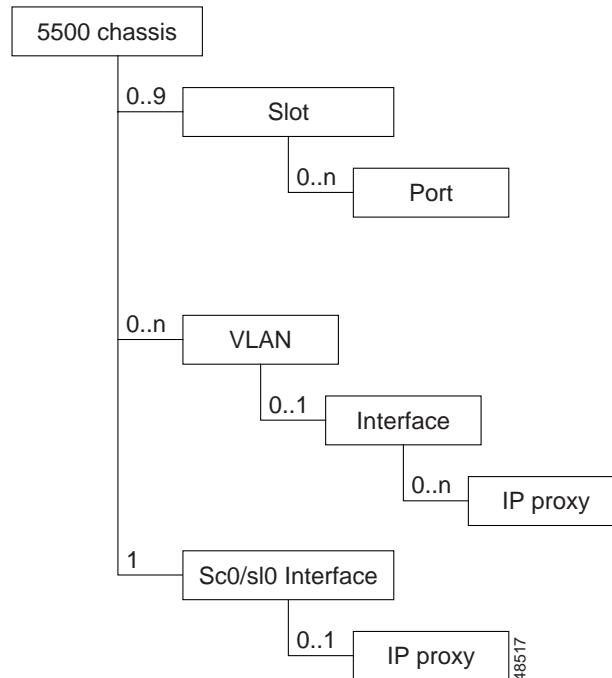
Table	Description
CISCO-STACK-MIB.moduleTable	Defines all of the modules (slots) on the chassis
CISCO-STACK-MIB.portTable	Defines all of the ports on the chassis
CISCO-STACK-MIB.vlanTable	Defines all of the VLANs on the chassis
SNMPv2-MIB.ifTable	Defines all of the interfaces on the chassis

Each entry in the moduleTable is modeled as a switch5500Slot object and every entry in the portTable is modeled as a switch5500Port object. To correlate the information, the attribute portModuleIndex defines the slot on which the port is located and the portIfIndex is used to correlate the portTable to its corresponding interface in the ifTable.

Each entry in the vlanTable is modeled as a switch5500VLAN object. The attribute vlanIfIndex associates each element in the VLAN table to its corresponding interface in the ifTable. The associated interface is shown as a child of its corresponding VLAN.

The SC0 and SL0 interfaces are modeled directly under the chassis object. In the MIB, one interface has a valid IP address while the other has an IP address of 0.0.0.0. While both interfaces are modeled, only the valid IP is shown.

The Catalyst 5500 subrack component is shown in Figure 6-10.

Figure 6-10 Catalyst 5500 Chassis Discovery

Cisco MGC Node Discovery

CMNM models and displays the trunking, signaling, and dial plan components associated with the active Cisco MGC host. When CMNM initially discovers a new Cisco MGC node, it retrieves the configuration for the active Cisco MGC host by telnetting into the active host, starting an MML session, and running the **prov-exp** command. This command puts the current configuration of the Cisco MGC host in a number of flat files as described in Table 6-7.

Table 6-7 Cisco MGC Host Export Files

Filename	Description
config.mml	MML description of all the signaling components.
export_trnkgrp.dat	Line-by-line description of each of the trunk groups.
export_trunk.dat	Line-by-line description of each of the trunks.
routing.mml	MML description of all the routing components.
XXX.mml	MML description of the dial plan components, where XXX is the customer group ID.

Once exported, the files are transferred back to the management system using FTP and are then parsed by CMNM. Hence CMNM can deploy objects that represent each of the signaling, trunking, and routing components.

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.

Managing Software Images and Configurations

CMNM lets you manage software images and configurations on the Cisco MGC node devices. You can:

- Back up (upload) the configuration of the Cisco MGC host, BAMS, Cisco SLT, and LAN switch.

- Restore (download) configuration on the Cisco MGC host, BAMS, Cisco SLT, and LAN switch.
- Download software modules and patches to Cisco MGC node devices.
- Back up (upload) software images from Cisco SLT and LAN switch.
- Automate or schedule configuration backups.

- Cancel or modify scheduled operations.
- Maintain a record of all software and configuration modifications.

The following sections detail the support for image and configuration management.

TFTP Server

CMNM uses a TFTP server to maintain software images and device configurations. All files that are downloaded to devices come from this TFTP server. Likewise, all backups from the devices are saved to the TFTP server.

The TFTP server makes use of the standard UNIX filesystem and can be maintained by anyone with the proper UNIX permissions. The system administrator is free to place new images or configurations on the server and archive or delete old software images and configurations. CMNM does not provide any explicit support for standard filesystem maintenance functions.

The location of the TFTP directory is found in the INETD configuration file `/etc/inetd.conf`. At startup, CMNM queries the contents of this file to figure out the location of the TFTP directory. By default, the directory (if the entry in the `inetd.conf` file is commented out) is `/tftpboot`.

Uploading and Downloading Cisco SLT and LAN Switch Images and Configurations

CMNM lets you move IOS images and configurations to and from the Cisco SLT and LAN switch.


The download process:

- Telnets into the select devices.
- Enters enable mode.
- Copies the configuration or image from the TFTP server:
 - copy tftp flash** (to copy software image)
 - copy tftp running-config** (to copy running configuration)
- Reboots the device (if necessary):
 - reload** (for Cisco SLT)
 - reset system** (for LAN switch)
 - confirm**

The upload process:

- Telnets into the devices.
- Enters enable mode.
- Copies the configuration or image back to the TFTP server.
 - copy flash tftp** (to copy software image)
 - copy config tftp** (to copy running Catalyst configuration)
 - copy running-config tftp** (to copy running IOS configuration)
- Copies or renames the file as specified by the user.

To upload or download Cisco SLT and LAN switch configurations:

-
- Step 1** Under MGC-Node-View, select a node, expand it, select a Cisco SLT or LAN switch, right-click the Cisco SLT or LAN switch icon, select **Tools**, then **SLT Upload/Download** or **LAN Switch Upload/Download**.
- Step 2** Select one or more devices from the list on the left of the screen.
- Step 3** In the Transfer box, enter the information about the Cisco SLT or LAN switch:
- Name of the image or configuration file on the TFTP server
 - Transfer type (configuration, image, or patch)
 - IP address, login ID, and password of the TFTP server
- Step 4** Indicate at the bottom of the screen whether the device should be rebooted.
- Step 5** If you want to schedule the transfer, enter the scheduling information in the Schedule box.
-  **Note** To see the currently scheduled transfer operations, click the **Current** tab.
-
- Step 6** When you have finished, click **Download** or **Upload** as appropriate.
-

Uploading and Downloading Cisco MGC Host and BAMS Images and Configurations

CMNM lets you upload and download Cisco MGC host configurations to a Cisco MGC host. You can upload BAMS configurations.

The Cisco SLT and LAN switch configurations and images are in a single file. The Cisco MGC host and BAMS configurations and patches are in many different files and directories. Hence when you specify a configuration on the TFTP server, CMNM assumes it is a directory containing all of the necessary data:

- MGC Host configurations are specified as a directory containing an MML batch-file along with supporting files (like the output from the Voice Services Provisioning Tool).
- MGC Host software patches are specified as a directory containing the software image to be installed. The installation script must be in this directory.

The download process performs a number of different steps depending on the type of device and data. In general, the following steps are performed:

- Telnets into the devices.
- Copies the configuration or patch from the TFTP server to the device.
- Runs the installation script to install the new software or runs whatever utility is necessary to load a new configuration.
- Activates the configuration or image (if necessary). This may involve rebooting the device.

Voice Services Provisioning Tool does not let you upload software images. CMNM lets you upload configuration data only from the Cisco MGC host and BAMS.

The configuration upload process performs the following steps:

- Telnets into devices.
- Extracts the current configuration (using, for example, the **prov_exp** command)

- Copies the configuration to the TFTP server.


When downloading a patch to a Cisco MGC host, CMNM performs the following steps:

- Warns you that the Cisco MGC host software will be shut down during the upgrade.
- Retrieves the patch from the TFTP repository.
- Copies the patch to the target Cisco MGC host:
 - Ensures that enough disk space is available.
 - Uses /var/tmp as the temporary storage location.
- Telnets to the target Cisco MGC host (as root for pkgadd privileges)
- Stops the Cisco MGC host daemons:
 - /etc/init.d/CiscoMGC stop
 - Waits until the processes physically stop (using UNIX ps).
- Installs the software:


```
pkgadd -n -d .pkgfile
```
- Runs pkginfo to ensure the package was installed correctly.
- Starts the Cisco MGC host daemons:


```
/etc/init.d/CiscoMGC start
```
- Ensures that the processes actually started (using UNIX ps).

To upload or download Cisco MGC host configurations or upload a BAMS configuration:

-
- Step 1** Under Host-View, select a host, right-click the host icon, select **Tools**, then **MGC Host Upload/Download** or under BAMS-View, select a BAMS, right-click the BAMS icon, select **Tools**, then **BAMS Upload/Download**.
- Step 2** Select one or more devices from the list on the left of the screen.
- Step 3** In the Transfer box, enter the information about the Cisco MGC hosts or BAMS:
- Name of the directory on the TFTP server containing the configuration files or name of the directory on the TFTP server where the configuration is to be stored
 - Transfer type (configuration, image, or patch)
 - IP address, login ID, and password of the TFTP server
- Step 4** If you want to schedule the transfer, enter the scheduling information in the Schedule box.
-  **Note** To see the currently scheduled transfer operations, click the **Current** tab.
-
- Step 5** When you have finished, click **Download** or **Upload** as appropriate.
-



Using Polling to Monitor Network Performance

Introduction to Performance Monitoring

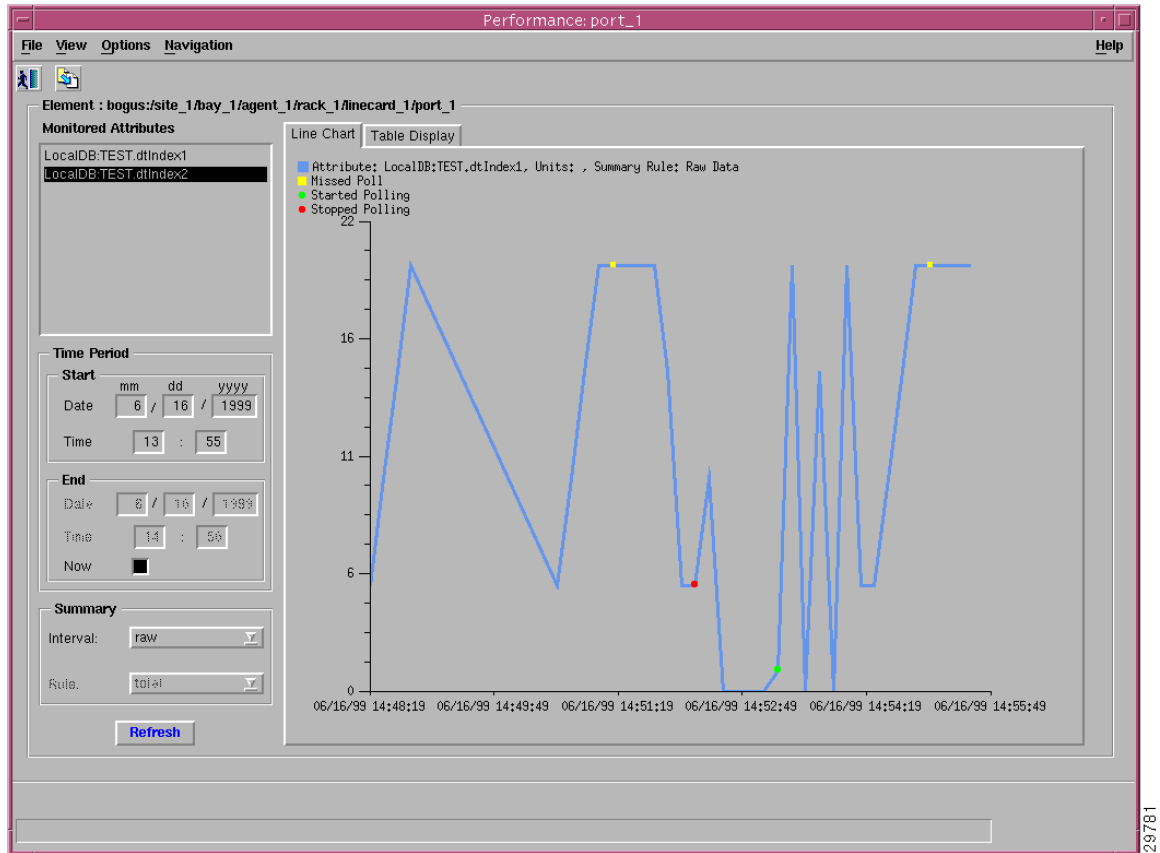
An important component of efficient network management is the ability to receive performance information on a large network of many devices to provide an overall view of the your network's functioning. You can then proactively manage your network elements by analyzing the performance data.

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 that 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 want 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 that 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.

Common Performance Data Collected for Several Devices

Many devices collect the same performance data. Common performance attributes are listed in Table 7-1, Table 7-2, and Table 7-3 and referenced in the following sections.

Table 7-1 IP Performance Counters

Counter	Description
SNMP:RFC1213-MIB.ipInReceived	Number of input datagrams received from interfaces, including those received in error.
SNMP:RFC1213-MIB.ipInHdrErrors	Number of input datagrams discarded due to errors in their IP headers including bad checksums.
SNMP:RFC1213-MIB.ipInAddrErrors	Number of input datagrams discarded because of invalid IP header destination address.

Table 7-1 IP Performance Counters

SNMP:RFC1213-MIB.ipForwDatagrams	Number of input datagrams for which this entity was not their final IP destination.
SNMP:RFC1213-MIB.ipInUnknownProtos	Number of locally addressed datagrams discarded because of an unknown or unsupported protocol.
SNMP:RFC1213-MIB.ipInDiscards	Number of input IP datagrams that were discarded for some reason (such as lack of buffer space).
SNMP:RFC1213-MIB.ipInDelivers	Total number of input datagrams successfully delivered to IP user-protocols.
SNMP:RFC1213-MIB.ipOutRequests	Total number of IP datagrams that local IP user-protocols supplied to IP in requests for transmission.
SNMP:RFC1213-MIB.ipOutDiscards	Number of output IP datagrams that were discarded for some reason (such as lack of buffer space).
SNMP:RFC1213-MIB.ipOutNoRoutes	Number of IP datagrams discarded because no route was found to transmit them to their destination.
SNMP:RFC1213-MIB.ipFragOKs	Number of IP datagrams that have been successfully fragmented at this entity.
SNMP:RFC1213-MIB.ipFragFails	Number of IP datagrams that have been discarded because they could not be fragmented.
SNMP:RFC1213-MIB.ipFragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation.

Table 7-2 TCP Performance Counter

Counter	Description
RFC1213-MIB.tcpActiveOpens	Number of times TCP ¹ connections have made a direct transition to the SYN-SENT state from the CLOSED 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.tcpCurrEstab	Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
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.tcpInErrs	Total number of segments received in error (for example, bad TCP checksums)
RFC1213-MIB.tcpInSegs	Total number of segments received, including those received in error.
RFC1213-MIB.tcpMaxConn	Total number of TCP connections the entity can support.
RFC1213-MIB.tcpOutRsts	Number of TCP segments sent containing the RST flag.

Table 7-2 TCP Performance Counter

RFC1213-MIB.tcpOutSegs	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
RFC1213-MIB.tcpPassiveOpens	Number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
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.udpInDatagrams	Total number of UDP ² datagrams delivered to UDP users.

1. Transmission Control Protocol
2. User Datagram Protocol

Table 7-3 UDP Performance Counters

Counter	Description
RFC1213-MIB.udpInDatagrams	Total number of UDP datagrams delivered to UDP users.
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.udpNoPorts	Total number of received UDP datagrams for which there was no application at the destination port.
RFC1213-MIB.udpOutDatagrams	Total number of UDP datagrams sent from this entity.

Performance Data Collected for the Cisco MGC Hosts

The following performance counters are collected for each Cisco MGC host:

- IP performance counters
- TCP performance counters
- UDP performance counters

In addition, the attributes in Table 7-4 are collected for the active Cisco MGC host.

Table 7-4 Cisco MGC Host Performance Counters

Counter	Description
SNMP:HOST-RESOURCES-MIB.hrSystemNumUsers	Number of users on the host
SNMP:HOST-RESOURCES-MIB.hrSystemProcesses	Number of processes running on system

Performance Data Collected for BAMS

The following performance counters are collected for each BAMS:

- IP performance counters

- TCP performance counters
- UDP performance counters

In addition, the attributes in Table 7-5 are collected.

Table 7-5 BAMS Performance Counters

Counter	Description
SNMP:HOST-RESOURCES-MIB.hrSystemNumUsers	Number of users on the host
SNMP:HOST-RESOURCES-MIB.hrSystemProcesses	Number of processes running on the system

Performance Data Collected for the Cisco SLT

The following performance counters are collected for each Cisco SLT:

- IP performance counters
- TCP performance counters
- UDP performance counters

In addition, the attributes in Table 7-6 are collected.

Table 7-6 Cisco SLT Performance Counters

Counter	Description
SNMP:OLD-CISCO-CHASSIS-MIB.nvRamUsed	Amount of RAM in use

No performance collection is done for the SS7 MTP2 channels.

For details on collecting performance data for the Cisco SLT TDM interfaces, see “Performance Data Collected for TDM Interfaces” section on page 7-7.

Performance Data Collected for the LAN Switch

The following performance counters are collected for each LAN switch:

- IP performance counters
- TCP performance counters
- UDP performance counters

In addition, the attributes in Table 7-7 are collected for the IOS LAN switch.

Table 7-7 IOS LAN Switch Performance Counters

Counter	Description
SNMP:OLD-CISCO-CHASSIS-MIB.nvRamUsed	Amount of RAM in use

The attributes in Table 7-8 are collected for the Catalyst LAN switch.

Table 7-8 Catalyst LAN Switch Performance Counters

Counter	Description
SNMP:CISCO-STACK-MIB.sysTrafficPeak	Peak traffic utilization

Performance Data Collected for Network Interfaces

The performance counters in Table 7-9 are collected for each network interface.

Table 7-9 Network Interface Performance Counters¹

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

1. No performance attributes are collected for loopback interfaces.

Performance Data Collected for TDM Interfaces

The counters in Table 7-10 are collected for each Cisco SLT TDM interface to the SS7 network.

Table 7-10 TDM Interface Performance Counters

Counter	Description
SNMP:RFC1406-MIB.dsx1TableBESs ¹	Number of bursty errored seconds
SNMP:RFC1406-MIB.dsx1TableCSSs	Number of controlled slip seconds
SNMP:RFC1406-MIB.dsx1TableDMs	Number of degraded minutes
SNMP:RFC1406-MIB.dsx1TableESs	Number of errored seconds
SNMP:RFC1406-MIB.dsx1TableLCVs	Number of line code violations
SNMP:RFC1406-MIB.dsx1TableLESs	Number of line errored seconds
SNMP:RFC1406-MIB.dsx1TablePCVs	Number of path coding violations
SNMP:RFC1406-MIB.dsx1TableSEFSs	Number of severely errored framing seconds
SNMP:RFC1406-MIB.dsx1TableSESs	Number of severely errored seconds
SNMP:RFC1406-MIB.dsx1TableUASs	Number of unavailable seconds

1. *Table* refers to the RFC-1406 DSX1 table and is either Current or Total.

Performance Data Collected for the Cisco 2900XL LAN Switch Port

In addition to the standard interface attributes, the counters in Table 7-11 are also collected for the Cisco 2900XL port.

Table 7-11 Cisco 2900XL LAN Switch Port Performance Counters

Counter	Description
SNMP:CISCO-C2900-MIB.c2900PortRxNoBwFrames	Frames discarded due to lack of bandwidth
SNMP:CISCO-C2900-MIB.c2900PortRxNoBufferFrames	Frames discarded due to lack of buffer
SNMP:CISCO-C2900-MIB.c2900PortRxNoDestUniFrames	Number of unicast frames discarded
SNMP:CISCO-C2900-MIB.c2900PortRxNoDestMultiFrames	Number of multicast frames discarded
SNMP:CISCO-C2900-MIB.c2900PortRxFcsErrFrames	Frames received with an FCS error
SNMP:CISCO-C2900-MIB.c2900PortCollFragFrames	Frames whose length was less than 64
SNMP:CISCO-C2900-MIB.c2900PortTxMulticastFrames	Frames successfully transmitted (multicast)
SNMP:CISCO-C2900-MIB.c2900PortTxBroadcastFrames	Frames successfully transmitted (broadcast)

Performance Data Collected for the CIAgent System Components

The following sections list the attributes collected for each CIAgent system component.



Note

For information about viewing this information, see the “Viewing CIAgent Device Information” section on page 9-36.

Fixed Disk

The counters in Table 7-12 are collected for each fixed disk object.

Table 7-12 Fixed Disk Performance Counters

Counter	Description
SNMP:HOST-RESOURCES-MIB.hrStorageAllocationFailures	Number of failed allocation requests
SNMP:HOST-RESOURCES-MIB.hrStorageUsed	Amount of storage used

Processor

The counters in Table 7-13 are collected for each processor object.

Table 7-13 Processor Performance Counters

Counter	Description
SNMP:HOST-RESOURCES-MIB.hrDeviceErrors	Number of errors detected on device
SNMP:HOST-RESOURCES-MIB.hrProcessorLoad	Average load on the processor

RAM

The counters in Table 7-14 are collected for each RAM object.

Table 7-14 RAM Performance Counters

Counter	Description
SNMP:HOST-RESOURCES-MIB.hrStorageAllocationFailures	Number of failed allocation requests
SNMP:HOST-RESOURCES-MIB.hrStorageUsed	Amount of storage used

Virtual Memory

The counters in Table 7-15 are collected for each virtual memory object.

Table 7-15 Virtual Memory Performance Counters

Counter	Description
SNMP:HOST-RESOURCES-MIB.hrStorageAllocationFailures	Number of failed allocation requests
SNMP:HOST-RESOURCES-MIB.hrStorageUsed	Amount of storage used

Cisco MGC Host Configuration Performance Counters

The Cisco MGC host writes out performance counters for many of the signaling components. These performance counters are in the form of ASCII flat files containing entries for all collected counters for all signaling components.

Performance data is stored directly on the signaling components themselves. You only see the performance data for any given component, not for all signaling components. All performance counters are predefined in the CEMF object model.

On the Cisco MGC host, you can specify multiple intervals for any given counter. For example, you can specify that a counter is to be written for each 5-minute, 15-minute, 30-minute, 60-minute, and 24-hour interval. However CMNM supports only a single interval for any given counter.

The Cisco MGC host administrator must ensure that the performance configuration writes out each counter only at a single interval by modifying the measProfs.dat and buckets.dat files so there is only a single entry (time interval) for each category. The administrator should choose the most granular interval (shortest time) necessary for each counter. If the administrator fails to do this and the Cisco MGC host

writes out the same counter at multiple intervals, CMNM collects all data points and stores them in the same attribute, causing spikes in the resulting performance displays. For this reason, the user must configure the Cisco MGC host such that each measurement is written out only at a single time interval.

On the Cisco MGC host, there are a number of files that determine which performance counters are collection as well as the frequency of their collection, as shown in Table 7-16.

Table 7-16 Cisco MGC Host Measurements File

MGC Host File	Description
buckets.dat	Defines the measurement buckets and intervals and their associated thresholds.
dmpRinks.dat	Defines how often the performance counters are to be collected and the maximum number of records and the maximum file size of the CSV files.
measCats.dat	Defines all of the counters in each category to be generated by the Cisco MGC host software.
measProfs.dat	Defines the profiles associated with each measurement category, including information concerning reporting intervals and measurements.

Measurement Filters

You can use measurement filters to specify the Cisco MGC host configuration performance counters that CMNM collects. Although the Cisco MGC host continues to write out all of its configuration performance counters, CMNM collects only the subset defined in its measurement filters.

During startup, CMNM reads the measurement filter file:

```
$CEMF_ROOT/config/hostController/measFilters
```

This file contains a list of all of the Cisco MGC host configuration performance measurements that CMNM collects. It lets you filter counters based on their measurement names and the MML component names.

The format of the measurement filter file is:

Measurement Name, *|*Component Name*

where the variables are defined in Table 7-17.

Table 7-17 CMNM Measurement Filters

Parameter	Description
<i>Measurement Name</i>	Any measurement specified in the Cisco MGC host measCats.dat file.
<i>Component Name</i>	Any MML component specified in the Cisco MGC host components.dat file. An asterisk (*) matches all components.

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:

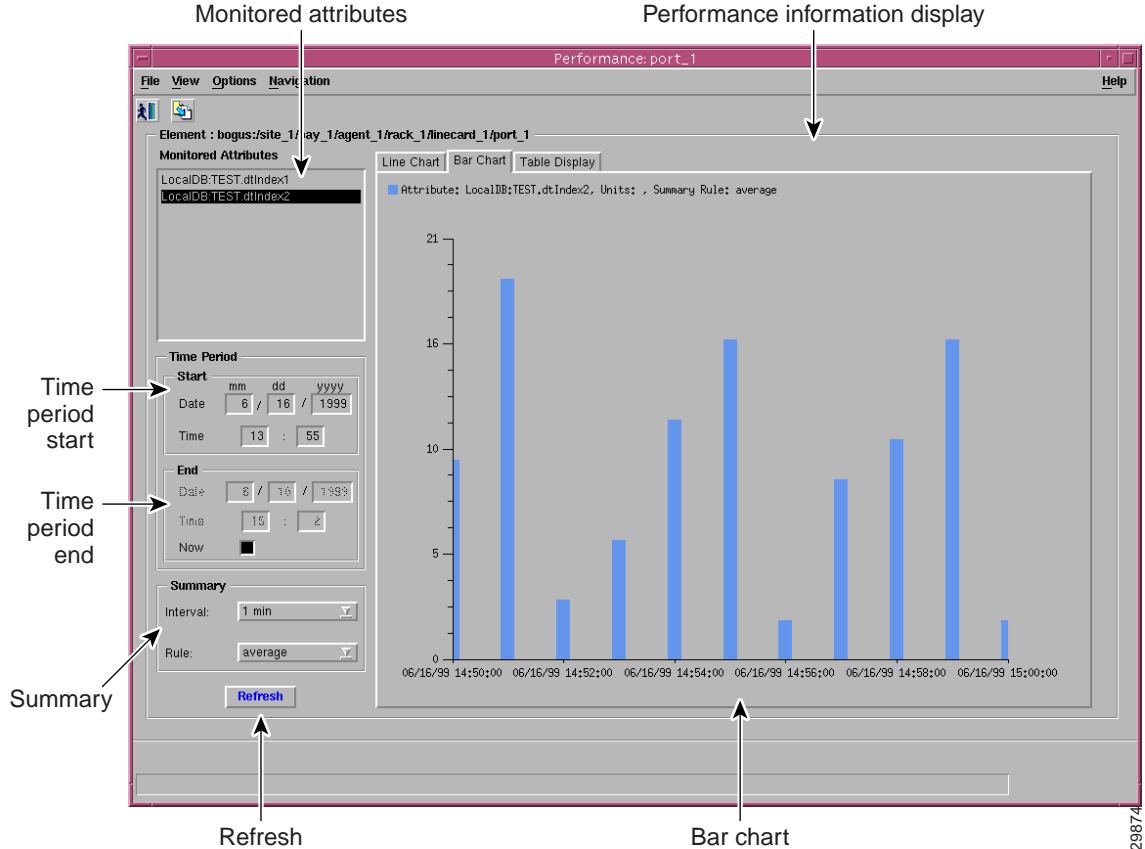
-
- Step 1** Open the appropriate window to display a relevant object.
 - Step 2** Place the cursor over the object.
 - Step 3** Press and hold the right mouse button.
 - Step 4** Move the cursor until the **Tools** option is highlighted, then highlight the **Performance Manager** option, as shown in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

Figure 7-2 Map Viewer Screen—Tools->Performance Manager Option



- Step 5** Release the right mouse button.
You see the Performance Manager screen shown in Figure 7-3.

Figure 7-3 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.













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 7-18 shows the different logical states.

Table 7-18 State Symbols

State Symbol	Description
	Indicates that the device has not been discovered. (This is the icon when the device is initially deployed.)
	Indicates that the device is in the process of discovering. The icon also has a hatch pattern.
	Indicates that the device has some outage or operational problem and is, therefore, out-of-service. Icons also have a hatch pattern.
	Indicates that the device 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 icons also have a hatch pattern.
	Indicates that the device is off-duty or administratively down.
	Indicates that the device is providing service.
	Indicates that the device is running in warm-standby mode.
	Indicates that the device is running in an unknown (other) mode.
	Indicates that the device is being tested.
	A hatch-pattern (without any corresponding state symbol) is used to indicate that the device is not being managed.
<None>	An icon with no hatch pattern or symbol indicates the device is running normally.

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.

Setting Different Polling Frequencies

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** On the Map Viewer screen, select the device you want to configure.
 - Step 2** Right-click to display the pull-down menu and select **States**, as shown in Figure 7-4. (This example uses a Cisco SLT, but the procedure is the same for other devices.)

Figure 7-4 *Map Viewer Screen—Tools>Open Polling Frequencies Option*



You see the screen in Figure 7-5.

Figure 7-5 *Polling Frequencies Screen*



- Step 3** You can set the frequency for performance polling, status polling, and auto-discovery. To change from minutes to hours, select from the pull-down menu, as shown in Figure 7-6.

Figure 7-6 *Polling Frequencies Screen—Frequency Pull-Down Menu*



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.

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 **States** as shown in Figure 7-7.

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



You see the screen in Figure 7-8.

Figure 7-8 *SLT States Screen*



Step 2 Click **Start Polling**.

You see the screen in Figure 7-9.

Figure 7-9 *Polling Configuration Prompt*



Step 3 Click **Yes** to proceed.

To stop polling at anytime during the process, click **Stop Polling**, as shown in Figure 7-10.

Figure 7-10 Stop Polling Screen**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.

**Note**

When polling is taking place, a sheet with an arrow pointed up appears just above the network or object icon. Figure 7-11 shows the 2600a-Ethernet-1 and 2600a-Serial-8 in polling states.

Figure 7-11 Map Viewer Screen—2600a in Polling State

Decommissioning, Rediscovering, and Rebooting Devices

You can commission or decommission devices such as the Cisco SLT, LAN switch, Cisco MGX 8260, BAMS, and Cisco MGC host.

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.

The decommissioned state is used in two circumstances:

- When the physical device is administratively off the network.
- When the physical device has a known problem and you do not want to manage it.

When a trap is received, CMNM checks to see if the destination object is decommissioned. If so, the trap is discarded. Otherwise trap processing continues as normal. In this way, you never receive any traps on a decommissioned device.

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

To decommission, rediscover, or reboot a device:

-
- Step 1** Click the network or device, right-click to display the pull-down menu, then select **States** as shown in Figure 7-12.

Figure 7-12 Map Viewer Screen—Open SLT States Option



You see the screen in Figure 7-13.

Figure 7-13 SLT States Screen



- Step 2** Click the **States** tab.
You see the screen in Figure 7-14.

Figure 7-14 SLT States Screen

Step 3 Click the relevant button to accomplish the task you want to perform.

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. 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
- Logical OR—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

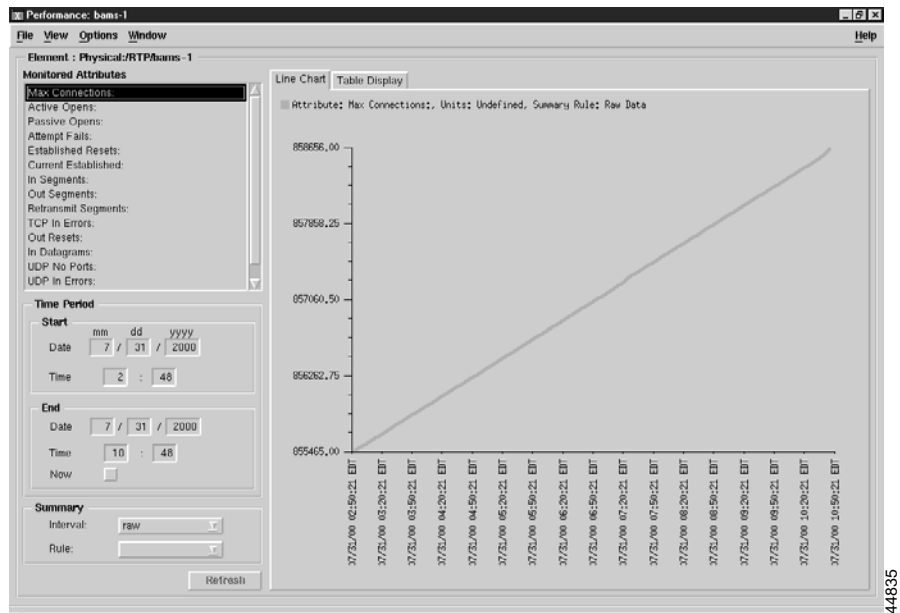
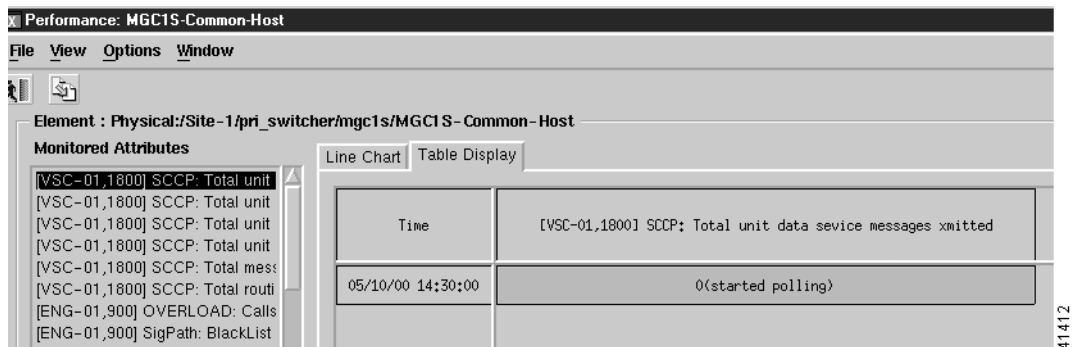


Figure 7-16 Sample Table Display Screen



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 7-23.
- 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 7-19. Note that you must select a chart before invoking these actions.

Table 7-19 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 7-23, 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 7-20, controls the behavior of the performance purging mechanism:

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

Table 7-20 *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 8-49.

Exporting Performance Data

CEMF has an exporting facility that lets you write performance data to an ASCII file. Using the `historyAdmin export` command, the northbound system can generate files that contain the performance data for an object during a selected interval.



Note

CMNM does not provide any CORBA or GUI interface to the CEMF history export facilities. You must manually perform the export (using the command `/opt/cemf/bin/historyAdmin export filename`), or the northbound system must perform it using Telnet or another facility.

The data is exported in the following format:

```
Object:<object path>
Object class:<object path>
Attribute: <attribute name>
Summary rule:<rule>
Summary interval: Raw | <summary interval>
<date> <time> <valueType> <value>
<date> <time> <valueType> <value>
...
Data exported: <current date/time>
```

For example, a sample file looks like:

```
> historyAdmin export dumpFile TAB 10 all criterial
Object: exampleView:/site_1/bay_1/agent_1/rack_1/linecard_2/port_2
Object Class: testPort
Attribute: LocalDB:TEST.dtIndex1
Summary interval: Raw
09 Jun 1999 11:50:03 Polled 10
09 Jun 1999 11:50:23 Polled 10
09 Jun 1999 11:50:43 Polled 15
09 Jun 1999 11:51:03 Missed <no value>
09 Jun 1999 11:51:23 Polled 20
09 Jun 1999 11:51:43 Polled 20
09 Jun 1999 11:52:03 Polled 0
09 Jun 1999 11:52:23 Polled 5
09 Jun 1999 11:52:43 Polled 0
09 Jun 1999 11:53:03 Polled 10
Data exported: Sun Jun 27 17:17:35 1999
```

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**.
-



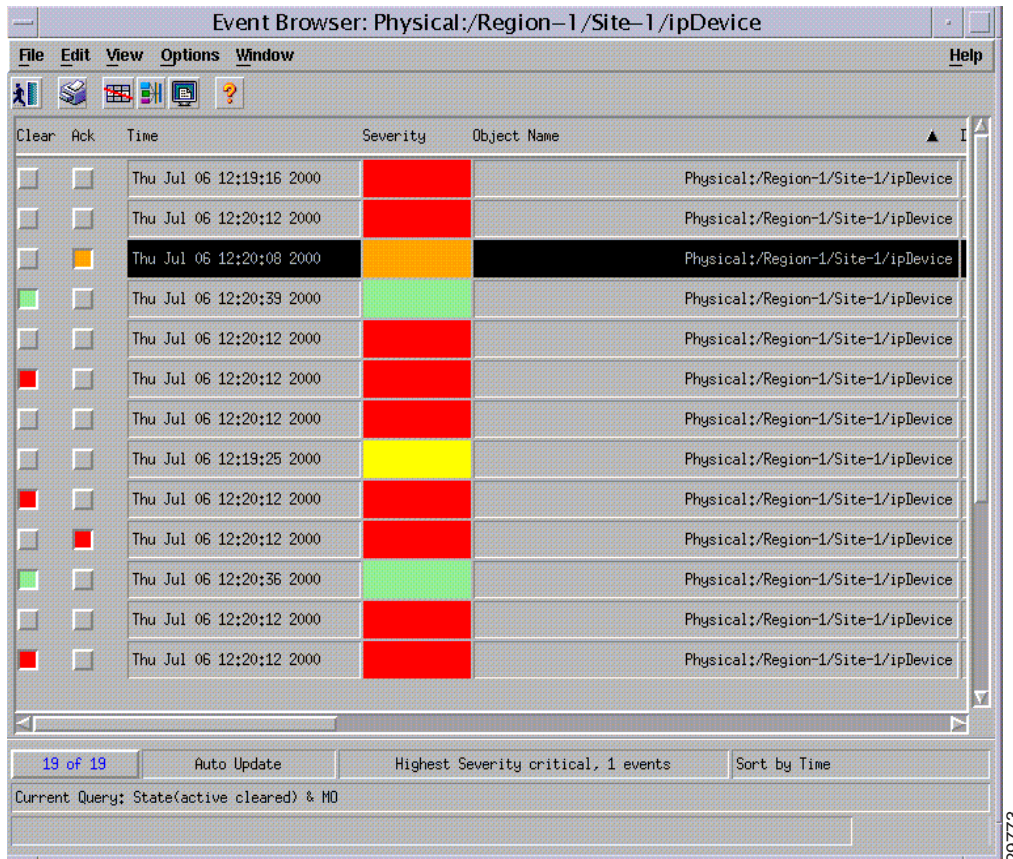
Managing Traps and Events

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.

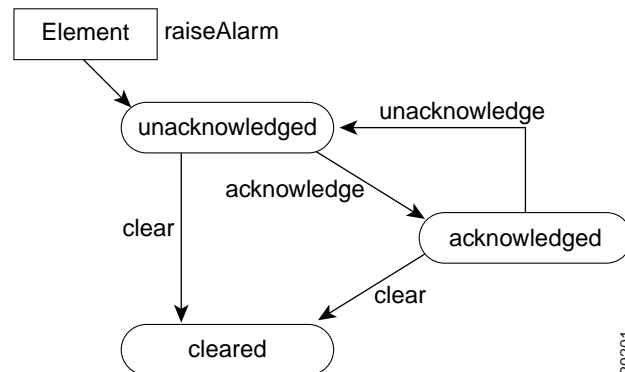
Event State

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

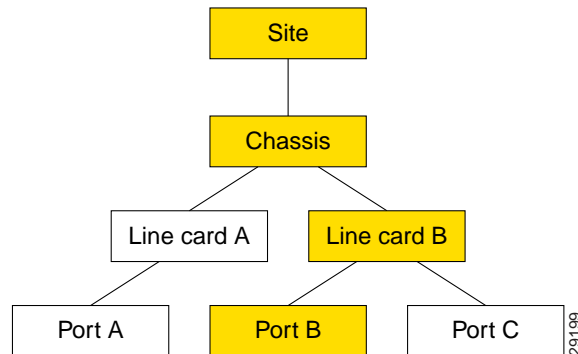
This is the management domain of SNMP trap information. The SNMP MIB specific information typically defines the equipment type generating a trap.

Event Propagation

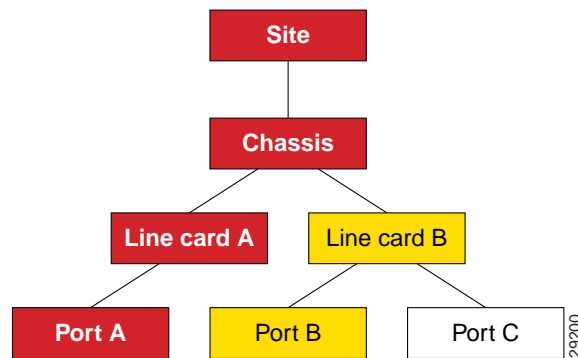
In order to make the identification of potential problems easy, CEMF propagates the alarm state of objects upwards through each object view.

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/Status 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 reestablished, 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 CMNM Manages Multiple IP Addresses for Presence Polling

By default, each CEMF object can contain only a single IP address. For example, when the user deploys a Cisco SLT, the user can specify only a single IP address. CEMF uses this IP address for all management transactions including presence polling and performance polling. In addition, the IP address is used to map incoming faults to the CEMF object. When a trap arrives from the network element, CEMF matches the IP address of the trap sender to the IP address of an object in the database.

In reality, a physical device may have more than one IP address. Traps may come from any interface on the device. Since CEMF/CMNM is aware of only a single IP address, traps received from an alternate interface might be dropped.

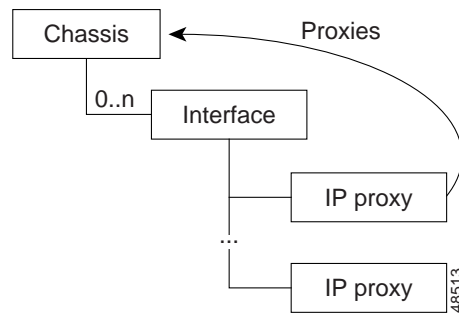
Any interface on the device may go down (either operationally or administratively). If the management interface goes down, all SNMP-based operations fail. That is, not all SNMP queries are completed, nor does status polling or performance polling function. CMNM is designed to avoid these situations by using trap proxies and IP address failover, which are described in the following sections.

Trap Proxies

To prevent the dropping of traps received from an alternate interface, CMNM models each IP address on the device. When a trap comes in on any interface, it is mapped to its logical chassis object.

During auto-discovery, the RFC1213-MIB.ipAddrTable is queried. Each IP address is deployed as a child of its corresponding interface (see Figure 8-5).

Figure 8-5 Multiple IP Address Proxies



The IP Proxy object acts as stand-in for its network element. When a trap is received from the network element, it is bound for one of the IP proxy objects. Internally, CMNM redirects the trap to the proxied object. For example, all traps received on any Cisco SLT interface are redirected to the SLT Chassis object. In this way all traps on all interfaces are shown, logically, on the object that represents that device.

IP Address Failover

Since CMNM models each IP Address on the device, it is possible to implement an IP address failover mechanism. When a device is first deployed, the user specifies an IP address on the management interface. If the management interface goes down or the management addresses becomes unreachable, CMNM automatically fails over to another IP address. When the management interface/IP address is restored, CMNM resumes using it for all device communication.

CMNM periodically polls each IP address to ensure that that route is reachable via SNMP. If the management IP address becomes unreachable, CMNM searches for a new IP address using the following rules:

- If any IP address is available on the current management interface, it is used.
- If the current management interface is down, each additional interface is searched, starting with Ethernet interfaces.

When CMNM searches for an alternate interface, it starts with the Ethernet interfaces. If none are available, it attempts to use any other available interfaces (for example TDM interfaces on a Cisco SLT). Once a usable interface is found, CMNM must decide which IP address to use on that interface. Because there is no way to distinguish IP addresses, CMNM simply uses the first available IP address child of the interface. Technically this should be the first IP address defined in the ipAddrTable for that interface.

If no IP addresses are available (they are all unreachable), CMNM raises a critical alarm on the chassis. This alarm indicates that the device is truly unreachable and requires immediate operator attention. Once at least one IP address is restored, the alarm is automatically cleared.

Status Polling

CMNM periodically polls each IP address to see if is reachable via SNMP by sending an SNMP get message to the IP address object, retrieving the value of the SNMP:RFC1213-MIB.sysUpTime attribute.

If the attribute is available, it assumed the IP address is reachable. Otherwise, the IP address is unreachable and is transitioned into the unreachable state. Once connectivity is reestablished, the object is transitioned back into the normal state.

Besides performing status polling on each IP address object, CMNM also performs status polling on various other components. These include:

- Network interfaces
- Cisco MGC node devices

Network Interface Status

CMNM performs status polling to reflect the state of each network interface. Depending on the operational and administrative status of the interface, the object representing the network interface is transitioned into different state as indicated in Table 8-2.

Table 8-2 Network Interface States

Admin Status	Operational Status	Network Interface State
Up	Up	up
Up	Down	down
Up	In Test	in-test
In Test	N/A	in-test
Down	N/A	off-duty
<not reachable>	N/A	unreachable

Note that the chassis is queried for the state of its interfaces. That is, the status of the interface reported by CMNM is identical to the status reported by the chassis on its current management IP address. However, the status of each interface is reported by the chassis via that object's specific IP addresses. In this way CMNM can better reflect the true health of the chassis.

Interface Alarms

When a network interface goes down, the device sends a link down trap to CMNM. When CMNM detects this trap, it transitions the object representing that interface to the down state. To handle the case where CMNM may have missed a trap, the status polling mechanism raises an alarm if it detects that the interface is down. When the interface comes back up, the device raises a link-up trap. If CMNM detects this trap, it transitions the interface back into the normal state. If CMNM missed this trap, the next status poll will detect that the interface is back up. Internally, CMNM transitions the interface back to the normal state and clears the appropriate alarms on the object.

When an interface goes down, all IP address on that interface become unreachable. Since, during the next status-poll cycle, all IP addresses on that interface will fail, CMNM automatically transitions all of the child IP address objects into the unreachable state. Doing so prevents a potential flood of alarms.

MGC Host Status

CMNM periodically checks the status of each MGC Node device. The attribute SNMP:CISCO-TRANSPATH-MIB.tpCompOpStatus is retrieved and its value is used to determine the required state of the object as indicated in Table 8-3

Table 8-3 Cisco MGC Host States

Component Status	Network Interface State
ACTIVE	active
STANDBY	standby
OOS	oos
<no answer>	not-running
<not reachable>	unreachable

BAMS Status

CMNM periodically checks the status of each BAMS device. The SNMP:ACECOMM-BAMS-SYSPARM-MIB.sysStatus attribute is retrieved and its value is used to determine the required state of the object as indicated in Table 8-4

Table 8-4 BAMS States

Component Status	Network Interface State
active	active
standby	standby
outage	oos
other	other
<no answer>	not-running
<not reachable>	unreachable

Polling Frequency

CMNM allows the user to configure status polling frequencies for each type of device. For example, the user can set the status polling frequency for Cisco SLT devices to be different than that of the Cisco MGC host devices.

The status polling frequency controls the rate at which the IP Address objects are polled. In addition, this frequency is used to determine the rate at which the status of the various devices is queried.

Given the polling interval, all objects are polled at some point in that interval. For example, if the status polling frequency for a Cisco SLT is set to 5 minutes, all IP address objects on all Cisco SLTs are polled at some point during a five-minute interval.

Manual SNMP Query

Besides the periodic polling, CMNM provides a mechanism to check the SNMP visibility of a device or set of devices. You can click a button that causes a manual SNMP poll to occur. The results of this manual poll are displayed.

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.

CMNM converts traps to alarms which are displayed in the Event Browser. For the Cisco SLT, the Catalyst LAN switches, and the Cisco MGX 8260, each trap has a corresponding CMNM alarm. For example, the linkDown trap from the Cisco SLT corresponds to the “Link down” Event Description in the CMNM Event Browser. For the BAMS and the Cisco MGC, the trap serves as an envelope that can carry any one of numerous alarm messages.

In addition to device-specific traps, CMNM generates internal alarms. Appendix A, “BAMS, Cisco MGC, and CMNM Messages” provides an explanation of these internal messages and references to documentation on alarm messages from the BAMS and the Cisco MGC.

BAMS Alarms

All BAMS alarms are carried on a single trap, the AlarmTrap.

Table 8-5 BAMS Traps

Trap	MIB
nusageAlarmTrap	ACECOMM-NUSAGE-MIB

See Appendix A, “BAMS, Cisco MGC, and CMNM Messages” for references to documentation on BAMS alarms.

Cisco SLT Alarms

Table 8-6 Cisco SLT Alarms



Alarm/Trap	MIB	Explanation
coldStart	SNMPv2-MIB	The device was started from a power-off state.  Note Clear this event manually.
warmStart	SNMPv2-MIB	The device was restarted from an on state.  Note Clear this event manually.
linkUp	IF-MIB	An interface is up after being down.
linkDown	IF-MIB	An interface is down. This is cleared by one or more Link Up traps for the same interface.



Table 8-6 Cisco SLT Alarms

Alarm/Trap	MIB	Explanation
authenticationFailure	SNMPv2-MIB	The device received an SNMP message that was improperly authenticated.
syslogAlarm	CISCO-SYSLOG-MIB	
configChange	CISCO-CONFIG-MAN-MIB-VISMI	There has been a configuration change. (Informational)

Catalyst LAN Switch Alarms



Catalyst 5500 Alarms

Table 8-7 Catalyst 5500 Alarms

Alarm/Trap	MIB	Explanation
coldStart	SNMPv2-MIB	The device was started from a power-off state.  Note Clear this event manually.
warmStart	SNMPv2-MIB	The device was restarted from an on state.  Note Clear this event manually.
linkUp	IF-MIB	An interface is up after being down.
linkDown	IF-MIB	An interface is down. This is cleared by one or more Link Up traps for the same interface.
authenticationFailure	SNMPv2-MIB	The device received an SNMP message that was improperly authenticated.
configChange	CISCO-CONFIG-MAN-MIB-VISMI	There has been a configuration change. (Informational)
switchModuleUp	CISCO-STACK-MIB	A module is up after being down.
switchModuleDown	CISCO-STACK-MIB	A module is down.

Catalyst 2900XL Alarms

Table 8-8 Catalyst 2900XL Alarms

Alarm/Trap	MIB	Explanation
coldStart	SNMPv2-MIB	The device was started from a power-off state.  Note Clear this event manually.
warmStart	SNMPv2-MIB	The device was restarted from an on state.  Note Clear this event manually.
linkUp	IF-MIB	An interface is up after being down.
linkDown	IF-MIB	An interface is down. This is cleared by one or more Link Up traps for the same interface.
authenticationFailure	SNMPv2-MIB	The device received an SNMP message that was improperly authenticated.
syslogAlarm	CISCO-SYSLOG-MIB	
configChange	CISCO-STACK-MIB	There has been a configuration change. (Informational)

Catalyst 2900 Alarms

Table 8-9 Catalyst 2900 Alarms



Alarm/Trap	MIB	Explanation
coldStart	SNMPv2-MIB	The device was started from a power-off state.  Note Clear this event manually.
warmStart	SNMPv2-MIB	The device was restarted from an on state.  Note Clear this event manually.
linkUp	IF-MIB	An interface is up after being down.

Table 8-9 Catalyst 2900 Alarms

Alarm/Trap	MIB	Explanation
linkDown	IF-MIB	An interface is down. This is cleared by one or more Link Up traps for the same interface.
authenticationFailure	SNMPv2-MIB	The device received an SNMP message that was improperly authenticated.
configChange	CISCO-STACK-MIB	There has been a configuration change. (Informational)
switchModuleUp	CISCO-STACK-MIB	A module is up after being down.
switchModuleDown	CISCO-STACK-MIB	A module is down.

Cisco MGC Host Alarms

CMNM handles the traps in Table 8-10 from the Cisco MGC hosts. Each trap is used as an envelope for alarms of that type. See Appendix A, “BAMS, Cisco MGC, and CMNM Messages” for references to documentation on MGC alarms.

Table 8-10 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

MGC Host and BAMS Resource Alarms

CMNM traps application-related events that occur on the Cisco MGC hosts or the BAMS.

Table 8-11 Resource Alarms

Alarm/Trap	MIB	Explanation
critAppDown	CRITAPP-MIB	A critical application is down.
critAppUp	CRITAPP-MIB	The application is up after being down. This clears the above alarm.
siFsAboveWarningThreshold	SIFSMONITOR-MIB	A monitored file system usage percentage is above the warning threshold.

Table 8-11 Resource Alarms

Alarm/Trap	MIB	Explanation
siFsBelowWarningThreshold	SIFSMONITOR-MIB	The monitored file system usage is below the warning threshold. This clears the above alarm.
siFsAboveCriticalThreshold	SIFSMONITOR-MIB	A monitored file system usage percentage is above the critical threshold.
siFsBelowCriticalThreshold	SIFSMONITOR-MIB	The monitored file system usage is below the critical threshold. This clears the above alarm.

Cisco MGX 8260 Alarms

Table 8-12 Cisco MGX 8260 Traps and Alarms



Trap	MIB	Alarm Description
coldStart	SNMPv2-MIB	The device was started from a power-off state.  Note Clear this event manually.
warmStart	SNMPv2-MIB	The device was restarted from an on state.  Note Clear this event manually.
linkUp	IF-MIB	An interface is up after being down.
linkDown	IF-MIB	An interface is down. This is cleared by one or more Link Up traps for the same interface.
authenticationFailure	SNMPv2-MIB	The device received an SNMP message that was improperly authenticated.

Table 8-13 Additional Cisco MGX 8260 Traps

Trap	MIB
shelfMajorAlarm	mms1600_trap
shelfMinorAlarm	mms1600_trap
shelfAlarmClear	mms1600_trap
shelfSecurityAlert	mms1600_trap
shelfColdStart	mms1600_trap
shelfHistoryChg	mms1600_trap
cardInserted	mms1600_trap
cardRemoved	mms1600_trap

Table 8-13 Additional Cisco MGX 8260 Traps

Trap	MIB
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
dsx3LineAdded	mms1600_trap
dsx3LineDeleted	mms1600_trap
dsx3LineModified	mms1600_trap
dsx3MajorAlarm	mms1600_trap
dsx3MinorAlarm	mms1600_trap

Table 8-13 Additional Cisco MGX 8260 Traps

Trap	MIB
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
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.

How Traps Are Cleared Using Correlation Files

CMNM can clear alarms using CEMF Clear Correlation files. On receipt of an incoming clear alarm, the rules defined in these files indicate which active alarms on a given object should be cleared. For example, a link-up alarm clears a link-down alarm, a process normal alarm clears a process error alarm, and a communication success alarm clears a communication failure alarm.

A sample Clear Correlation file is:

```
CLEAR_CORRELATION_RULE
    INCOMING_ALARM_CLASS    linkUpAlarmClass
    ALARM_CLASS_TO_CLEAR   linkDownAlarmClass
END_RULE
```

When a clear condition is received, the cleared alarm is automatically removed from the appropriate screens and the clear alarm is forwarded to northbound systems like any other alarm.

The following sections map the alarms to their clear conditions for each Cisco MGC node device.

Cisco MGC Host Clear Correlation

Table 8-14 maps the alarms to their clear conditions for the Cisco MGC host.

Table 8-14 Cisco MGC Host Clear Correlation

Alarm	Clear Condition
processingError	processingNormal
communicationFailure	communicationSuccess
qualityOfServiceError	qualityOfServiceNormal
equipmentError	equipmentNormal
environmentError	environmentNormal

Cisco SLT Clear Correlation

Table 8-15 maps the alarms to their clear conditions for the Cisco SLT.

Table 8-15 Cisco SLT Clear Correlation

Alarm	Clear Condition
IF-MIB.linkDown	IF-MIB.linkUp

LAN Switch Clear Correlation

Table 8-16 maps the alarms to their clear conditions for the LAN switch.

Table 8-16 LAN Switch Clear Correlation

Alarm	Clear Condition
IF-MIB.linkDown	IF-MIB.linkUp
CISCO-STACK-MIB.switchModuleDown	CISCO-STACK-MIB.switchModuleUp

CIAgent Clear Correlation

Table 8-17 maps the alarms to their clear conditions for the CIAgent.

Table 8-17 *CIAgent Clear Correlation*

Alarm	Clear Condition
CRITAPP-MIB.critAppDown	CRITAPP-MIB.critAppUp ¹
CRITAPP-MIB.critAppNotAllRunning	CRITAPP-MIB.critAppAllRunning
SIFSMONITOR-MIB.siFsBelowWarningThreshold	SIFSMONITOR-MIB.siFsAboveWarningThreshold ²
SIFSMONITOR-MIB.siFsBelowCriticalThreshold	SIFSMONITOR-MIB.siFsAboveCriticalThreshold ³

1. The varbind criAppName in the trap/clear must match.
2. The varbind siFsMonName in the trap/clear must match.
3. The varbind siFsMonName in the trap/clear must match.

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, BAMS, and LAN switch) to northbound systems.



Note

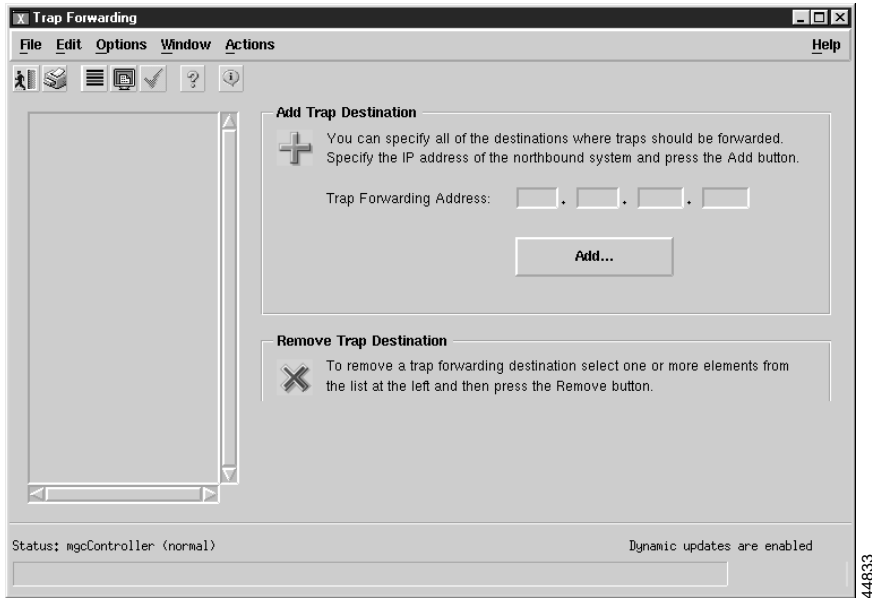
If you plan to configure CMNM to forward traps to northbound systems, you should configure SNMP Version 1 traps only on network devices. CMNM only forwards SNMP Version 1 traps to northbound systems. For more information on configuring SNMP on network devices, see Chapter 3, “Configuring Network Devices 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 MGC-Node-View icon 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 8-6.

Figure 8-6 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 8-7.

Figure 8-7 Action Report Screen



Step 4 Click **Close**, then close the Trap Forwarding screen shown in Figure 8-6.


Step 5 Select the MGC-Node-View 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 8-6 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 select **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 8-23.

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 8-8, 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:

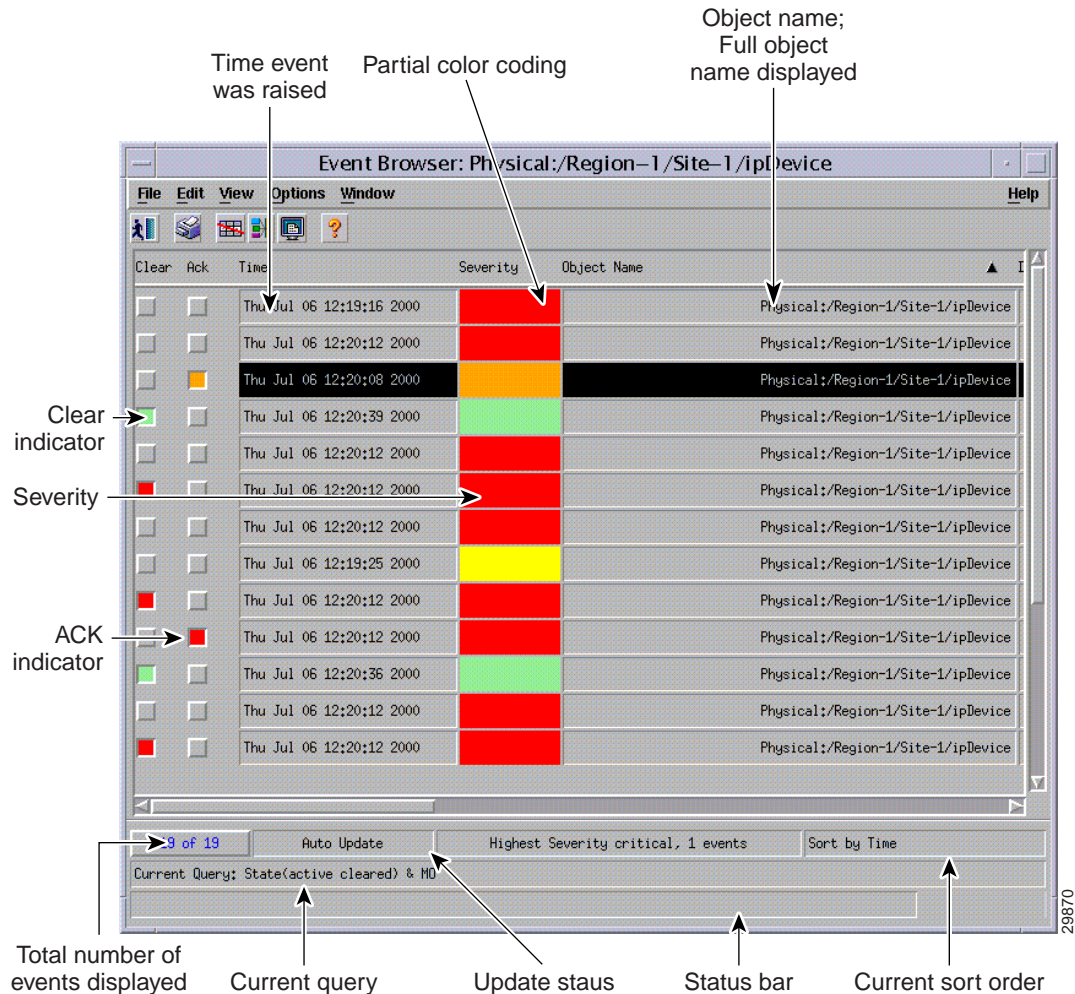
- Clear (an indicator to show if an event is active or cleared)
- Ack (an indicator to show if an event is acknowledged or unacknowledged).

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 8-8 Event Browser Screen



Menus are available that provide you with 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 8-36.

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

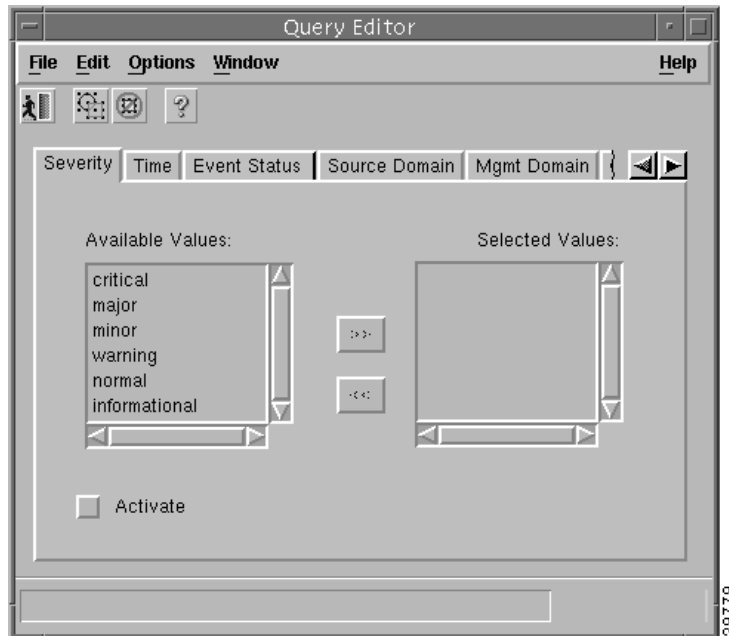
To define a query, click the  icon in the CEMF Launchpad window, or

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 8-9, 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 8-9 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.

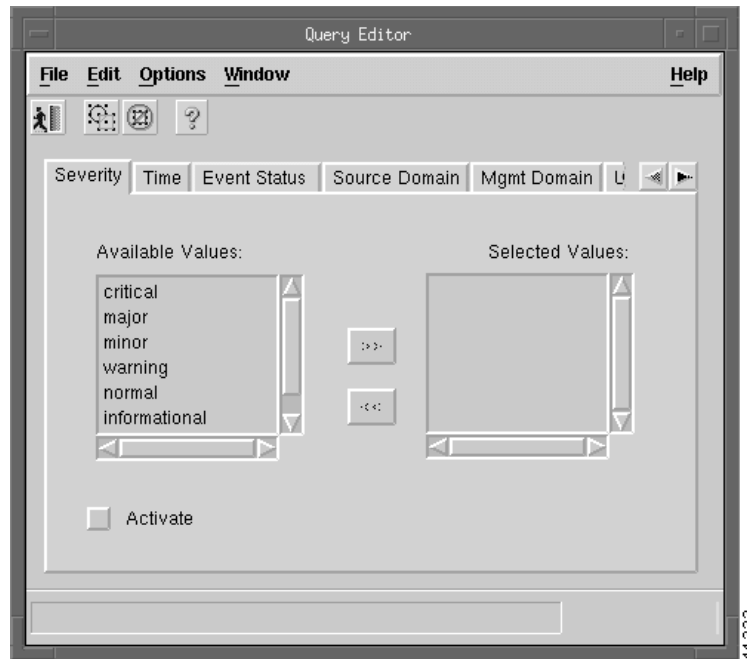
Setting Filtering Criteria

To set filtering (query) criteria:

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

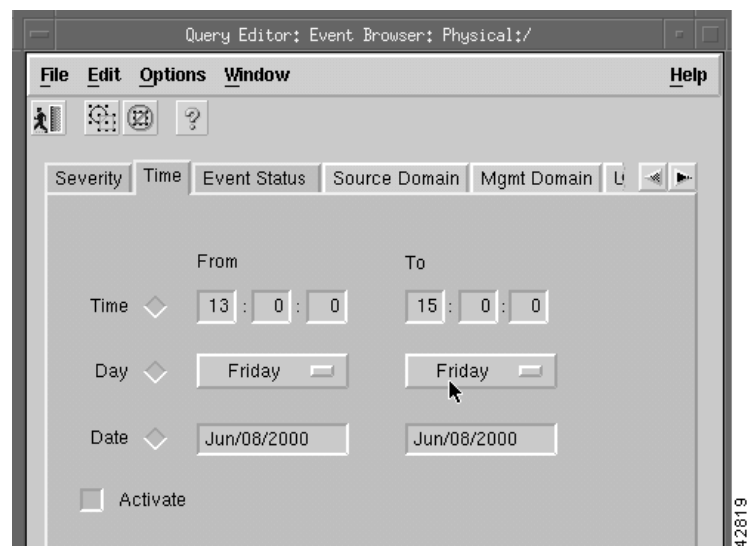
You see the screen in Figure 8-10.

Figure 8-10 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 8-11.

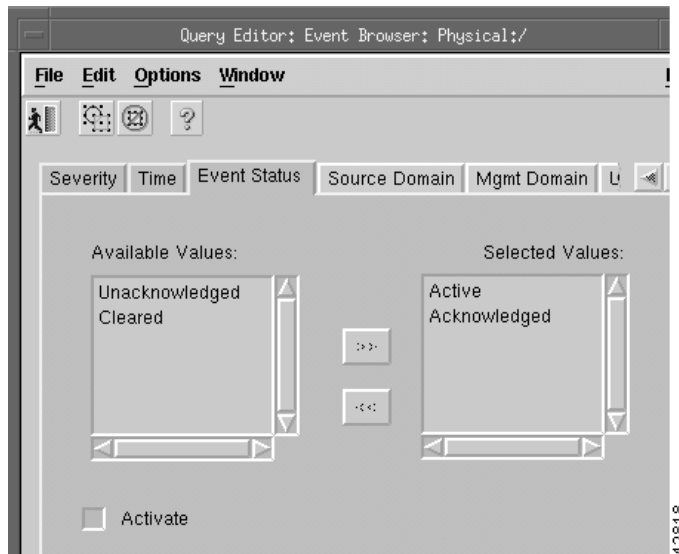
Figure 8-11 Query Editor Screen—Time Tab



- 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 8-12.

Figure 8-12 Query Editor Screen—Event Status Tab

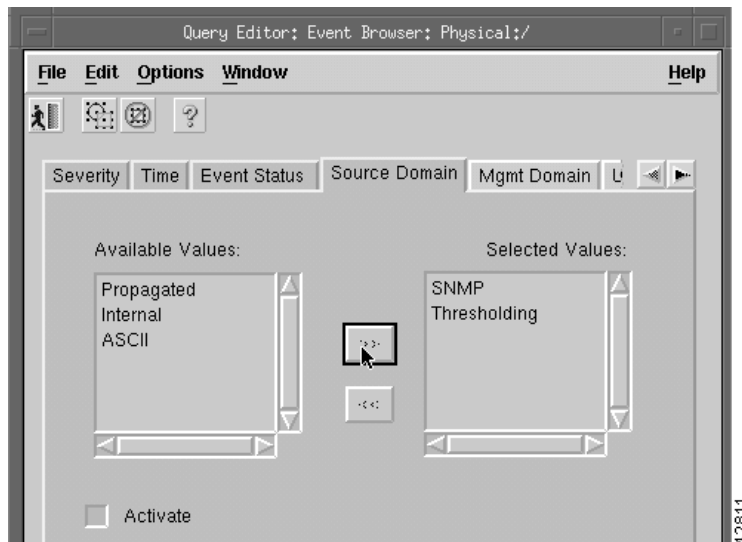


Step 7 From the Available Values list, select the events and click the right arrows to transfer them to the Selected Values list.

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

You see the screen in Figure 8-13.

Figure 8-13 Query Editor Screen—Source Domain Tab

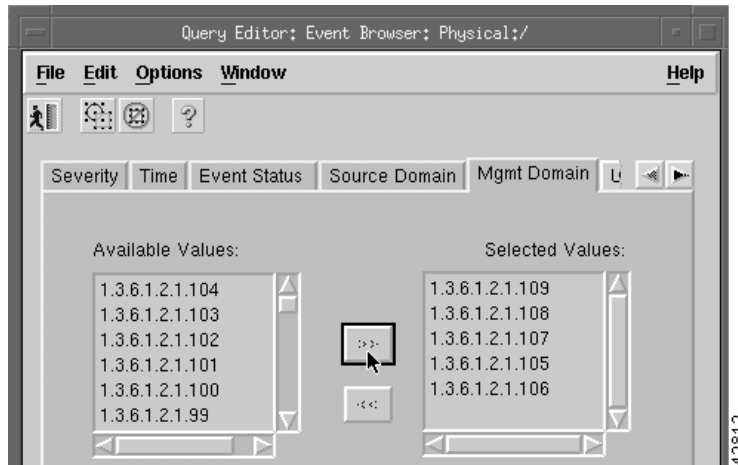


Step 9 From the Available Values list, select Domain values and click the right arrows to transfer the values to the Selected Values list.

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

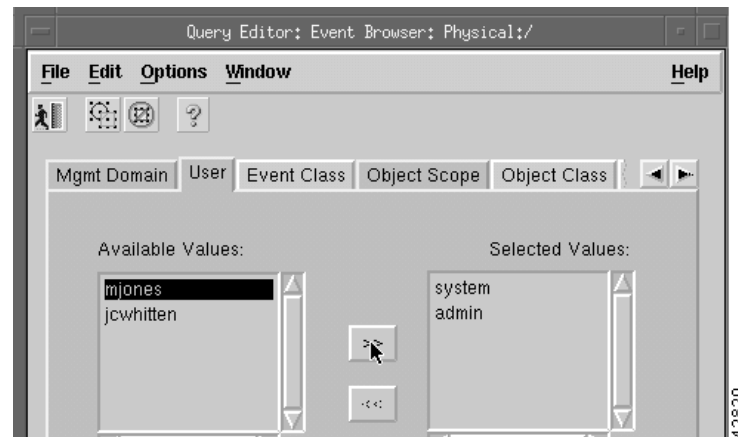
You see the screen in Figure 8-14.

Figure 8-14 Query Editor Screen—Mgmt Domain Tab



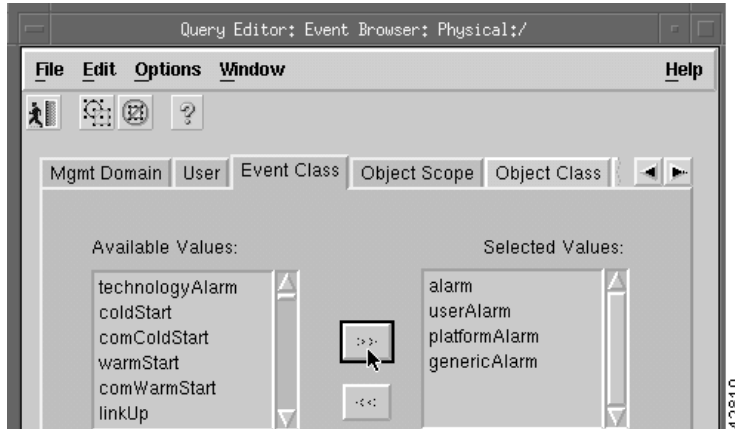
- Step 11** From the Available Values list, select management domains and click the right arrows to transfer the values to the Selected Values list.
- Step 12** Click the arrows on the right side of the tabs to scroll to additional tabs.
- Step 13** Click the **User** tab.
You see the screen in Figure 8-15.

Figure 8-15 Query Editor Screen—User Tab



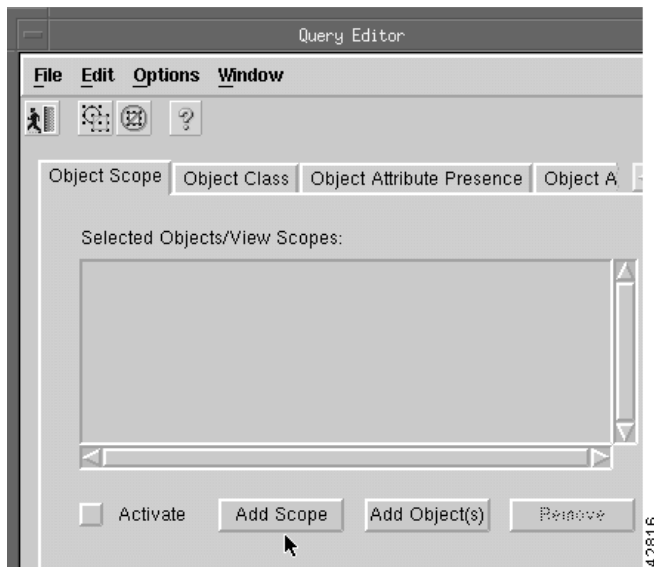
- Step 14** From the Available Values list, select users and click the right arrows to transfer the values to the Selected Values list.
- Step 15** Click the **Event Class** tab.
You see the screen in Figure 8-16.

Figure 8-16 Query Editor Screen—Event Class Tab



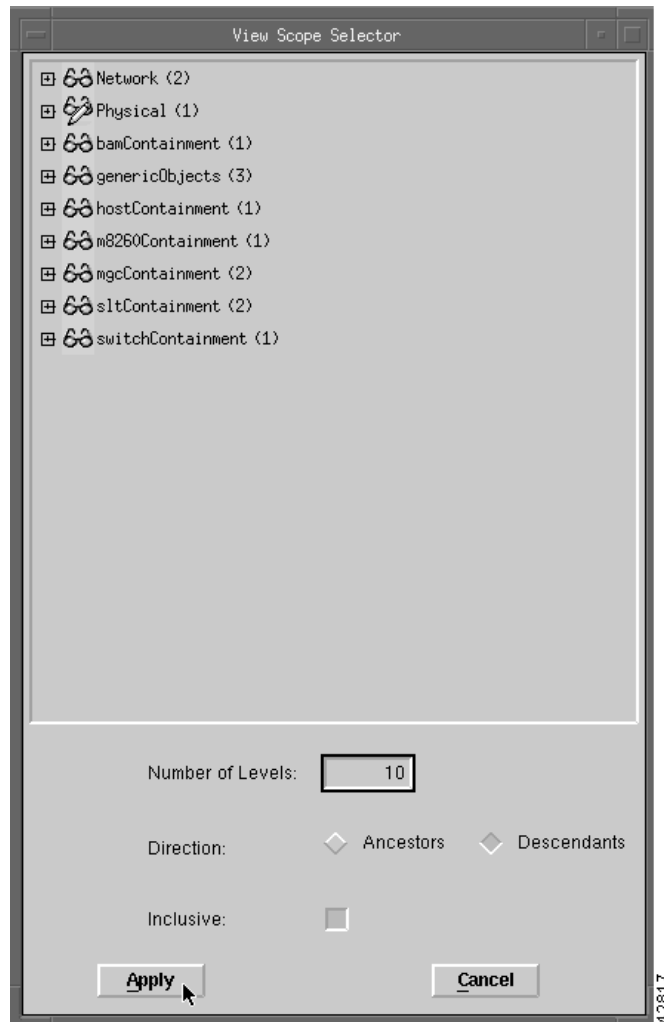
- Step 16** From the Available Values list, select event classes and click the right arrows to transfer the values to the Selected Values list.
- Step 17** Click the **Object Scope** tab to display all the events of a node and all its children.
You see the screen in Figure 8-17.

Figure 8-17 Query Editor Screen—Object Scope Tab



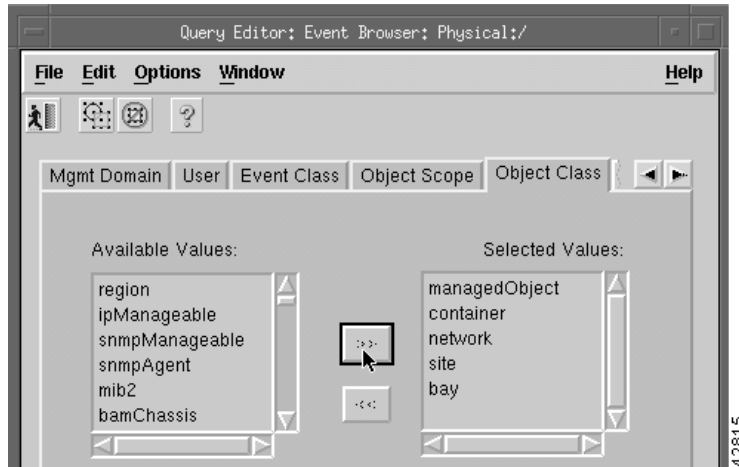
- Step 18** Click **Add Scope**.
You see the screen in Figure 8-18.

Figure 8-18 View Scope Selector Screen



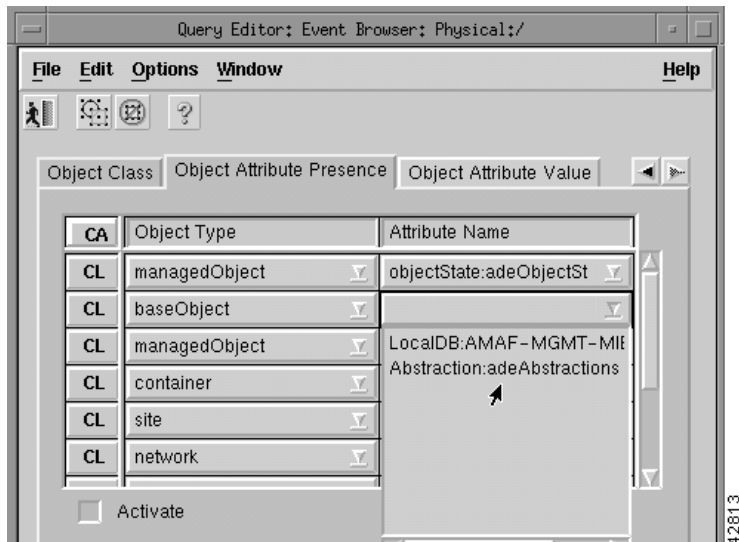
- Step 19** In the View Scope selector, select the node.
- Step 20** Type the number of levels to view. This can be more than needed.
- Step 21** Click the diamond to the left of Descendants and click **Apply**.
- Step 22** On the Query Editor screen, click the **Object Classes** tab.
You see the screen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

Figure 8-19 Query Editor Screen—Object Class Tab



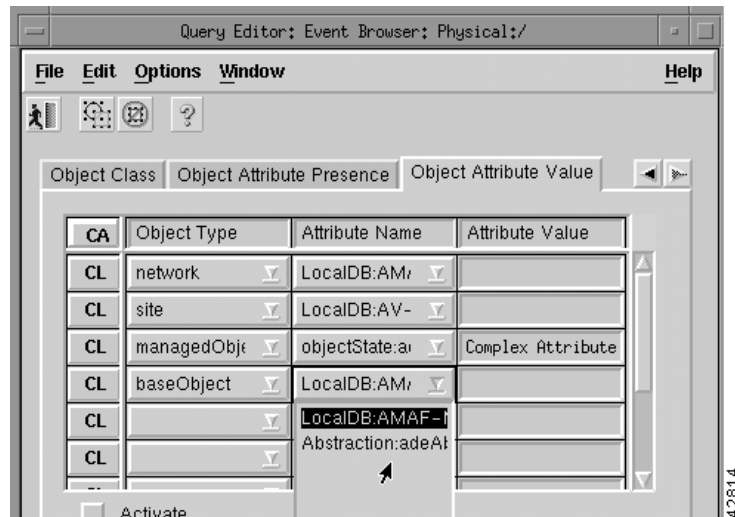
- Step 23** From the Available Values list, select the desired object classes and click the right arrows to transfer the values to the Selected Values list.
- Step 24** Click the **Object Attribute Presence** tab. Click a pull-down menu under Object Type to select a value and click a pull-down menu under Attribute Name to select a value, as shown in Figure 8-20.

Figure 8-20 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 8-21.

Figure 8-21 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

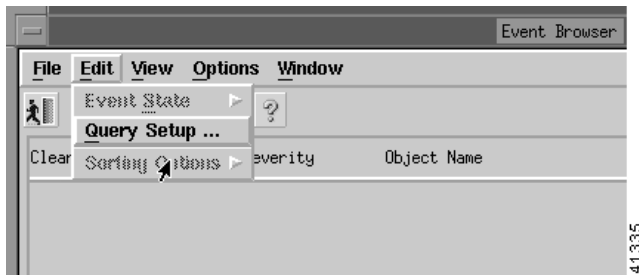
Query changes are saved for the immediate session only. When you close the Event Browser, the query criteria is reset to the default.

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 8-22.

Figure 8-22 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 8-24.
- 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.

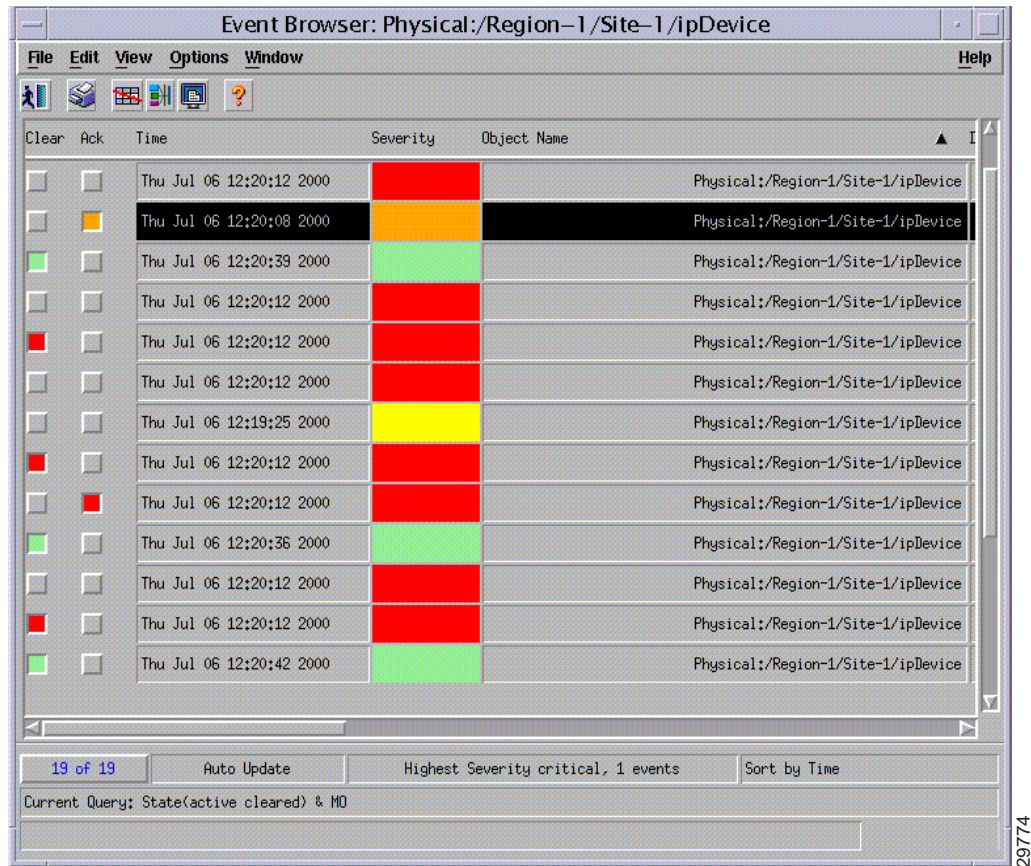
To view the event history:

-
- Step 1** Configure the event query (refer to the “Filtering Events Using Queries” section on page 8-23.)
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 8-23 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 8-24 is displayed.

Figure 8-24 Full Event Description Screen

The screenshot shows a window titled "Full Event Description" with the following fields and sections:

- Object Name:** IpDevice
- Severity:** critical
- Time and Date:** 10/07/99 16:19:36
- Event State:** Cleared/Unacknowledged
- Management Domain:** (empty)
- Communication Domain:** (empty)
- Event Description:** No Description Available
- Acknowledgement Details:**
 - Acknowledgement User: (empty)
 - Acknowledgement Time and Date: (empty)
 - Acknowledgement Comment: (empty)
- Clearing Details:**
 - Clearing Method: User
 - User Responsible for Clearing: admin
 - Clearing Time and Date: 10/08/99 11:30:50
 - Clearing Reason: Engineer informed

At the bottom of the window are two buttons: "Clearing Event" and "Close". A small number "29775" is visible in the bottom right corner of the window frame.



Note

If the event has not been cleared, the Event State displays Active and the Clearing Method, User Responsible for Clearing, and 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—The Communications domain from which the event was reported
- Management Domain—The Management domain from which the event was reported
- Event Description—A brief description of the reported event
- Event State—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

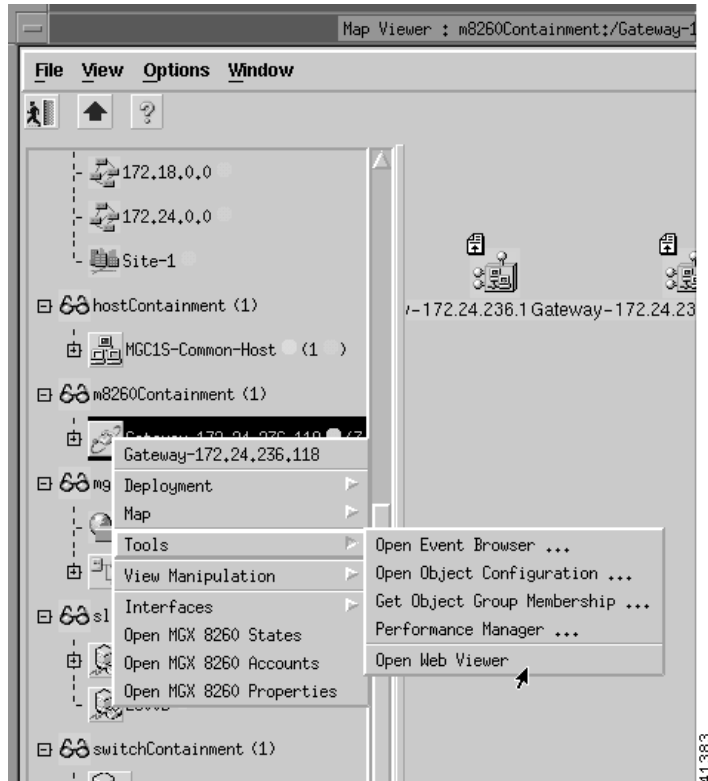
- Clearing Method—Indicates if the event was cleared by the network or by a user.
- User Responsible for Clearing—Displays the user name responsible for clearing the event.
- Clearing Time and Date—Indicates the time and date the event was cleared.
- Reason for clearing—The information that was entered 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, select **Tools**, then select **Open Web Viewer**, as shown in Figure 8-25.

Figure 8-25 Map Viewer Screen—Tools>Open Web Viewer Option



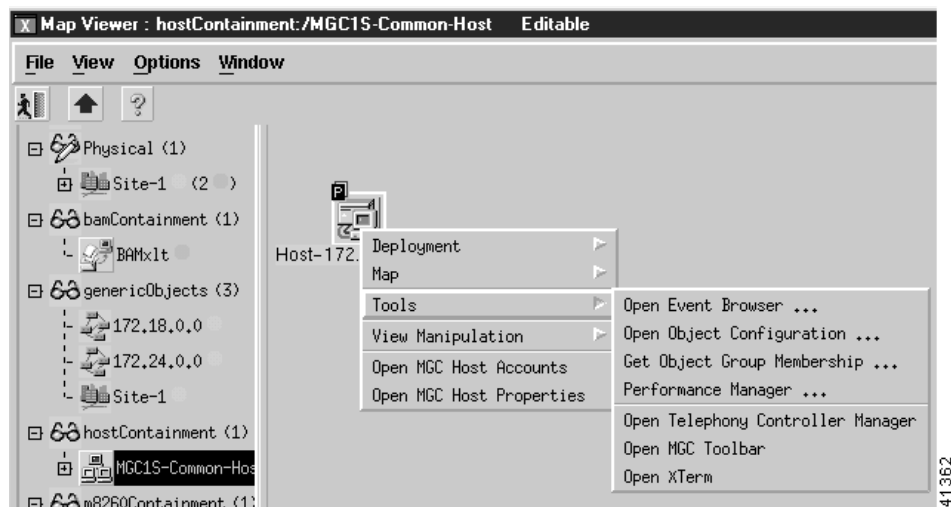
Step 2 When the Web Browser appears, type your user ID and password and click **Login**.

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 8-26.

Figure 8-26 Map Viewer Screen—Tools>Open MGC Toolbar Option



You see the screen in Figure 8-27.

Figure 8-27 MGC Toolbar



From the MGC Toolbar you can click the following buttons:

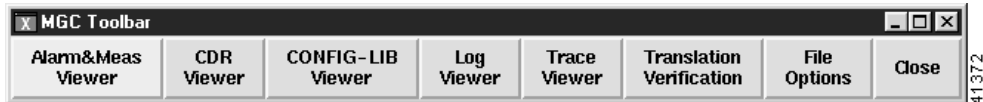
- Alarm&Meas Viewer—View alarms on the Cisco MGC host.
- CDR Viewer—View call detail records (CDRs).
- CONFIG-LIB Viewer—Configure a library.
- Log Viewer—View a log file.
- Trace Viewer—View a trace file.
- Translation Verification—Verify a translation.
- File Options—View a configuration of the files.

- Close—Close the MGC Toolbar.

Alarm and Measurements Viewer

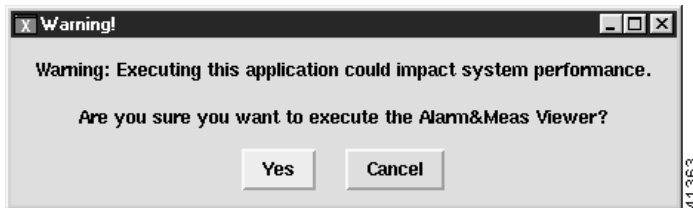
Step 1 On the MGC Toolbar, click **Alarm&Meas Viewer** to view alarms on the Cisco MGC host.

Figure 8-28 MGC Toolbar—Alarm&Meas Viewer Option



You see the screen in Figure 8-29.

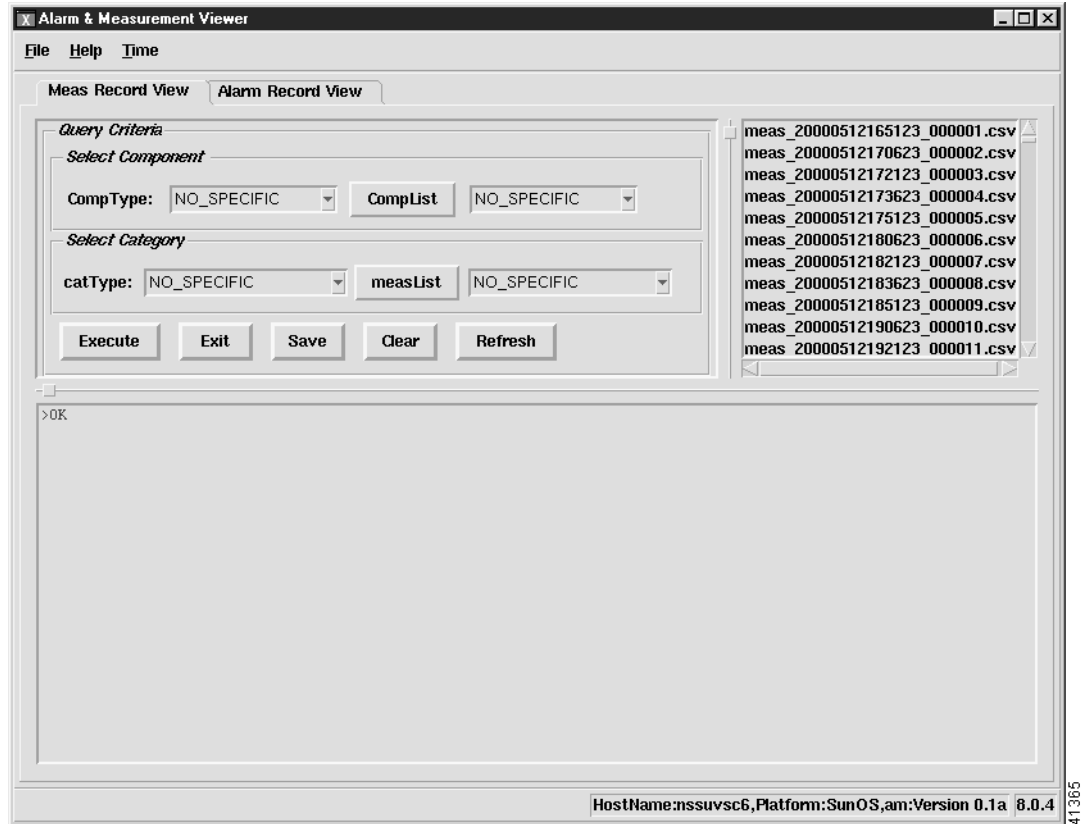
Figure 8-29 Alarm&Meas Viewer Warning Screen



Step 2 Click **Yes**.

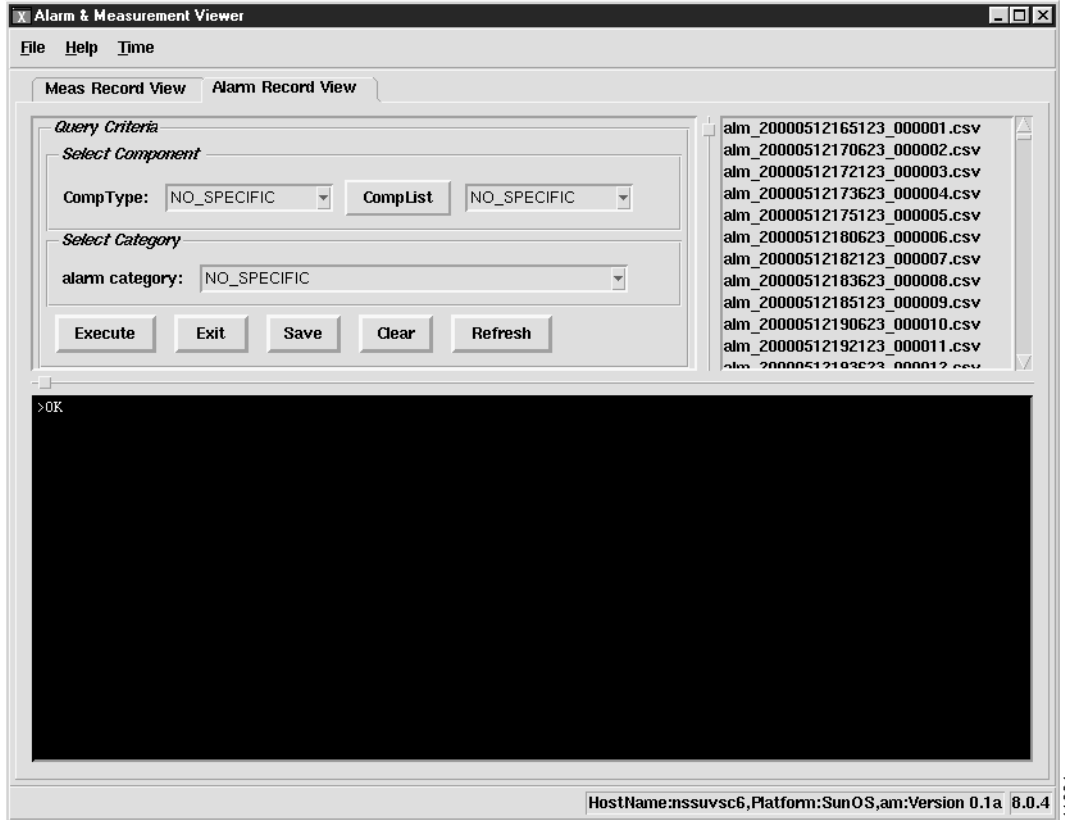
You see the screen in Figure 8-30.

Figure 8-30 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 8-31.

Figure 8-31 Alarm & Measurement Viewer Screen—Alarm Record View Tab

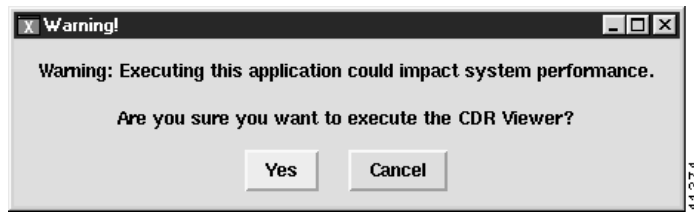


- Step 8** In the Select Component box, use the Comp Type and CompList pull-down menus to select values.
- Step 9** In the Select Category box, use the alarmCategory pull-down menu to select a value.
- Step 10** Select a file from the list on the right of the screen.
- Step 11** Click **Execute** to run the query.
- The results appear in the box at the bottom of the screen.

CDR Viewer

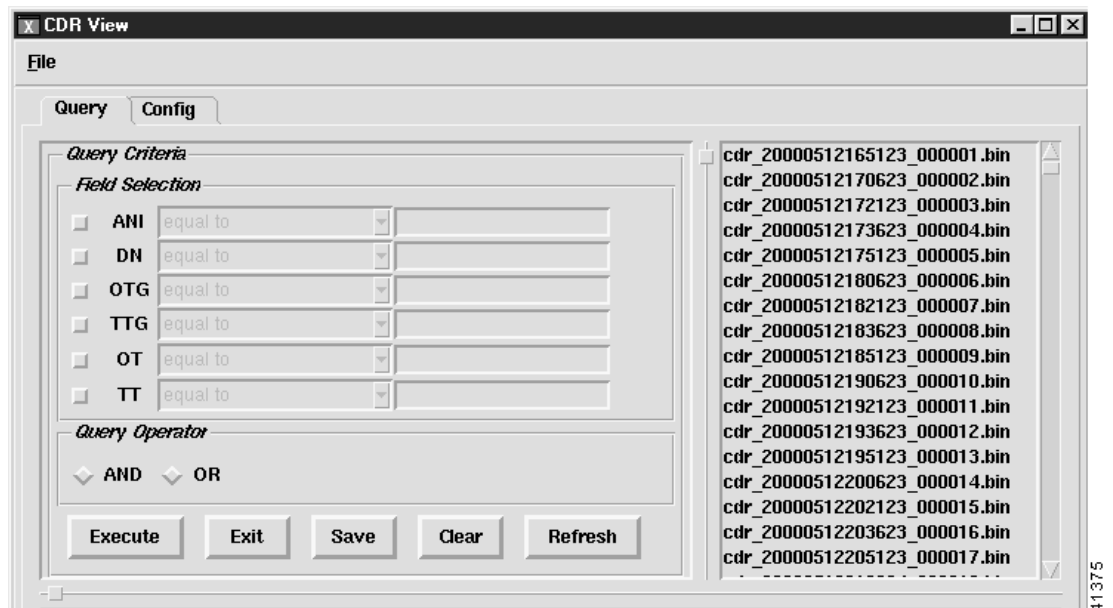
- Step 1** On the MGC Toolbar, click **CDR Viewer** to view CDR records.
- You see the screen in Figure 8-32.

Figure 8-32 CDR Viewer Warning Screen



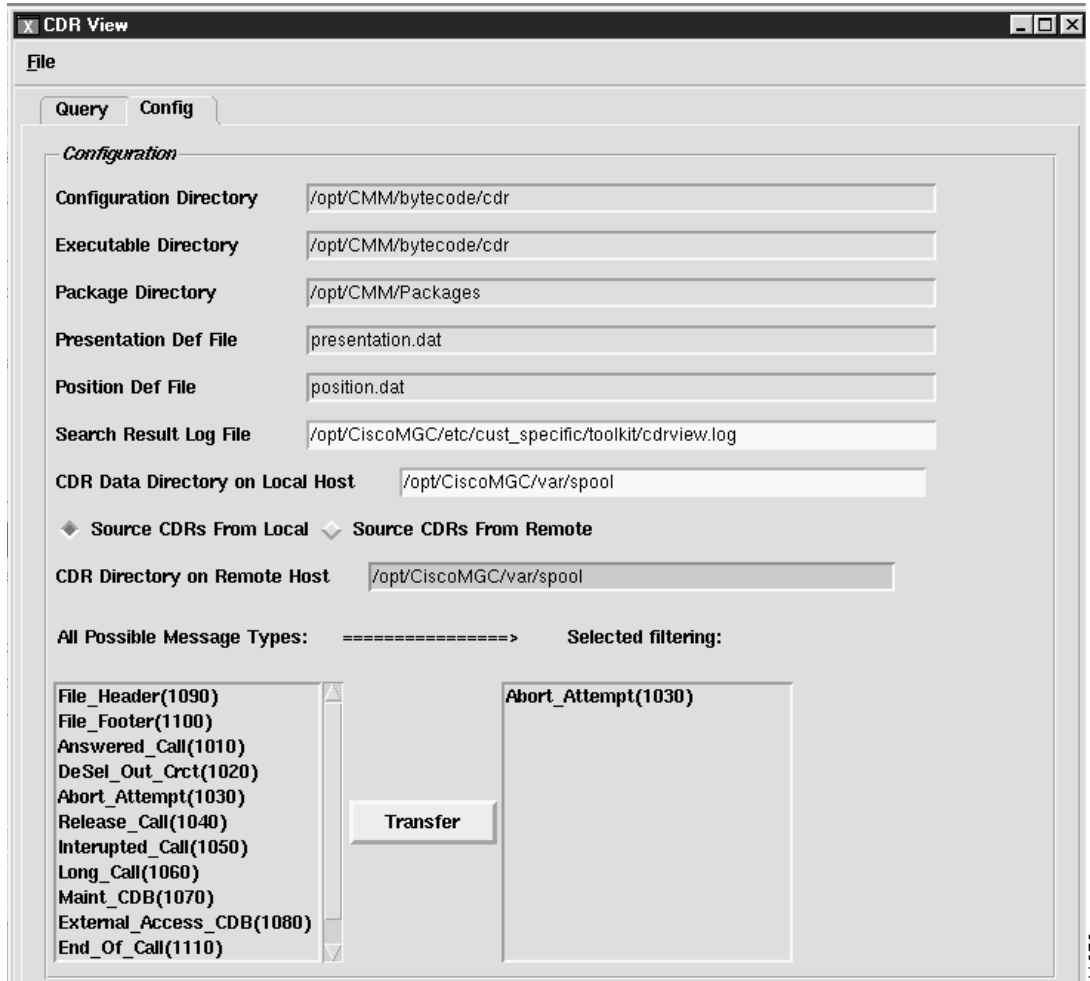
- Step 2** Click **Yes** to proceed.
 You see the screen in Figure 8-33.

Figure 8-33 CDR View Screen—Query Tab



- Step 3** Select an action to perform.
Step 4 Click the **Config** tab.
 You see the screen in Figure 8-34.

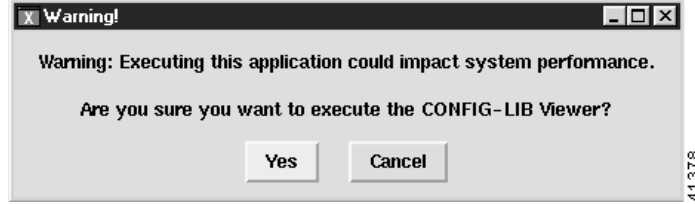
Figure 8-34 CDR View Screen—Config Tab



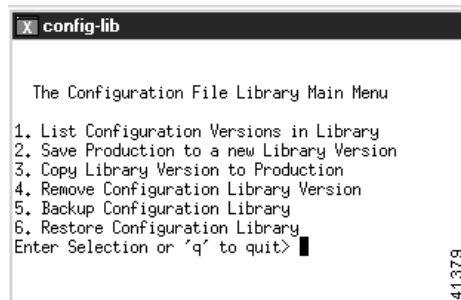
- Step 5** From the All Possible Message Types list, select the messages you want to filter and click **Transfer** to transfer them to the Selected filtering list.

CONFIG-LIB Viewer

- Step 1** On the MGC Toolbar, click **CONFIG-LIB Viewer** to configure a library.
You see the screen in Figure 8-35.

Figure 8-35 CONFIG-LIB Viewer Warning Screen

- Step 2** Click **Yes** to continue.
You see the screen in Figure 8-36.

Figure 8-36 config-lib Screen

- Step 3** Enter the number of the list item to be executed and press **Enter**.

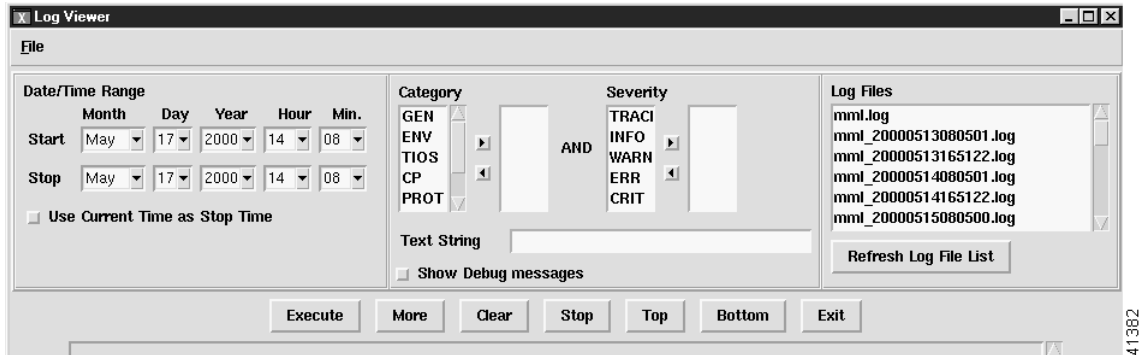
Log Viewer

- Step 1** On the MGC Toolbar, click **Log Viewer** to view a log file.
You see the screen in Figure 8-37.

Figure 8-37 Log Viewer Warning Screen

- Step 2** Click **Yes** to proceed.
You see the screen in Figure 8-38.

Figure 8-38 Log Viewer Screen



Step 3 Select categories and severities from the lists, then select a log file.

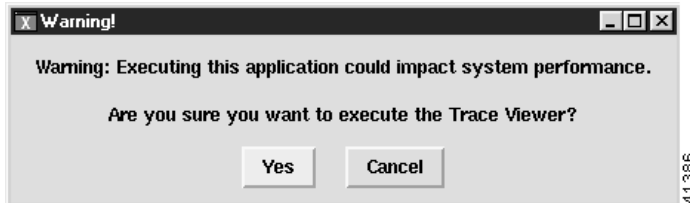
Step 4 Select an action to execute.

Trace Viewer

Step 1 On the MGC Toolbar, click **Trace Viewer** to view a trace file.

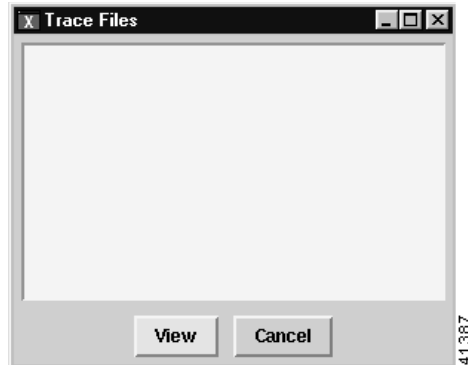
You see the screen in Figure 8-39.

Figure 8-39 Trace Viewer Warning Screen



Step 2 Click **Yes** to continue.

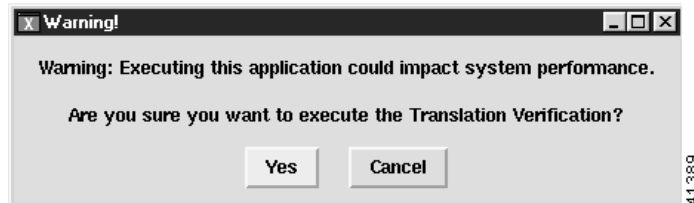
You see the screen in Figure 8-40.

Figure 8-40 Trace Files Screen

Step 3 Select a trace file to view and click **View**.

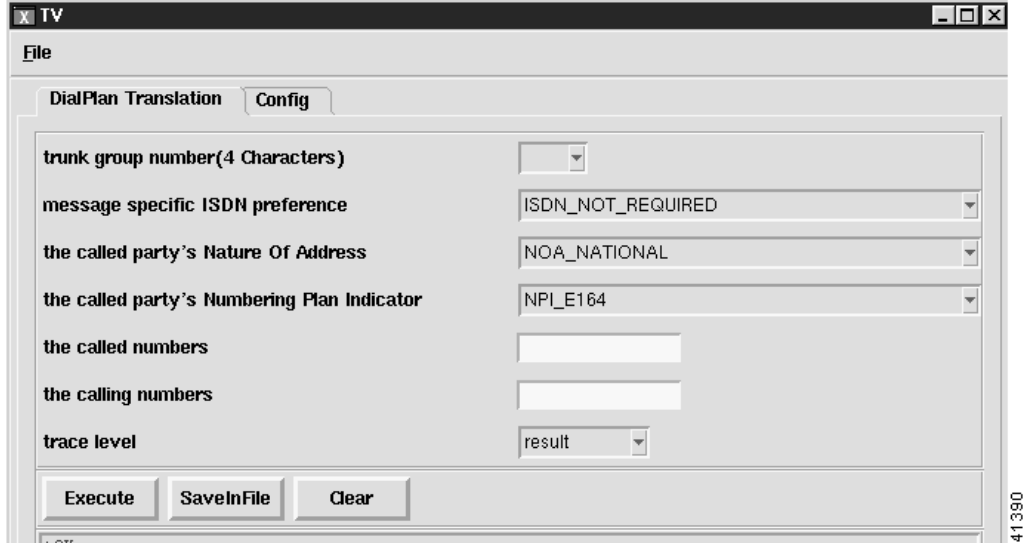
Translation Verification

Step 1 On the MGC Toolbar, click **Translation Verification** to verify a translation. You see the screen in Figure 8-41.

Figure 8-41 Translation Verification Warning Screen

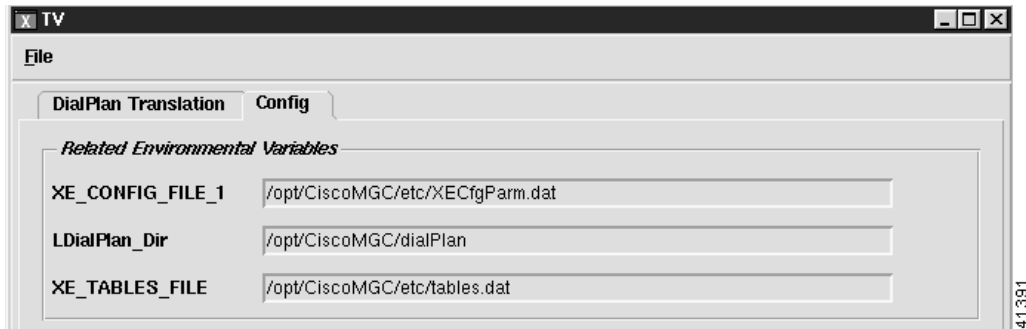
Step 2 Click **Yes** to continue. You see the screen in Figure 8-42.

Figure 8-42 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 8-43.

Figure 8-43 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 8-44.

Figure 8-44 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 8-18.

Table 8-18 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 MGC host file systems
- Cisco SLT accounts
- Cisco SLT properties
- LAN switch accounts
- LAN switch properties
- BAMS accounts
- BAMS properties
- BAMS file systems
- CIAgent device information
- Ethernet interface properties
- TDM interface properties
- Serial interface properties

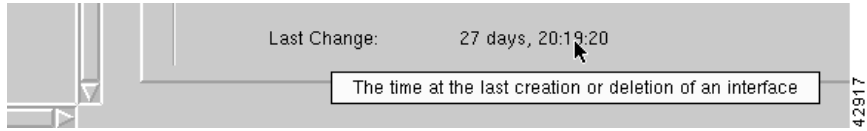
Viewing Accounts and Properties

For detailed information, you can view accounts and properties from the Map Viewer by clicking **View** on the CEMF Launchpad.



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 Cisco MGC host.
 - Step 2** Right-click to display the pull-down menu, then select **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.

- Step 3** Click the **SNMP** tab to view SNMP properties for the selected Cisco MGC host. You see the screen in Figure 9-3.

Figure 9-3 MGC Host Accounts Screen—SNMP Tab



Viewing Cisco MGC Host Properties

To view Cisco MGC host properties:

- Step 1** From the Map Viewer, select the Cisco MGC host.
- Step 2** Right-click to display the pull-down menu, then select **Properties**. You see the screen in Figure 9-4 with the properties of the Cisco MGC host displayed on the General tab.

Figure 9-4 MGC Properties Screen—General Tab



- Step 3** Click the **Detail** tab to view the configuration of the selected Cisco MGC host.
You see the screen in Figure 9-5.

Figure 9-5 *MGC Properties Screen—Detail Tab*



- Step 4** Click the **Host** tab to view the host configuration.
You see the screen in Figure 9-6.

Figure 9-6 MGC Properties Screen—Host Tab



- Step 5** Click the **Network** tab to view the host and peer network addresses.
You see the screen in Figure 9-7.

Figure 9-7 *MGC Properties Screen—Network IP Addresses Tab*



- Step 6** Click the **Software** tab to view the software on the selected Cisco MGC host.
You see the screen in Figure 9-8.

Figure 9-8 MGC Properties Screen—Software Tab



Viewing Cisco MGC Host File Systems

To view Cisco MGC host file systems:

-
- Step 1** From the Map Viewer, select the Cisco MGC host.
 - Step 2** Right-click to display the pull-down menu, then select **File Systems**.

You see the screen in Figure 9-9 with the file systems of the Cisco MGC host displayed on the General tab.

Figure 9-9 MGC File Systems Screen—General Tab



- Step 3** Click the **Monitor** tab to view the file systems of the selected Cisco MGC host that you can monitor. You see the screen in Figure 9-10.

Figure 9-10 MGC File Systems Screen—Monitor Tab



- Step 4** Click the **Exceptions** tab to view the Cisco MGC host exceptions.
You see the screen in Figure 9-11.

Figure 9-11 MGC File Systems Screen—Exceptions 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 **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 with the account information for the selected Cisco SLT.

Figure 9-12 SLT Accounts Screen



- Step 3** Click the **SNMP** tab to view SNMP properties for the selected Cisco SLT.
You see the screen in Figure 9-13.

Figure 9-13 SLT Accounts Screen—SNMP Tab



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 **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 9-14 with the properties of the Cisco SLT displayed on the General tab.

Figure 9-14 SLT Properties Screen—General Tab



- Step 3** Click the **Details** tab to view details about the selected Cisco SLT.
You see the screen in Figure 9-15.

Figure 9-15 SLT Properties Screen—Details Tab



- Step 4** Click the **Network** tab to view the IP addresses configured on the selected Cisco SLT. You see the screen in Figure 9-16.

Figure 9-16 SLT Properties Screen—Network Tab



- Step 5** Click the **Memory** tab to view memory pool for the selected Cisco SLT.
You see the screen in Figure 9-17.

Figure 9-17 SLT Properties Screen—Memory Tab



- Step 6** Click the **Configuration** tab to view the configuration information for the selected Cisco SLT. You see the screen in Figure 9-18.

Figure 9-18 SLT Properties Screen—Configuration 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 **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 9-19.

Figure 9-19 LAN Switch Accounts Screen



- Step 3** Click the **SNMP** tab to view SNMP properties for the selected LAN switch.
You see the screen in Figure 9-20.

Figure 9-20 LAN Switch Accounts Screen—SNMP Tab



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 **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 9-21.

Figure 9-21 LAN Switch Properties Screen—General tab



Step 3 Click the **Details** tab.

You see the screen in Figure 9-22 with details for the selected LAN switch.

Figure 9-22 LAN Switch Properties Screen—Details Tab



Step 4 Click the **Network** tab.

You see the screen in Figure 9-23 with the IP addresses for the selected LAN switch.

Figure 9-23 LAN Switch Properties Screen—Network Tab



- Step 5** Click the **Memory** tab.
- Step 6** Select a memory pool supported by the LAN switch.
You see the screen in Figure 9-24 with the details for the selected memory pool displayed.

Figure 9-24 LAN Switch Properties Screen—Memory Tab



Step 7 Click the **Configuration** tab.

You see the screen in Figure 9-25 with the configuration information displayed.

Figure 9-25 LAN Switch Properties Screen—Configuration 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 **BAMS**, then select **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 9-26 with the account information displayed for the selected BAMS.

Figure 9-26 BAM Accounts Screen



- Step 3** Click the **SNMP** tab to view SNMP properties for the selected BAMS.
You see the screen in Figure 9-27.

Figure 9-27 BAMS Accounts Screen—SNMP Tab



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 **BAMS**, then select **Properties**.
You see the screen in Figure 9-28 with the properties of the selected BAMS displayed.

Figure 9-28 BAM Properties Screen



Step 3 Click the **Details** tab.

You see the screen in Figure 9-29 with configuration information for the selected BAMS.

Figure 9-29 BAM Properties Screen—Details Tab



Step 4 Click the **BAMS** tab.

You see the screen in Figure 9-30 with information about the selected BAMS.

Figure 9-30 BAM Properties Screen—BAMS Tab



- Step 5** Click the **Network** tab.
You see the screen in Figure 9-31 with IP addresses for the selected BAMS.

Figure 9-31 *BAM Properties Screen—Network Tab*



Step 6 Click the **Poll** tab.

You see the screen in Figure 9-32 with polling information for the selected BAMS.

Figure 9-32 *BAM Properties Screen—Poll Tab*



Step 7 Click the **Software** tab.

You see the screen in Figure 9-33 with the software running on the selected BAMS.

Figure 9-33 *BAM Properties Screen—Software Tab*



Viewing BAMS File Systems

To view BAMS file systems:

-
- Step 1** From the Map Viewer, select the BAMS.
 - Step 2** Right-click to display the pull-down menu, then select **File Systems**.
You see the screen in Figure 9-34 with the file systems of the BAMS displayed on the General tab.

Figure 9-34 BAMS File Systems Screen—General Tab



- Step 3** Click the **Monitor** tab to view the file systems of the selected BAMS that you can monitor. You see the screen in Figure 9-35.

Figure 9-35 BAMS File Systems Screen—Monitor Tab



- Step 4** Click the **Exceptions** tab to view the BAMS exceptions.
You see the screen in Figure 9-36.

Figure 9-36 BAMS File Systems Screen—Exceptions Tab



Viewing CIAgent Device Information

You can look at the following CIAgent device information:

- Disk partitions
- Processor
- RAM
- Virtual memory



Note

For more information about CIAgent device information, see the “Performance Data Collected for the CIAgent System Components” section on page 7-8.

To view CIAgent device information:

-
- Step 1** From the Map View, select a BAMS.
- Step 2** Right-click to display the pull-down menu, select **Devices**, then select one of the following:
- **Disk Partitions**—You see the screen in Figure 9-37.
 - **Processor**—You see the screen in Figure 9-38.
 - **Ram**—You see the screen in Figure 9-39.
 - **Virtual Memory**—You see the screen in Figure 9-40.

Figure 9-37 CIAgent Device Information—Disk Partitions



Figure 9-38 CIAgent Device Information—Processor



Figure 9-39 CIAgent Device Information—RAM



Figure 9-40 CIAgent Device Information—Virtual Memory



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 **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 9-41 with the properties of the selected interface displayed on the General tab.

Figure 9-41 *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 9-42.

Figure 9-42 Ethernet Properties Screen—Details Tab



Viewing TDM Interface Properties

To view Time Division Multiplexing (TDM) interface properties:

-
- Step 1** From the Map Viewer, select the TDM.
- Step 2** Right-click to display the pull-down menu, then select **Properties**.

You see the screen in Figure 9-43 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 9-43 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 9-44.

Figure 9-44 TDM Properties Screen—Details 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 **Properties**.
You see the screen in Figure 9-45 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 9-45 *Serial Interface Properties Screen—General Tab*



Step 3 Select the interface type from the pull-down menu as shown in Figure 9-46.

Figure 9-46 Serial Interface Properties Screen—Interface Type Pull-down Menu



- Step 4** Select **Admin Status**.
- Step 5** Select **Operational Status** as shown in Figure 9-47.

Figure 9-47 *Serial Interface Properties Screen—Operational Status Pull-down Menu*



- Step 6** Click the **Details** tab.
You see the screen in Figure 9-48 with the transmission details for the selected interface displayed.

Figure 9-48 Serial Interface Properties Screen—Details Tab

Using Diagnostic Tools

CMNM provides a number of tools to monitor the health of the network elements. Most tools are accessible via the context-menu (right-click) associated with objects. Other diagnostic tools are available using a button in the diagnostics dialog.

For all IP devices, CMNM allows you to launch a ping application to test network connectivity. When you select the ping menu item, the standard UNIX ping application is displayed. By using the ping application, you can tell the difference between an SNMP agent failure (heartbeat polling) and a true network connectivity failure.

Other diagnostic tools are also offered depending on the type of device. The diagnostic tools that are launched via the context-menu service are indicated as type S; the remaining diagnostic tools, launched using a button in the diagnostics dialog, are indicated as type D, as shown in Table 9-1.

Table 9-1 Diagnostic and Configuration Tools

Diagnostic Tool	Available Devices	Description	Type
IP Ping	All IP devices	Standard UNIX ping application	D
SNMP Ping	All IP devices	On-demand status poll/SNMP query	D

Table 9-1 Diagnostic and Configuration Tools

Diagnostic Tool	Available Devices	Description	Type
Traceroute	All IP devices	Standard UNIX traceroute application	D
Alarm Log	Cisco MGC host/BAMS	Displays and saves current alarm log (see the “Processes and Alarms” section on page 9-50)	D
Process Status	Cisco MGC host/BAMS	Displays and saves current process status (see the “Processes and Alarms” section on page 9-50)	D
System Log	BAMS	Displays the BAMS system log	D
Status Check	Cisco MGC host	See the “MGC Host Status Check” section on page 9-49	D
Cross-Device Audit	BAMS	Audits BAMS against the Cisco MGC host configuration (see the “Configuration Audit” section on page 9-50)	D
Telnet	All IP devices	Standard Telnet application	S
MGC Toolbar	Cisco MGC host	MGC diagnostic tools toolbar	S
Xterm	MGC Host/BAMS	Standard Xterm application	S
CiscoView	Cisco SLT/LAN switch	CiscoView application	S
VSPT	Cisco MGC node	Voice Services Provisioning Tool	S
CMM	Cisco MGC host	Cisco MGC Manager	S
Web Viewer	Cisco SLT/ LAN switch	Launches web browser pointing to device	S

MGC Host Status Check

CMNM provides an entire suite of tools that can be used to determine various facets of the Cisco MGC host's operating status. The MGC Host Status Check dialog contains a number of buttons that let you invoke different status check services as shown in Table 9-2.

Table 9-2 Status Check Operations

Operation	Description
rtrv-admin-state	Retrieves the administrative state for all (applicable) components.
rtrv-dest	Retrieves state information for all DPCs ¹ and Signaling Paths.
rtrv-eqpt	Retrieves service state of all I/O cards.
rtrv-ne-health	Retrieves CPU occupancy and disk utilization (8.x).
rtrv-lnk-ctr	Retrieves all linkset service states.
rtrv-ssn	Retrieves the state of all local SSNs.
rtrv-rte	Retrieves the SS7 routes for all point codes.
rtrv-sc	Retrieves the attributes of all signaling channels and linksets.
rtrv-rssn	Retrieves the state of all remote SSNs ² .
rtrv-tc	Retrieves the state of bearers for all signaling paths.

1. Destination point codes
2. Subsystem numbers

Because these commands may be time-consuming, you always see a warning dialog asking you if you want to run the command.

After the command is run, you see the results in the Action Result window. If the diagnostic command generates more information than can be shown in the Action Result window, the results are written to a file and you see the name of that file.

Configuration Audit

CMNM lets you initiate an audit whereby the trunking information on the BAMS is compared to the trunking information on its associated Cisco MGC hosts. This operation collects all trunking information and performs a step-by-step comparison to identify any discrepancies. Any differences are displayed in the Action Result window and written to a file.

You can launch the audit service from any BAMS diagnostic dialog. CMNM retrieves all of the trunking information on the BAMS using the **prov-rtrv:trunkgrp** command. The system then retrieves the trunking information for all of the Cisco MGC hosts associated with the selected BAMS. A step-by-step comparison is done to ensure that all of the trunk groups or circuits defined on the BAMS are in synchrony with all of the Cisco MGC hosts associated with this BAMS.

Processes and Alarms

The alarm log is retrieved using the **rtrv-alm**s MML command. The process status is retrieved using the **rtrv-softw:all** MML command.

On the BAMS, the system log is retrieved using the MML command:

```
RTRV-FILES::/acec/files/syslog
```

CMNM provides the mechanism to retrieve and view the alarm and system logs. In addition, CMNM provides a mechanism that lets you save the alarm log or system log to a file on the management system so that an external system can retrieve it.

File System Monitor

The CIAgent lets you monitor file systems on devices where the supported SNMP agent is installed. The CIAgent is installed on Cisco MGC host and BAMS devices.

CIAgent monitors each file system and sends a trap if file system utilization reaches a threshold you define. Each file system is polled at a frequency you define. You can specify an overall (global) polling frequency or you can specify individual polling frequencies for each filesystem. You can turn traps on or off for individual file systems.

Each file system is represented by an entry in the SIFSMONITOR-MIB.siFsMonitorTable. CMNM implements a dialog that lets you view and manipulate the polling frequencies and thresholds for each file system. You can also view utilization of each file system (SNMP:SIFSMONITOR-MIB.siFsTable) and those file systems that have exceeded the specified threshold values (SNMP:SIFSMONITOR-MIB.siFsExceptionTable).

Identifying Where You Can Launch Features in CMNM

Table 9-3 shows you from where you can launch the various features in CMNM.

Table 9-3 Launching CMNM Features

Feature	Launch Point	Description
MGC Node Deployment	MGC-Node-View	Deploys a new Cisco MGC node object
MGC Host Deployment	Host-View, MGC Node	Deploys a new Cisco MGC host device
SLT Deployment	SLT-View, MGC Node	Deploys a new Cisco SLT device
LAN Switch Deployment	Switch-View, MGC Node	Deploys a new LAN switch device
BAMS Deployment	BAMS-View, MGC Node	Deploys a new BAMS device
Seed File Deployment	All Views	Displays Seed File deployment dialog
Trap Forwarding Dialog	All Views	Displays Trap forwarding dialog
Performance Manager	MGC Node, BAMS, SLT, LAN Switch	Opens Performance Manager application
MGC Node States	MGC-Node-View, MGC Node	Opens MGC Node States dialog
MGC Host Properties	Host-View, MGC Host	Opens Host Properties dialog
MGC Host File Systems	Host-View, MGC Host	Opens Host File System properties dialog
MGC Host States	Host-View, MGC Host	Opens Host States dialog
MGC Host Accounts	Host-View, MGC Host	Opens Host Accounts dialog
MGC Host Diagnostics	Host-View, MGC Host	Opens Host Diagnostic dialog
MGC Host Image/Configuration Download/Upload	Host-View, MGC Host	Opens MGC Host Software Image/Configuration Backup/Restore dialog
SLT Properties	SLT-View, SLT	Opens SLT Properties dialog
SLT States	SLT-View, SLT	Opens SLT States dialog
SLT Accounts	SLT-View, SLT	Opens SLT Accounts dialog
SLT Diagnostics	SLT-View, SLT	Opens SLT Diagnostic dialog
SLT Image/Configuration Download/Upload	SLT-View, SLT	Opens SLT Software Image/Configuration Backup/Restore dialog
LAN Switch Properties	Switch-View, LAN Switch	Opens LAN Switch Properties dialog
LAN Switch States	Switch-View, LAN Switch	Opens LAN Switch States dialog
LAN Switch Accounts	Switch-View, LAN Switch	Opens LAN Switch Accounts dialog
LAN Switch Diagnostics	Switch-View, LAN Switch	Opens LAN Switch Diagnostic dialog
LAN Switch Image/Configuration Download/Upload	Switch-View, LAN Switch	Opens LAN Switch Software Image/Configuration Backup/Restore dialog
BAMS Properties	BAMS-View, BAMS	Opens BAMS Properties dialog
BAMS File Systems	BAMS-View, BAMS	Opens BAMS File System properties dialog

Table 9-3 Launching CMNM Features

BAMS States	BAMS-View, BAMS	Opens BAMS States dialog
BAMS Accounts	BAMS-View, BAMS	Opens BAMS Accounts dialog
BAMS Diagnostics	BAMS-View, BAMS	Opens BAMS Diagnostic dialog
BAMS Image/Configuration Download/Upload	BAMS-View, BAMS	Opens BAMS Software Image/Configuration Backup/Restore dialog
Trunking Configuration Audit	BAMS	Opens the Configuration Audit dialog
Signaling Dialogs	Signaling Folder, All Signaling components	Opens the various Signaling component property dialogs, one for each type of signaling component
Trunking Dialogs	Trunking Folder, All Trunking components	Opens the various Trunking component property dialogs, one for each type of trunking component
Routing Dialogs	Routing Folder, All Routing Components	Opens the various Routing component property dialogs, one for each type of routing component
Network Interface/Subrack Component Properties	Various	Opens the properties dialog for the network interface and subrack components (interfaces, ports, slots, and so on)
SS7 MTP2 Channel Properties	SLT, MTP2 Channels	Opens the SS7 MTP2 Properties dialog
CIAgent Component Properties	CIAgent Components	Opens the properties dialogs for the various CIAgent component
VSPT	MGC Node	Launches Voice Services Provisioning Tool application
MGC Toolbar	MGC Host	Launches MGC Host toolbar applications
CMM	MGC Host	Launches Cisco MGC Manager
XTerm	MGC Host, BAMS	Opens an XTerm window
CiscoView	LAN Switch, SLT	Launches CiscoView application
Telnet	MGC Host, BAMS, SLT, LAN Switch	Launches UNIX Telnet application
Web Browser (Netscape)	SLT, LAN Switch	Launches web browser, pointing to the internal web server on Cisco 2600 and Cisco 2900XL devices



BAMS, Cisco MGC, and CMNM Messages

This appendix provides two kinds of information about event messages displayed in the CMNM Event Browser:

- For BAMS and Cisco MGC-related messages, it provides references from which you can navigate to the relevant document to look up the message you are interested in. A short description of each document is included.
- For CMNM internal messages, it provides a short explanation of each message along with any recommended action.

For information on alarm messages for the other devices managed by CMNM, see the following sections of Chapter 8:

- For the Cisco SLT, see Chapter 8, “Cisco SLT Alarms”.
- For Catalyst LAN switches, see Chapter 8, “Catalyst LAN Switch Alarms”.
- For the Cisco MGX 8260, see Chapter 8, “Cisco MGX 8260 Alarms”.

For information on application-related alarm messages for the Cisco MGC Host and the BAMS, see Chapter 8, “MGC Host and BAMS Resource Alarms”.

Looking Up BAMS and Cisco MGC Messages

Use this procedure to locate information for a specific message.

-
- Step 1** In the Event Browser, check the Object Name to determine the network object that generated the event. Note the event description.
 - Step 2** In this document, go to the section that applies to that object.
 - Step 3** Click on the name of the document or section (displayed in blue to indicate a link) that contains the information you want. The linked document opens.
 - Step 4** Press Ctrl+F for your browser’s Find dialog box. In the dialog box, enter some of the initial text of the event description and click OK.



Note

If your search text is not found, it means that the Event Browser description does not exactly match the generated message. You can search on a different part of the description string, or scroll through the document to find the message.

Cisco MGC Host Messages

The Cisco MGC Software Reference Guide (MGC Version 7.0

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/sw_ref/index.htm) is a reference to Cisco MGC MML commands, system messages, XECfgParm, and billing interface. The System Messages chapter documents alarms and informational events in a chart (Table 2-2, Version 7 http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/sw_ref/elsysmsg.htm#83882) that includes the following information on each event:

- Alarm category—Alarm/event message, corresponding to the event description in the CMNM Event Browser.
- Description—Brief description of alarm/event.
- Severity level—The severity of the alarm/event.
- Event reporting—Whether the event is reported to the management interface and can be obtained using SNMP. (In the Event Browser, you will see only those events that are reported.)
- Alarm/event cause—The condition causing the alarm/event.
- SNMP trap type—Which SNMP trap type pertains to the event, displayed with a numeric code for the trap type:
 - 0 = No error
 - 1 = Communication alarm
 - 2 = Quality of service
 - 3 = Processing error alarm
 - 4 = Equipment error alarm
 - 5 = Environment error alarm
- Suggested Action—Recommendations for resolving the problem.

BAMS Messages

The BAMS traps alarms and minor, major, or critical events and forwards them to network management systems such as CMNM. The severity level for message forwarding defaults to minor and above, but may be changed by the BAMS system administrator.

The Billing and Measurements Server (Version 2.x) User Guide

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/bams2/> includes an appendix (Appendix A. Troubleshooting

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/bams2/app_a.htm) that provides a discussion of these messages and their use in troubleshooting. Messages are related to the tasks the BAMS performs, and the appendix also includes an explanation of BAMS tasks. The message documentation is organized by task.

The following categories of information are provided for each system message:

- Message ID—a six-character label that uniquely identifies each message. The first three characters are the application task ID, which identifies the application task that generated the message. (For example, MGR denotes the Manager task and MSC denotes the Mass Storage Control task.) The second three characters are the message number; for example, 013 or 122.
- Text—The verbal part of the message that appears in the system log file, generally corresponding to the event description in the CMNM Event Browser.

- Arguments—Variable parts of the message, enclosed in angle brackets.
- Description—An explanation of the event that generated the message.
- Action—what you should do as a result of the event described in the message. In some cases (for example, informational messages), no action may be required. Actions for error messages (manual, warning, minor, major, and critical) may include steps that should be followed to identify and correct problems. Error actions may also describe how BAMS responds to the specified error condition.

CMNM Internal Messages

The following messages may be generated by CMNM itself and reflect errors in deployment, discovery, or configuration. See the next section, “Solving Deployment and Discovery Errors”, for how to correct deployment and discovery errors.

Table A-1 CMNM Internal Events

Message	Explanation	Action
Subrack discovery failed. Check logs	CMNM failed to discover components on the device. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent does not run on the device, (3) the device is not reachable.	(1) Check the SNMP community strings and correct if needed. (2) If MGC or BAMS, check that the snmpdm and mib2agt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. For more information, refer to the log file <CEMF_INSTALLED_DIR>/logs/mgcController.log
BAMS is not configured to receive Call Data Records from any MGC Host	Since the BAMS server is not configured to collect data from any MGC Host, CMNM cannot deploy the device to the right MGC node. Thus, its alarm status will not be propagated in the MGC-Node-View.	Check your BAMS configuration and check the VSC status.

Table A-1 CMNM Internal Events

Message	Explanation	Action
Could not get BAMS Poll table	CMNM failed to retrieve BAMS configuration via SNMP. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent does not run on the device, (3) the device is not reachable. As a result, CMNM cannot deploy the device to the correct MGC node. Thus, its alarm status will not be propagated in the MGC-Node-View.	(1) Check the SNMP community strings and correct if needed. (2) Check that the snmpdm and sagt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. For more information, refer to the log file <CEMF_INSTALLED_DIR>/logs/mgcController.log.
No IP addresses defined on this device. All traps from it will be ignored.	CMNM failed to find any address on this device via SNMP. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent does not run on the device, (3) the device is not reachable.	(1) Check the SNMP community strings and correct if needed. (2) Check that the snmpdm and mib2agt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.
Could not get password for host <IP Address>	Password is not specified for the deployed VSC host. As a result, CMNM cannot fully discover the device.	Correct the password information, then rediscover the device.
<Host name>: Could not collect inventory: Password not specified	Password is not specified for the deployed device. As a result, CMNM cannot fully discover the device.	Correct the password information, then rediscover the device.
<Host name>: Could not get Host Device table. Check IP address and read-community string.	CMNM failed to retrieve the device table from the device. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent or the hostagt process does not run on the device, (3) the device is not reachable.	(1) Check the SNMP read-community string and correct if needed. (2) Check that the snmpdm and hostagt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.

Table A-1 CMNM Internal Events

Message	Explanation	Action
<Host name>: Could not get Host Files System. Check IP address and read-community string.	CMNM failed to retrieve the device table from the device. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent or the fsagt process does not run on the device, (3) the device is not reachable.	(1) Check the SNMP read-community string and correct if needed. (2) Check that the snmpdm and fsagt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.
<Host name>: Could not get Host Storage table. Check IP address and read-community string.	CMNM failed to retrieve the device table from the device. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent or the hostagt process does not run on the device, (3) the device is not reachable.	(1) Check the SNMP read-community string and correct if needed. (2) Check that the snmpdm and hostagt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.
Could not get IP Address table from <device name>. Check IP address and read-community string.	CMNM failed to retrieve the interface table from the device. The problem may be (1) wrong SNMP community strings, (2) Invalid IP Address, (3) the device is not reachable.	(1) Check the SNMP read-community string and correct if needed. (2) Check the IP address. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.
Failed to launch action <Action name>. Perhaps hostController is not running.	The most probable cause is that the CMNM process <i>hostController</i> is down while CMNM is trying to discover a VSC.	Verify that the hostController is running. For example, enter: <pre>ps -ef grep hostController</pre> If the hostController is running, rediscover the device. If not, contact the TAC.
The IP Address <IP Address> is not reachable.	CMNM failed to do SNMP ping with this address.	Check the network connection.
This device is not reachable.	CMNM cannot reach the device using SNMP. If the device has multiple IP addresses, then all of them are unreachable.	(1) Check the SNMP community strings and correct if needed. (2) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.

Solving Deployment and Discovery Errors

If you receive a message about a problem in device deployment or discovery, use these procedures to change the deployment information or rediscover network elements

Changing Password or Community Strings

To change the password or community strings for a device:

-
- Step 1** In the Map Viewer, select the object and right-click.
 - Step 2** From the pull-down menu, choose Accounts. You see the Accounts dialog box.
 - Step 3** On the Accounts tab, check and if needed change the password.
 - Step 4** On the SNMP tab, check and if needed change the SNMP community strings.
 - Step 5** Click the Save button on the toolbar. Close the dialog box.
 - Step 6** If you made a change in community strings to any device, or in password to the MGC host, rediscover the device as described in “Rediscovering a Device After a Problem” below.
-

Changing IP Address

If the wrong IP address was entered, the device must be redeployed. To redeploy a device:

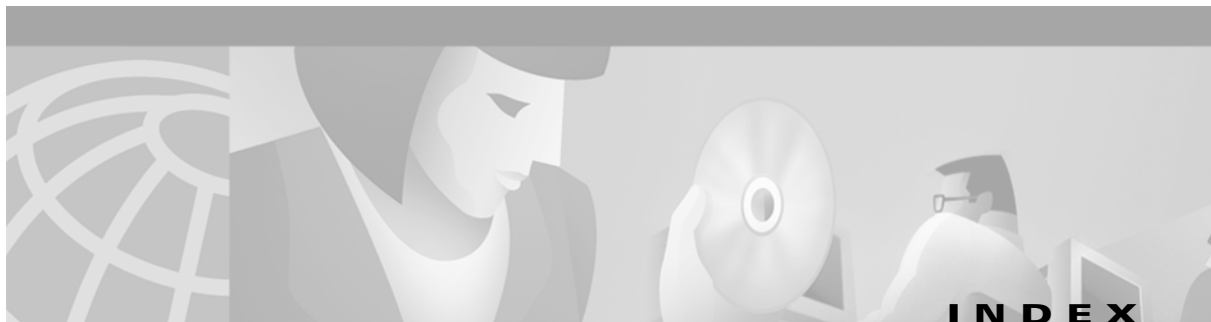
-
- Step 1** In the Map Viewer, select the object and right-click.
 - Step 2** From the pull-down menu, select Deployment and then Delete Objects. You see the Deployment Wizard dialog box with the message, “Ready to delete 1 object”.
 - Step 3** Click the Finish button. You get a message that the object has been deleted. Click OK.
 - Step 4** Redeploy the device following the instructions in Chapter 6, “Manually Deploying a Site, Object, or Network”.
 - Step 5** After deployment, rediscover the device as described in “Rediscovering a Device After a Problem” below.
-

Rediscovering a Device After a Problem

Follow these steps to rediscover a device after correcting a problem that interfered with discovery.

-
- Step 1** In the Map Viewer, select the object and right-click.
 - Step 2** Choose States. You see the States dialog box.
 - Step 3** On the States tab, click Rediscover. You are asked if you want to rediscover the device.
 - Step 4** Click Yes. CMNM rediscovers the device. During discovery, Current State is discovering. When the discovery is complete, Current State changes to active.

Step 5 Close the dialog box.



A

- access **4-3**
- access control **5-1**
- access specifications **5-3**
 - creating new **5-11**
 - modifying **5-18**
- accounts
 - setting up **5-4**
 - user **5-4**
 - viewing **9-1**
 - viewing BAMS **9-25**
 - viewing Cisco MGC host **9-2**
 - viewing Cisco SLT **9-11**
 - viewing LAN switch **9-18**
- adjacent point code **1-13, 1-14**
- administrative password **5-21**
- Alarm&Meas Viewer **8-39, 8-40**
- alarms
 - application-related for the MGC host and BAMS **8-13**
 - BAMS and Cisco MGC **A-1**
 - Cisco MGX 8260 **8-14**
 - Cisco SLT **8-10**
 - CMNM internal **A-3**
 - LAN switch **8-11**
- alarms, setting how long they are stored **8-49**
- APC **1-13, 1-14**
- attributes, seed file **6-2**
- authenticationFailure **8-11**
- average summary rule **7-25**

B

- BAF **1-1**
- BAMS **1-1**
 - deploying **6-11**
 - viewing accounts **9-25**
 - viewing properties **9-27**
- BAMS alarms, troubleshooting **A-1**
- BAMS messages **A-2**
- Bellcore Automatic Message Accounting Format (BAF) **1-1**
- Billing and Measurements Server **1-1**
 - deploying **6-11**

C

- C7 IP link **1-13**
- c7iplnk **1-13**
- Catalyst 2900 **1-1**
- Catalyst 2900 traps **8-12**
- Catalyst 2900XL traps **8-12**
- Catalyst 5000 **1-1**
- Catalyst 5500 **1-1**
- CDR Viewer **8-39, 8-42**
- CEMF, performance enhancements **2-7**
- CEMF client **2-6**
- CEMF concepts
 - CEMF network model **1-5**
 - Element Manager **1-2**
 - events **8-2**
 - event state **8-3**
 - management domain **8-4**
 - object **1-5, 1-6**

- object type **1-6**
 - object types and 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 **4-7**
 - CISCO-CONFIG-MAN-MIB-V1SMI **8-11, 8-14**
 - Cisco Media Gateway Controller (Cisco MGC) **1-1**
 - Cisco MGC alarms, troubleshooting **A-1**
 - Cisco MGC host **1-1**
 - deploying **6-9**
 - traps **8-13, 8-17**
 - viewing accounts **9-2**
 - viewing properties **9-3, 9-8, 9-33**
 - Cisco MGC host messages **A-2**
 - Cisco MGC Manager (CMNM) **1-2, 1-3**
 - Cisco MGC node **1-1**
 - Cisco MGX 8260 **1-3**
 - deploying **6-11**
 - managing faults **8-38**
 - traps **8-13**
 - Cisco SC2200 **1-1**
 - Cisco Signaling Controller **1-1**
 - Cisco Signaling Link Terminal **1-1**
 - Cisco SLT **1-1**
 - deploying **6-10**
 - viewing accounts **9-11**
 - viewing properties **9-13**
 - Cisco SS7 PRI Gateway Solution **1-2, 1-3**
 - CISCO-STACK-MIB **8-13**
 - CISCO-SYSLOG-MIB **8-11**
 - Cisco Tandem Offload Solution **1-2, 1-3**
 - CISCO-TRANSPATH-MIB **8-13**
 - CiscoView **1-2, 2-12, 2-13**
 - Cisco Virtual Switch Controller (Cisco VSC) **1-1**
 - Cisco VSC3000 **1-1**
 - CiscoWorks 2000 **2-12**
 - clearing details
 - clearing method **8-38**
 - clearing time and date **8-38**
 - reason for clearing **8-38**
 - user responsible for clearing **8-38**
 - close window **4-9**
 - CMM **1-2**
 - CMNM
 - how it models the Cisco MGC node **1-12**
 - installing **2-1, 2-10**
 - key features **1-2**
 - overview **1-1**
 - uninstalling **2-14**
 - CMNM internal messages **A-3**
 - CMNM session, quitting **4-4**
 - coldStart **8-10**
 - commAlarm **8-13**
 - configChange **8-11**
 - CONFIG-LIB Viewer **8-39, 8-44**
 - connectivity network
 - containment hierarchy **1-14, 1-15**
 - Cooked partitions **2-2, 2-3, 2-7**
 - create new objects, deployment **6-6**
 - Ctrl + **4-5**
-
- D**
 - data collection **7-3**
 - data summaries **7-2**
 - decommissioning devices **7-20**
 - deploying
 - BAMS **6-11**
 - Billing and Measurements Server **6-11**
 - Cisco MGX 8260 **6-11**
 - Cisco SLT **6-10**
 - LAN switch **6-10**
 - media gateway network **6-8**
 - deploying a network, using a seed file **6-1**

deployment **6-1**
 deployment wizard **6-6**
 deployment wizard, open from existing object **6-7**
 destination point code **1-14**
 diagnostic tools **9-48**
 disable toolbar **4-8**
 discovery **4-3**
 DNS requirements **2-9**
 documentation
 BAMS **xv**
 CEMF **xv**
 suite of **xv**
 DPC **1-14**
 DPNSS **1-13**

E

edit alarm state
 acknowledge alarms **8-34**
 acknowledge alarms with comment **8-34**
 clear alarms **8-34**
 unacknowledge alarms **8-34**
 Element Manager **1-2**
 end date data entry box **7-24**
 end time data entry box
 Performance Manager **7-24**
 enetif **1-13**
 environmentError **8-13**
 equipmentError **8-13**
 errored state **8-6**
 Ethernet interface **1-13**
 viewing properties **9-40**
 Event Browser
 drop down menu options **8-22**
 event history **8-35**
 event history enabled **8-36**
 full color coding **8-35**
 full event description **8-36**
 full event description screen **8-37**
 launch **8-21**
 manage an event from the menu bar **8-34**
 manage an event from the window **8-33**
 managing events **8-33**
 manual update **8-34**
 no color-coding **8-35**
 open the query editor **8-23**
 partial color-coding **8-35**
 print **8-23**
 refresh **8-36**
 screen information **8-23**
 select type of color coding **8-35**
 set color coding **8-35**
 view the event history **8-35**
 Event Browser screen **8-21**
 events **4-3**
 history **8-35**
 how CEMF models **8-2**
 managing **8-33**
 modifying filtering criteria **8-31**
 setting how they are color coded **8-35**
 sorting **8-32**
 states **8-3**
 viewing event history **8-35**
 external node **1-13**
 extnode **1-13**

F

FAS path **1-13**
 faspath **1-13**
 fault management, introduction **8-1**
 faults
 how CMNM manages **8-5**
 managing Cisco MGX 8260 **8-38**
 feature lists **5-1, 5-3**
 file menu **4-8, 4-9**
 File Options **8-39, 8-48**
 forwarding traps **8-19**

full event description, Event Browser **8-36**
 full event description screen
 acknowledge details **8-38**
 clearing details **8-38**
 Event Browser **8-37**
 event description **8-37**
 event state **8-37**
 management domain **8-37**
 object name **8-37**
 severity **8-37**
 time and date **8-37**

G

graphs and charts **7-26**
 groups **4-3**

H

hard drive partitioning **2-3**
 hardware requirements **2-1**
 help **4-9**
 history storage criteria **7-3**

I

IF-MIB **8-10**
 installing CMNM **2-1**
 IP FAS path **1-13**
 ipfaspath **1-13**
 IP link **1-13**
 iplnk **1-13**
 ISDN-PRI **1-13**

L

LAN switch **1-3**
 deploying **6-10**

traps **8-11**
 viewing accounts **9-18**
 viewing properties **9-20**
 linkDown **8-10**
 linkset **1-13**
 linkUp **8-10**
 lnkset **1-13**
 logicalOR
 summary rule **7-25**
 login screen **4-2**
 Log Viewer **8-39, 8-45**

M

management domain **8-4**
 managing events in Event Browser **8-33**
 manual deployment **6-6**
 max summary rule **7-25**
 media gateway network
 deploying **6-8**
 MGCP path **1-13**
 mgcppath **1-13**
 MGC Toolbar **8-39**
 min summary rule **7-25**
 missed poll **7-3**
 MML **1-14**
 mms1600_trap **8-15**
 modifying
 access specifications **5-18**
 user groups **5-17**
 users **5-16**
 monitored attributes **7-24**
 mouse **4-4, 4-5**
 multiple disk drives **2-2**
 multiple Event Browser sessions **8-2**

N

NAS path **1-13**
 naspath **1-13**
 navigating through CMNM **4-4**
 navigation **4-5, 4-6**
 network devices, viewing information about **9-1**
 normal state **8-6**
 northbound systems, forwarding traps to **8-19**
 now checkbox
 Performance Manager **7-24**

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 **2-5**
 object types **1-6**
 open the query editor
 Event Browser **8-23**

P

password **4-2**
 changing administrative **5-21**
 password requirements **6-1**
 perfMeasFilters **7-14**
 performance data **7-23, 7-28**
 performance enhancements **2-7**
 Performance Manager
 end time data entry box **7-24**
 graphs and charts **7-3**
 history storage criteria **7-3**
 how data is collected **7-3**
 missed polls **7-3**

now checkbox **7-24**
 opening **7-10**
 points, color coding **7-28**
 refresh button **7-25**
 sample line chart screen **7-26**
 sample table display screen **7-26**
 screen **7-12**
 start date data entry box **7-24**
 start polling events point **7-26**
 start time data entry box **7-24**
 stop polling events point **7-26**
 summary interval **7-24**
 summary rule **7-25**
 viewing a chart **7-27**
 view performance statistics **7-24**
 view points and values on a line chart **7-28**
 view raw data **7-27**
 Performance Manager data **7-2**
 Performance Manager screen **7-12**
 performance monitoring, introduction **7-1**
 performance statistics, printing from Performance Manager **7-30**
 permission level **5-3**
 point code **1-13**
 points color-coding **7-28**
 polling **7-1**
 changing defaults **7-14**
 decommissioning devices **7-20**
 different states of a device **7-13**
 on demand **7-20**
 presence **8-6**
 rediscovering devices **7-20**
 setting frequencies **7-12**
 starting on a device **7-17**
 understanding state symbols **7-13**
 POM DynamicReconfiguration **6-16**
 pop-up menu, deployment **6-7**
 print **4-8**
 printing performance statistics **7-30**

print view displayed in window **4-8**
 processingError **8-13**
 progress bar, Event Browser **8-24**
 propagation, event **8-4**
 properties
 viewing **9-1**
 viewing BAMS **9-27**
 viewing Cisco MGC host **9-3, 9-8, 9-33**
 viewing Cisco SLT **9-13**
 viewing Ethernet interface **9-40**
 viewing LAN switch **9-20**
 viewing serial interface **9-44**
 viewing TDM interface **9-42**
 pcode **1-13**

Q

Q.931 protocol **1-13**
 qualityOfService **8-13**
 Query Editor
 modifying filtering criteria **8-31**
 screen **8-7, 8-20, 8-24**
 set up sort options **8-32**
 sort options
 object name **8-32**
 severity **8-32**
 time **8-32**
 quitting a CMNM session **4-4**

R

raw data
 Performance Manager **7-2**
 Raw partitions **2-3, 2-4, 2-8**
 rediscovering devices **7-21**
 Reflection, configuring **2-15**
 refresh button **7-25**

S

security **5-1**
 seed file **6-1, 6-2**
 selecting items **4-6**
 serial interface, viewing properties **9-44**
 Service Switching Points (SSPs) **1-13**
 severity, colors used **8-3**
 sgcpath **1-13**
 SGCP path **1-13**
 shelfAlarmClear **8-14**
 shelfColdStart **8-14**
 shelfMajorAlarm **8-14**
 shelfMinorAlarm **8-14**
 shelfSecurityAlert **8-14**
 shortcut keys **4-5**
 show toolbar **4-8**
 Signaling Transfer Point (STP) **1-13**
 SNMP **7-25, 8-4**
 SNMPv2-MIB **8-10**
 software requirements **2-6**
 sorting events **8-32**
 sort options **8-32**
 source domain **8-4**
 SS7 network **1-13**
 SS7 path **1-13**
 ss7path **1-13**
 SS7 route **1-13**
 ss7route **1-13**
 ss7subsys **1-13**
 SS7 subsystem **1-13**
 Start Date data entry box, Performance Manager **7-24**
 starting a CMNM session **4-1**
 start time data entry box, Performance Manager **7-24**
 Status Dialog screen **4-7**
 status information, viewing **4-7**
 STP **1-14**
 summarized data **7-2**
 summary interval **7-24**

summary rule **7-25**
 switchModuleDown **8-13**
 switchModuleUp **8-13**
 syslogAlarm **8-11**

T

TCAP IP path **1-13**
 tcapipath **1-13**
 tdmif **1-13**
 TDM interface **1-13**
 viewing properties **9-42**
 TDM link **1-13**
 toolbar **4-7, 4-8**
 total
 summary rule **7-25**
 Trace Viewer **8-39, 8-46**
 Translation Verification **8-39, 8-47**
 traps
 BAMS **8-10**
 Cisco MGC host **8-17, 8-18, 8-19**
 Cisco SLT **8-10**
 forwarding to other systems **8-17**
 LAN switch **8-11**
 receipt not guaranteed **8-17**
 troubleshooting alarms **A-1**

U

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

viewer **4-3**
 viewing a chart **7-27**
 view points and values on a line chart **7-28**
 view raw data **7-27**
 view the event history **8-35**
 view up-to-date Performance Manager information **7-3**
 Voice Services Provisioning Tool **1-2, 1-3**
 VSC **1-1**
 VSPT **1-2**

W

warmStart **8-10**
 Web Viewer **1-2, 1-4**
 window refresh, Event Browser **8-36**

X

XDMCP connection **2-15**

