Cisco Media Gateway Controller Node Manager User Guide

Release 2.8(1)
December 15, 2009

Americas 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: 408 527-0883

Customer Order Number:
Text Part Number: OL-18339-03

CONTENTS

I N D E X

Preface

Revised: December 15, 2009, OL-18339-03

Document Objectives

This user guide provides information for installing, configuring, and using the Cisco Media Gateway Controller (MGC) Node Manager (MNM). It also contains reference information for administrators, service technicians, and users.

Note
- From Cisco MNM Release 2.7(3) onward, Cisco VSPT is packaged with Cisco MNM and is no longer available as a free customer download.
- Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, Cisco ITP-L will replace Cisco SLT in publications and the product.

Audience

The audience for this document is network operators and administrators. This audience is assumed to have experience in telecommunications networks, protocols, and equipment, and a familiarity with data communications networks, protocols, and equipment.

Related Documentation

This document contains information that is related to Cisco Media Gateway Controller Node Manager software. For additional information on those subjects, see the documents at this URL:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/tsd_products_support_series_home.html

The user guide for Cisco MNM on Cisco.com is available from the Cisco MNM Launch Pad. To open the user guide for Cisco MNM on Cisco.com, click the **Manual** button on the Cisco MNM Launch Pad.

This document contains information that is related to Cisco PGW 2200 Softswitch software installation and configuration. For additional information on those subjects, see the documents at this URL:

http://www.cisco.com/en/US/products/hw/vcallcon/ps2027/tsd_products_support_series_home.html

Cisco Voice Services Provisioning Tool Documentation

The Cisco VSPT provides an integrated provisioning graphical user interface for the Cisco PGW 2200 Softswitch and the Cisco Billing and Measurements Server (BAMS).

You can find the Cisco VSPT documentation at this URL:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps2272/tsd_products_support_series_home.html

Cisco Element Management Framework Documentation

For more information on Cisco EMF 3.2, see documents at this URL:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps829/tsd_products_support_eol_series_home.html

Cisco Billing and Measurements Server Documentation

For more information on the Cisco BAMS, see documents at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps522/tsd_products_support_series_home.html

Cisco H.323 Signaling Interface Server Documentation

For more information on the Cisco H.323 Signaling Interface (HSI) Server, see documents at this URL:

- *Cisco H.323 Signaling Interface User Guide,* at

  http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/hsi/4.3/guide/43ug.html

- *Release Notes for Cisco H.323 Signaling Interface, Cisco HSI Release 4.3 and Related Patches* at

  http://www.cisco.com/en/US/products/hw/vcallcon/ps2027/prod_release_notes_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Document Change History

Release Number	Document Number	Change Date	Change Summary
2.8(1) Patch 1	OL-18339-03	December 2009	Removed information related to TALI interface.
2.8(1) Patch 1	OL-18339-02	February 2009	Updated to document new features in Cisco MNM Release 2.8(1) Patch 1.
2.8(1)	OL-18339-01	December 2008	Initial release

C H A P T E R 1

Overview of Cisco Media Gateway Controller Node Manager

Revised: December 15, 2009, OL-18339-03

This chapter includes the following sections:

- An introduction to Cisco Media Gateway Controller (MGC) Node Manager (MNM), including terms and architecture of the Cisco PGW 2200 Softswitch.

- Key feature descriptions of Cisco MNM.

- An overview of Cisco Element Manager Framework (Cisco EMF), the framework for Cisco MNM.

- An explanation of how Cisco MNM models the network, which describes the various ways you can view and manage your network using Cisco MNM.

Introduction

Cisco Media Gateway Controller Node Manager provides fault, configuration, provisioning, and performance management for two kinds of Cisco PGW 2200 Softswitch-based networks:

- A Cisco PGW 2200 Softswitch node (shown in Figure 1-1), which consists of these components:

  - A Cisco PGW 2200 Softswitch host,

  - One or more Cisco IP Transfer Point LinkExtenders (Cisco ITP-Ls) integrated in the AS5350 or AS5400 access servers. The Cisco ITP-L serves as the signaling gateway to the SS7 network.

  - A Cisco 2811 ITP-L service router. The Cisco 2811 ITP-L service router functions as the signaling gateway to the SS7 network.

  - The Cisco Catalyst 5500, Catalyst 6509, or Catalyst 2900 XL LAN switch, which provides IP connectivity for all node elements.

  - Optionally, the node may include a Cisco Billing and Measurements Server (BAMS) and a Cisco H.323 Signaling Interface (HSI) server associated with the Cisco PGW 2200 Softswitch (see Figure 1-1).

- A Cisco PGW 2200 Softswitch farm, a cluster of Cisco PGW 2200 Softswitch nodes operating in concert with a cluster of two or more Internet Transfer Points (ITPs). In this configuration, one or more ITPs, rather than an ITP-L, serve as the signaling gateway to the SS7 network. The farm of Cisco PGW 2200 Softswitch hosts appears as a single point code to the public switched telephone network (PSTN).

See the Cisco MNM release notes for the software releases supported on these components:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/prod_release_notes_list.html

Note Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, Cisco ITP-L will replace Cisco SLT in publications and the product.

Figure 1-1   Cisco MNM with Cisco PGW 2200 Softswitch Node
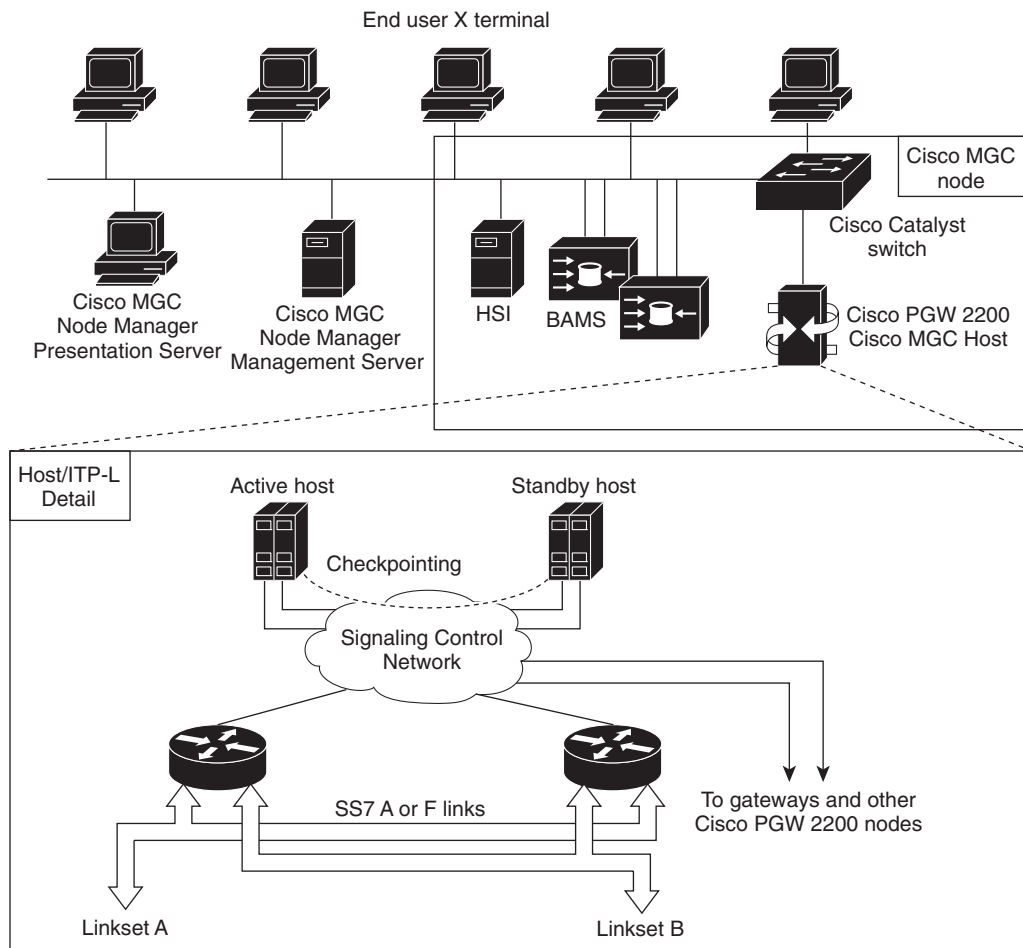
Terms Used in This Document

The following terms are used in this document:

- Cisco BAMS—A UNIX-based software application that accepts individual call detail blocks generated by Cisco PGW 2200 Softswitches, which 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 EMF—The element management framework upon which Cisco MNM is built.

- Cisco PGW 2200 Softswitch—The key to Cisco's voice domain solutions. The Cisco PGW 2200 Softswitch node comprises a number of different components, including the Cisco PGW 2200 Softswitch host and a Cisco ITP-L or an integrated ITP-L.

- Cisco PGW 2200 Softswitch host—A Sun host server running Cisco PGW 2200 Softswitch software.

- Cisco PGW 2200 Softswitch node—The logical grouping of the active and standby Cisco PGW 2200 Softswitch hosts, control signaling network, Cisco ITP-Ls, LAN switches, HSI servers, and the BAMS.

- Cisco PGW 2200 Softswitch farm—A cluster of Cisco PGW 2200 Softswitch nodes, each containing one or a failover pair of Cisco PGW 2200 Softswitch hosts, using two or more Cisco ITPs as the signaling gateway to the SS7 network.

- CiscoView—A graphical device management tool for chassis views and a diagnostic tool for non-Sun components. CiscoView ships as part of the LAN Management Solution (LMS) package that comes with Cisco MNM. Only the CiscoView part of LMS is provided.

- Cisco Voice Services Provisioning Tool (Cisco VSPT)—Graphical user interface for provisioning most Cisco PGW 2200 Softswitch MML parameters. Some parameters are not configurable in Cisco VSPT/MML because they only need to be set once during installation by editing the file, XECfgParm.dat.

> **Note**   For more information on XECfgParm.dat, see the section, "Configuring the Execution Environment", of the *Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide* at the following link
>
> http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9.8/Installation/Guide/Install98.html

- Cisco HSI—An optional server that enables the Cisco PGW 2200 Softswitch to interoperate with an H.323 network.

Overview of the Cisco PGW 2200 Softswitch Node Architecture

The Cisco PGW 2200 Softswitch node comprises a combination of the following components:

- Cisco PGW 2200 Softswitch host—A Sun server running the Cisco PGW 2200 Softswitch software, which is responsible for most of the Cisco PGW 2200 Softswitch functionality, including (depending on the configuration) number analysis, routing, and switching.

- Cisco ITP-L—A Cisco router that terminates Signaling System 7 (SS7) signaling lines from the PSTN and provides an interface to the Cisco PGW 2200 Softswitch host.

  The Cisco 2811 ITP-L consists of a customized Cisco IOS Release 12.4(11)SW2 software image running on a Cisco 2811 router.

  The integrated Cisco ITP-L runs on a Cisco AS5350 or AS5400 access server.

- Cisco LAN switch—An Ethernet switch connecting the Cisco ITP-L to the Cisco PGW 2200 Softswitch host, Cisco BAMS, Cisco HSI server, Cisco MNM, and the Cisco Voice Services Provisioning Tool.

  A Cisco Catalyst 2900XL, 5500, or 6509 can be managed by Cisco MNM.

- Cisco BAMS - Provides measurement and billing mediation from Cisco PGW 2200 Softswitch Call Detail Records (CDRs).

- Cisco HSI Server—A Cisco HSI system that adds an H.323 interface to the
  Cisco PGW 2200 Softswitch. This interface allows calls to be established between the PSTN and an
  H.323 network.

A Cisco PGW 2200 Softswitch node is (optionally) fully redundant. This means that each
Cisco PGW 2200 Softswitch might have multiples of each type of subcomponent. At any given time, one
Cisco PGW 2200 Softswitch host is considered active and the other standby. If the active
Cisco PGW 2200 Softswitch host fails, the standby host becomes active. There is no concept of active
or standby with LAN switches, Cisco ITPs, Cisco ITP-Ls, or the Cisco BAMSs. If two are present, both
are active at all times providing redundancy.

> **Note** The version of Cisco MNM you use depends on your Cisco PGW 2200 Softswitch version. Cisco MNM
> Release 2.8(1) supports Cisco PGW 2200 Softswitch Releases 9.5(2) through 9.8(1). However,
> Cisco VSPT is version specific.

Key Features of Cisco MNM

The most common Cisco EMF installation includes plug-in modules referred to as element managers or
Element Management Systems (EMS). In the Cisco PGW 2200 Softswitch node architecture, Cisco
MNM is a Cisco EMF-based EMS responsible for managing the Cisco PGW 2200 Softswitch node.
Cisco MNM adds specific graphical user interface (GUI) windows and modeling behavior to the
standard Cisco EMF system to allow the management of network elements.

Cisco MNM uses Cisco EMF to manage the following components:

- Cisco PGW 2200 Softswitch
- Cisco ITP-L
- Cisco LAN Switch (Cisco Catalyst 2900, 5500, and 6509 only)
- Cisco BAMS
- Cisco HSI

The key features of Cisco MNM are

- Fault management—Cisco MNM provides fault management of the Cisco PGW 2200 Softswitch
  node (the Cisco PGW 2200 Softswitch host, the Cisco ITP-L, the Cisco LAN switch, the Cisco HSI
  server, and the Cisco BAMS). You can see the alarms generated by these elements in the Cisco MNM
  system.

  When the Cisco PGW 2200 Softswitch host detects a problem with one of its connections, it
  generates a trap. Cisco MNM receives these traps and delegates them to the graphical object that
  represents that connection. For example, if Cisco MNM receives a trap that the link to a media
  gateway is down, Cisco MNM delegates that trap to the object that represents the media gateway
  link. You can then acknowledge and clear the alarms and forward traps.

  In order to make the identification of potential problems easy, Cisco EMF propagates the alarm state
  of network elements upwards through the node and physical views. If an object receives an alarm,
  it changes color to reflect its new state, and all parent objects also change color to reflect the most
  severe alarm on any of the children.

  Cisco MNM periodically polls each managed object to ensure that the device is still reachable
  through SNMP. If the device is not reachable, an annotation appears on the display in the Map
  Viewer, an alarm is generated, and the object is placed in an error state. After the object loses

connectivity, Cisco MNM continues to poll the object until it can be reached. Once connectivity is re-established, 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 6, "Managing Faults with Cisco MNM."

- Performance monitoring—Cisco MNM collects and displays performance information from the Cisco PGW 2200 Softswitch node, helping you to monitor the health and performance of the network. Cisco MNM collects performance information from all the components of the Cisco PGW 2200 Softswitch node.

    You can:

    - Graph and display the performance information
    - View performance data associated with an object and graph that data over time
    - Configure the objects to poll and the frequency of the polling
    - Export the performance data in .csv, tab, and comma-delimited formats for use by other applications

    For more information on performance monitoring, see Chapter 7, "Managing the Performance of Cisco MNM Devices."

- User Administration—Cisco MNM supports role-based access to its management functions. The administrator defines user groups and assigns users to these groups. Cisco MNM supports control of administrative state variables for Cisco PGW 2200 Softswitch node resources. For more information on access control, see Chapter 4, "Setting Up Cisco MNM Security."

- Billing and Measurements

    - Cisco MNM collects trunk group and bearer channel measurements from the Cisco BAMS, and the Cisco BAMS creates measurement files from the CDRs on the Cisco PGW 2200 Softswitch Host.
    - Third-party billing packages are supported directly by the Cisco BAMS.

- Configuration

    - Cisco Voice Services Provisioning Tool—A Cisco PGW 2200 Softswitch and Cisco BAMS configuration GUI tool included with Cisco MNM 2.8(1). Also provides tools for PGW backup, restore, and configuration checking.
    - CiscoView—Used to configure and monitor the Cisco ITP-L and LAN switches. CiscoView is delivered on an LMS CD in the Cisco MNM media kit. Only the CiscoView part of LMS is provided.

- Troubleshooting—Cisco MNM provides a full range of diagnostic and troubleshooting tools, such as IP and SNMP Ping, Alarm and System Log, Host Status Check, Cross-Device Audit, and the MGC toolbar that includes CDR Viewer, Log Viewer, Trace Viewer, and Translation Verification Viewer.

- Secure communications—If you install the Cisco EMF SSH add-on, you can use SSH-based secure communications with SSH-enabled components:

    - Cisco PGW 2200 Softswitch
    - Cisco BAMS
    - Cisco HSI server
    - Cisco ITP-L
    - Cisco Integrated ITP-L

- Cisco Catalyst switches (2900XL, 5500 and 6509)

The components must have SSH installed, and you must define their security policy (at deployment or in the Accounts dialog box) as "ssh." With SSH support installed, all operations that previously used Telnet or File Transfer Protocol (FTP) instead use ssh (the secure shell counterpart of Telnet) or sftp (the secure shell counterpart of FTP) when communicating with SSH-enabled components.

Overview of Cisco EMF

Cisco MNM is based on Cisco EMF, 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.

Cisco EMF 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.

Cisco EMF Components

Cisco EMF consists of

- A series of applications that form a front-end GUI to process input (the Cisco EMF Client software)
- A series of back-end server processes that maintain a model of the network and carry out the actual interfacing to the network elements (the Cisco EMF Server software) (see Figure 1-2)

Network Operations Center (NOC) users typically interact with the Cisco EMF Client software by connecting from an X terminal workstation. Cisco MNM supports up to 10 active, concurrent sessions.

Figure 1-2   Cisco EMF Processes
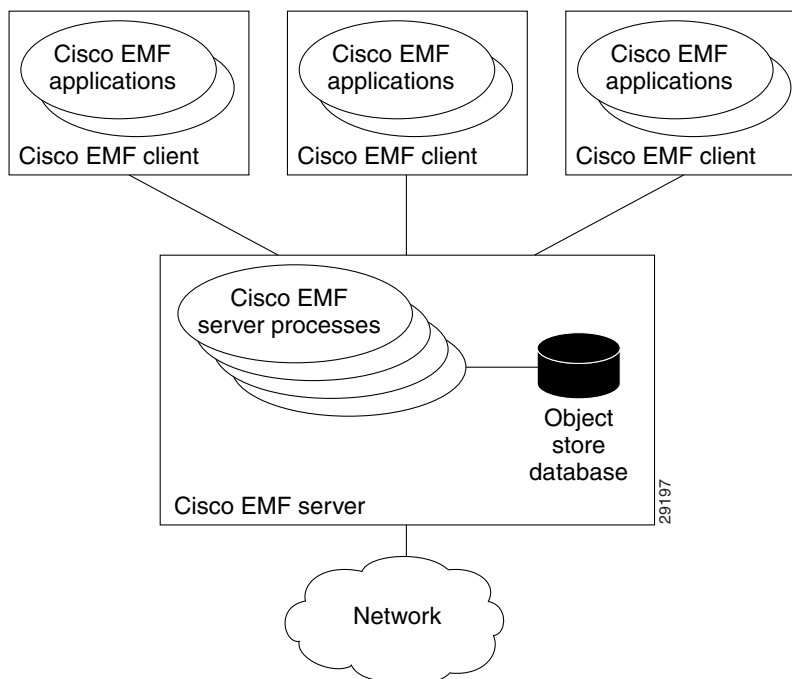
Cisco EMF comes with the following set of applications accessed from the launchpad (see Figure 1-3) each of which opens when you start a Cisco MNM session:

- Map Viewer—View, build, and monitor a network with the Map Viewer. You can monitor the network using network and network object connections.

- Object Group Manager—Organize network elements into object groups. You can create, delete, and modify object groups.

- Access Manager—Set up users and user groups, assign passwords, and define access parameters.

- Event Browser—Displays the Event Browser and Query Editor. You can create object groups or browse events from these screens.

- Discovery—Because Cisco MNM requires a login and password in order to fully discover and deploy a device, the Cisco EMF Automatic Discovery feature is not used by Cisco MNM. Cisco MNM performs discovery of device components and configurations once the device has been identified (IP address, host name, and login information entered into Cisco MNM), as described in Chapter 5, "Deploying Your Network in Cisco MNM."

- Cisco MNM Manuals—Opens a browser window and displays links to the following documents:
  - Cisco Media Gateway Control Node Manager End-User Guides
    You can also see these documents at
    http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/products_user_guide_list.html.

- Event Manager
  - Notify—Create notification profiles that consist of a series of notifications to be carried out as a result of the profile being triggered.
  - Thresholds—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 Groups—Filter and organize events based on specified criteria, such as severity, state, or type of network element, and then create a scoreboard to show the state of the group at a glance.
  - PreFilter—Pre-filter some messages collected in Cisco MNM according to the defined rules.
  - Version—Display the version and patch information for Cisco MNM and Cisco VSPT (if installed together with Cisco MNM).

Figure 1-3   Cisco EMF Launchpad
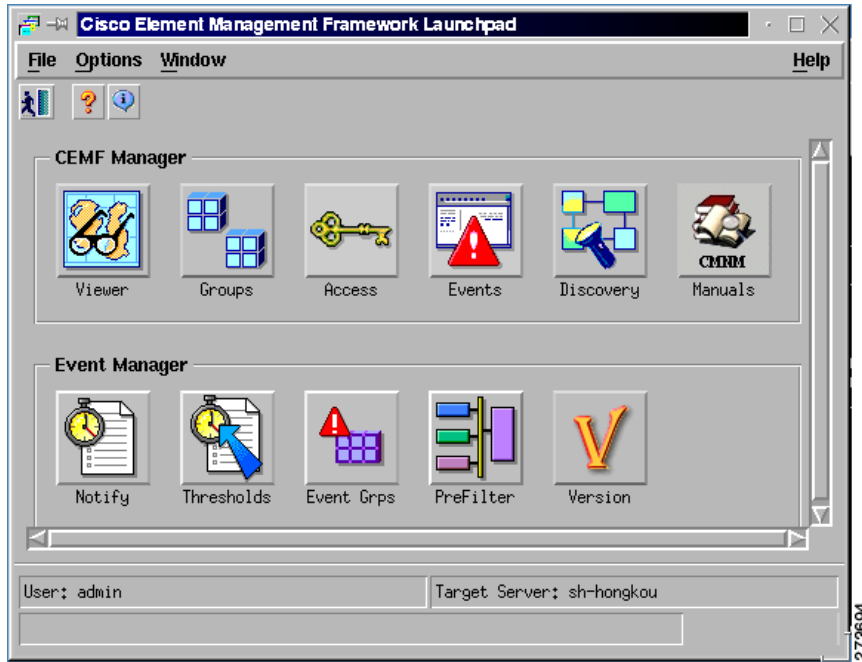
How Cisco EMF Models the Network

Cisco EMF keeps a model of the managed network in its database and uses the model to keep track of the current state of the network.

The Cisco EMF model of the network uses the following components:

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

    An object can represent:

    - A router or a switch

    - A site, region, or node

    - Services provided by the network, for example, a permanent virtual connection (PVC)

    - A subscriber or a customer

- Object classes—Each object within Cisco EMF has an associated object class. Each class of object indicates a different kind of element. Examples of classes are routers, line cards, or sites. 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 an icon used within the Map Viewer browser.

    You can perform powerful queries on different classes of objects. For example, you can show all events in the system from Cisco ITP-Ls or create a group of Cisco LAN Switch objects.

- Object 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 number, and upstream power.

These attributes are associated with the object according to the granularity of object types. A type is 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 1-4.

Figure 1-4   Example of Object Types and Attributes
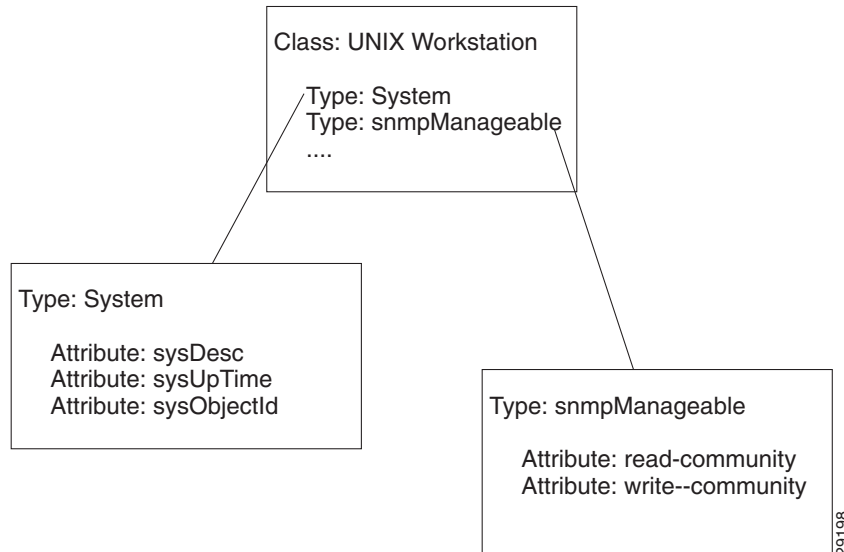
In Figure 1-4, a UNIX Workstation class is specified. This class of object includes two types: System and snmpManageable. The System type includes the sysDesc, sysUpTime, and sysObjectId attributes. The snmpManageable type includes the read-community and write-community attributes.

- Views—A view is a collection of objects in a hierarchical relationship. Each object can have a number of parents and children. See "How Cisco MNM Models the Network" for more information on Cisco MNM views.

- Object groups—An object group is 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 manually or by building a query and are accessible through the Object Group Manager application.

How Cisco MNM Models the Network

Cisco MNM applies the Cisco EMF network object model to the Cisco PGW 2200 Softswitch node. The hub of Cisco MNM network management is the Map Viewer. From the Map Viewer you can access network objects by navigating through one of the views to find the object. Each view represents a different way of containing and grouping the objects, such as by device type, by Cisco PGW 2200 Softswitch node, and by physical or network view. Cisco MNM views are summarized in Table 1-1 and described in detail on the following pages.

Note This section provides conceptual information about the network model that is displayed in the Map Viewer. For information on using the Map Viewer, see Chapter 3, "Getting Started with Cisco MNM," "Using the Map Viewer" section on page 3-10.

Table 1-1   Cisco MNM Views in the Map Viewer

View	Description
MGC-Node-View	Displays all of the Cisco PGW 2200 Softswitch nodes in the network along with their logical children (Cisco ITP-Ls and Cisco PGW 2200 Softswitch hosts), and all the Cisco PGW 2200 Softswitch farms along with their logical children (Cisco PGW 2200 Softswitch nodes containing hosts only) and propagates child alarms to the parents. This view also includes all of the signaling, dial plan, and trunking components of the Cisco PGW 2200 Softswitch node. For more information, see the "MGC Node View" section on page 1-10. If you are using BAMS Phase 3, this view displays each BAMS node associated with the Cisco PGW 2200 Softswitch.
Host-View	Presents all of the Cisco PGW 2200 Softswitch host devices in the network. For more information, see the "Host View" section on page 1-19.
ITP-L-View	Presents all of the Cisco ITP-L devices in the network, including integrated ITP-Ls and integrated ITP-L coresident EMs. This view also contains all of the interfaces on each Cisco ITP-L. For more information, see the "ITP-L View" section on page 1-19.
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 1-20.
BAMS-View	Presents all of the Cisco BAMS in the network. For more information, see the "BAMS View" section on page 1-21.
HSI-View	Presents all Cisco HSI devices in the network. See the "HSI View" section on page 1-21.
Physical	Displays all of the Cisco PGW 2200 Softswitch network devices grouped by physical location (buildings, sites, or regions), and propagates child alarms to the parents. For more information, see the "Physical View" section on page 1-22.
Network	Displays all IP devices within their relative networks and subnets. This is a standard Cisco EMF view. For more information, see the "Network View" section on page 1-22.

MGC Node View

The MGC node view displays all of the Cisco PGW 2200 Softswitch node elements in the network. For each Cisco PGW 2200 Softswitch node, all of the logical components of the node are displayed, as illustrated in Figure 1-5.

Figure 1-5   MGC Node View
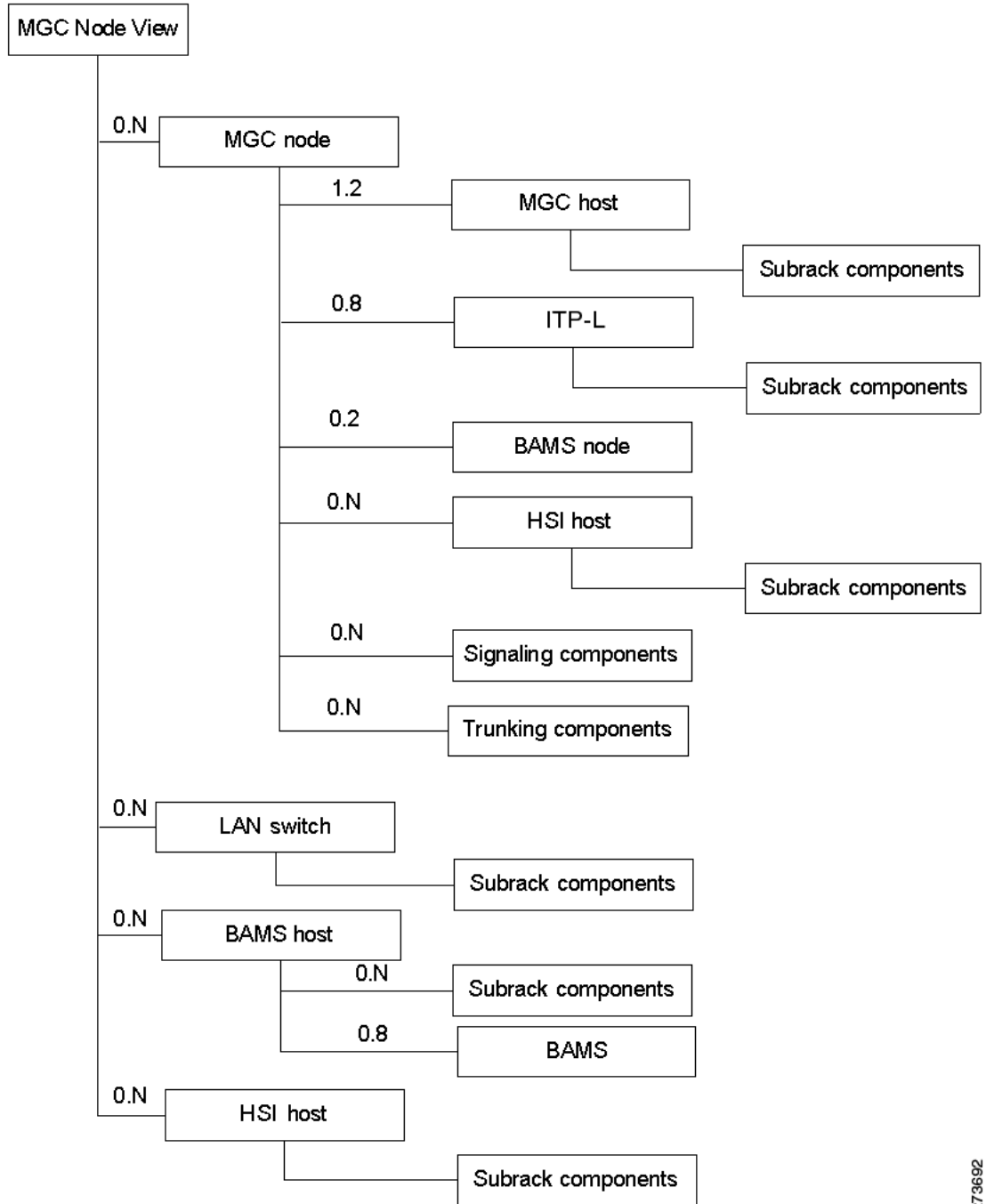
The MGC node view also displays all of the Cisco PGW 2200 Softswitch farms in the network. For each Cisco PGW 2200 Softswitch farm, all of the logical components of the farm are displayed, as illustrated in Figure 1-6.

Figure 1-6   *MGC Farm View*
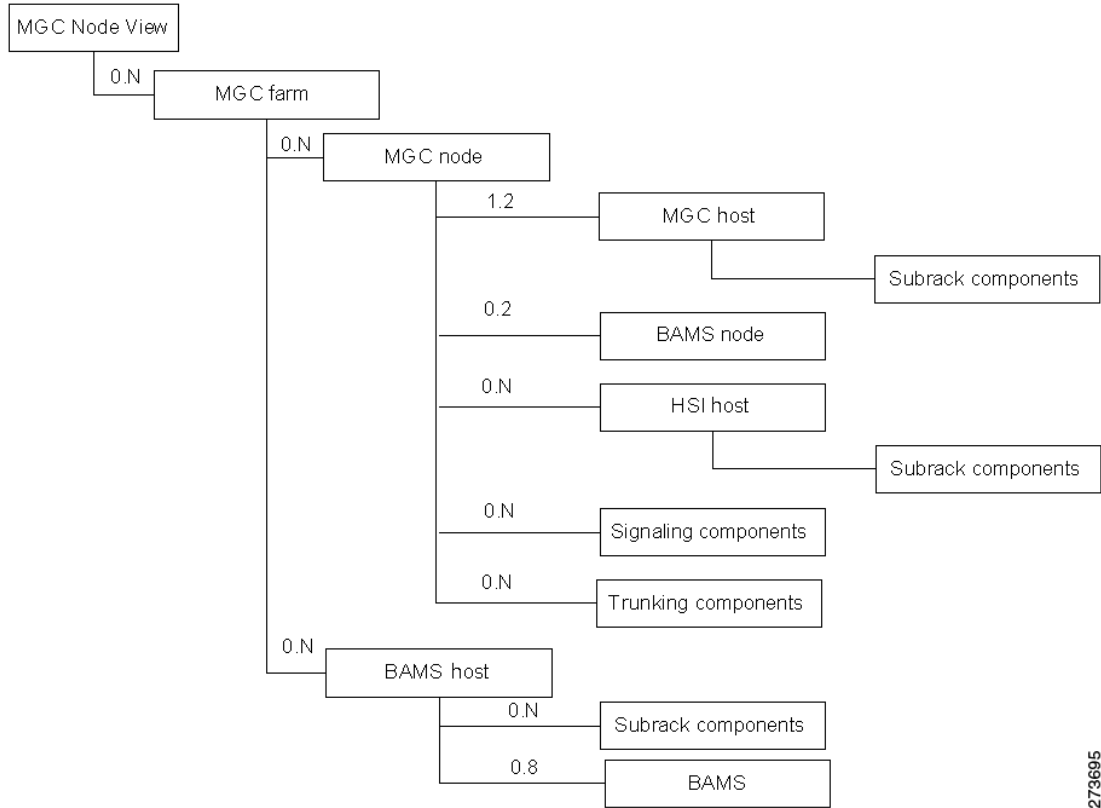
Each Cisco PGW 2200 Softswitch node is represented with its child elements.

- In the case of a *nonfarm node*, these child elements include the Cisco PGW 2200 Softswitch hosts, Cisco BAMS, Cisco HSI server, Cisco ITP-Ls (including integrated ITP-Ls and integrated ITP-L coresident EMs), and each device's network interfaces. Depending on the configuration, there can be a maximum of two Cisco PGW 2200 Softswitch host devices (active/standby pair), two Cisco BAMS (active/standby pair), two or more Cisco HSI servers, eight Cisco ITP-Ls, and two LAN switches. These configurations are shown in Figure 1-5.

- In the case of a node in a farm, the child elements include the Cisco PGW 2200 Softswitch hosts, Cisco BAMS, and Cisco HSI server. Depending on the configuration, there can be a maximum of two Cisco PGW 2200 Softswitch host devices (active/standby pair), two Cisco BAMS (active/standby pair), two or more Cisco HSI servers, and one or more ITPs. These configurations are shown in Figure 1-6.

Note   The Cisco BAMS must be configured to collect CDRs for a Cisco PGW 2200 Softswitch host in the same node to actively poll the host.

In addition to the physical devices, the logical configuration of the active Cisco PGW 2200 Softswitch host is also displayed. This logical configuration includes the signaling and trunking information from the active Cisco PGW 2200 Softswitch host.

Cisco PGW 2200 Softswitch Host Signaling and Trunking Components

This section provides information about how Cisco MNM models the following components in the node view:

- Cisco PGW 2200 Softswitch host signaling network
- Cisco PGW 2200 Softswitch host trunking components

Cisco PGW 2200 Softswitch Host Signaling Network

Cisco MNM displays the status of the Cisco PGW 2200 Softswitch host signaling network on the Map Viewer interface. This includes showing the status of the logical connections from the active Cisco PGW 2200 Softswitch host to these elements:

- Interfaces (Ethernet)
- Signal transfer points (STPs)
- Destination point code (SS7 routes)
- Connected Cisco PGW 2200 Softswitches
- TCAP nodes
- Media gateways
- Cisco ITP-L
- LAN switches

When the common Cisco PGW 2200 Softswitch host object is first deployed, the object database is populated with objects that represent the logical connections from the active Cisco PGW 2200 Softswitch host to the external devices. Cisco MNM then monitors the status of these connections and 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 PGW 2200 Softswitch host.

Cisco MNM monitors the status of the signaling network by processing and decoding alarms, known as *traps,* from the active Cisco PGW 2200 Softswitch host. Upon receipt of an appropriate trap, Cisco MNM maps the trap to the node representing the logical connection, and an alarm associated with the node is displayed.

Cisco MNM communicates with the Cisco PGW 2200 Softswitch host using

- SNMP—SNMP is used for receiving real time statistics, partial MIB based discovery, and alarm traps.
- FTP—FTP or SFTP (Secure FTP) is used for bulk transfers of historical performance statistics and uploading MML discovery files.
- Man-Machine Language (MML)—MML is the TL1 based command line interface on the Cisco PGW 2200 Softswitch Host, the Cisco BAMS and the Cisco HSI server. It is used for EMS information, configuration, and control functions when the SNMP MIBS do not cover the needed functionality.

Cisco PGW 2200 Softswitch Host Signaling Objects

The Cisco PGW 2200 Softswitch software defines over 20 different types of network signaling component types. Cisco MNM queries the configuration of the active Cisco PGW 2200 Softswitch host and represents the objects in the display.

The hierarchical structure or relationship of the components is based on the configuration defined by the active Cisco PGW 2200 Softswitch host. This configuration can vary from installation to installation. Cisco MNM, however, is able to handle any type of configuration present on the host.

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

Table 1-2 describes the classes used to represent the signaling network in Cisco MNM.

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 PGW 2200 Softswitch connects to external switches and other Service Switching Points (SSPs).
association	Association	Represents an SCTP association
bripath	Basic Rate Interface signalling services	Basic Rate Interface signaling services.
c7iplnk	C7 IP link	Identifies a link between a Cisco ITP-L IP address and port, and the SS7 network.
dchan	D Channel	D channel backup.
domainprof	Domain	The domain table defines the domain profile that is associated with a given domain name.
dpc	Destination point code	SS7 destination point code.
dpnsspath	DPNSS Path	DPNSS signaling path that is back-hauled over IP to or from a Network Access Server (destination).
eisuppath	EISUP path	Signaling service or signaling path to an externally located Cisco PGW 2200 Softswitch.
extnode	External node	MGW with which the Cisco PGW 2200 Softswitch communicates.
files	Files	Customer-specific flat files that can be used to provision trunks and dial plans.
gwpool	Gateway pool	The Gateway Pool component is used to organize a set of border gateways with the same capabilities on the Cisco PGW 2200 Softswitch.
h248path	H.248 signaling service	Signaling service or signaling path to a trunking gateway.
insipheader	Inbound SIP Header	The Inbound SIP Header component allows you to manage inbound SIP header tables.
ipfaspath	IP FAS path	Transport service or signaling path from a gateway to a Cisco PGW 2200 Softswitch

Table 1-2   Classes Representing Signaling Network (continued)

MML Type	Name	Description
ipgw	IP Gateway	The IP Gateway component allows you to manage the border gateways within a gateway pool.
ipinmapping	IP In Trunk Mapping	IP addresses and ports allowed in incoming messages on the SIP or EISUP incoming trunk
iplnk	IP link	IP connection between a Cisco PGW 2200 Softswitch Ethernet interface and a Cisco MGW.
iproute	IP Route	Static IP route.
lnkset	Linkset	Group of all communication links that connect the Cisco PGW 2200 Softswitch to an adjacent STP.
m3uakey	M3ua Key	M3UA Routing key. The parent of the M3UAKEY is the OPC.
m3uaroute	M3ua Route	M3UA route, used to determine how to get an SS7 message to a particular destination using M3UA. M3UA route is similar to SS7ROUTE.
mgcppath	MGCP path	Signaling service or signaling path to a trunking gateway.
mltipfas	Multiple IPFAS services and IP links	Multiple IPFAS/IPNFAS signaling paths and D channels.
naspath	NAS path	Q.931 protocol path between the Cisco PGW 2200 Softswitch and the Cisco MGW.
opc	Origination point code	Origination (own) point code.
outsipheader	Outbound SIP Header	The Outbound SIP Header component allows you to manage inbound SIP header tables.
profile	Profile	Profile table stores all kinds of service profiles, for example, SIP profiles, EISUP profiles, common profiles, domain profiles, and so on. A profile allows you to define a collection of properties and associate trunk groups, domains, or other components with that profile accordingly.
sessionset	Session set	A pair of backhaul links used to communicate with external nodes that support IPFAS.
sgp	SGP	SS7 Signaling Gateway Process.
sipiversion	SIP-I version	SIP-I version Controls the entries in the sipIVersion.dat file, which controls mapping between SIP-I variants.
siplnk	SIP IP link	A SIP IP link used to communicate with the SIP proxy servers.
sippath	SIP Path	SIP signaling service or signaling path to proxy server.
ss7path	SS7 path	Specifies the protocol variant and the path that the Cisco PGW 2200 Softswitch uses to communicate with a remote switch (SSP) sending bearer traffic to the Cisco MGWs.
ss7route	SS7 route	Path from the Cisco PGW 2200 Softswitch through a linkset to another Cisco PGW 2200 Softswitch.
ss7subsys	SS7 subsystem	Logical entity that mates two Signal Transfer Points (STPs).
suakey	Sua Key	SUA Routing key. The parent of the SUAKEY is the OPC.

Table 1-2   Classes Representing Signaling Network (continued)

MML Type	Name	Description
suaroute	Sua Route	SUA route. It is used to determine how to get an SS7 message to a particular destination using SUA.
tcplink	Backhaul TCP Link	Backhaul TCP Link.

Containment Hierarchy of the Signaling Network

When Cisco MNM retrieves the current configuration from the active Cisco PGW 2200 Softswitch host, it establishes the containment hierarchy of the signaling network. Figure 1-7 shows some of the components in the signaling network.

Figure 1-7   Hierarchical Example of Signaling Components
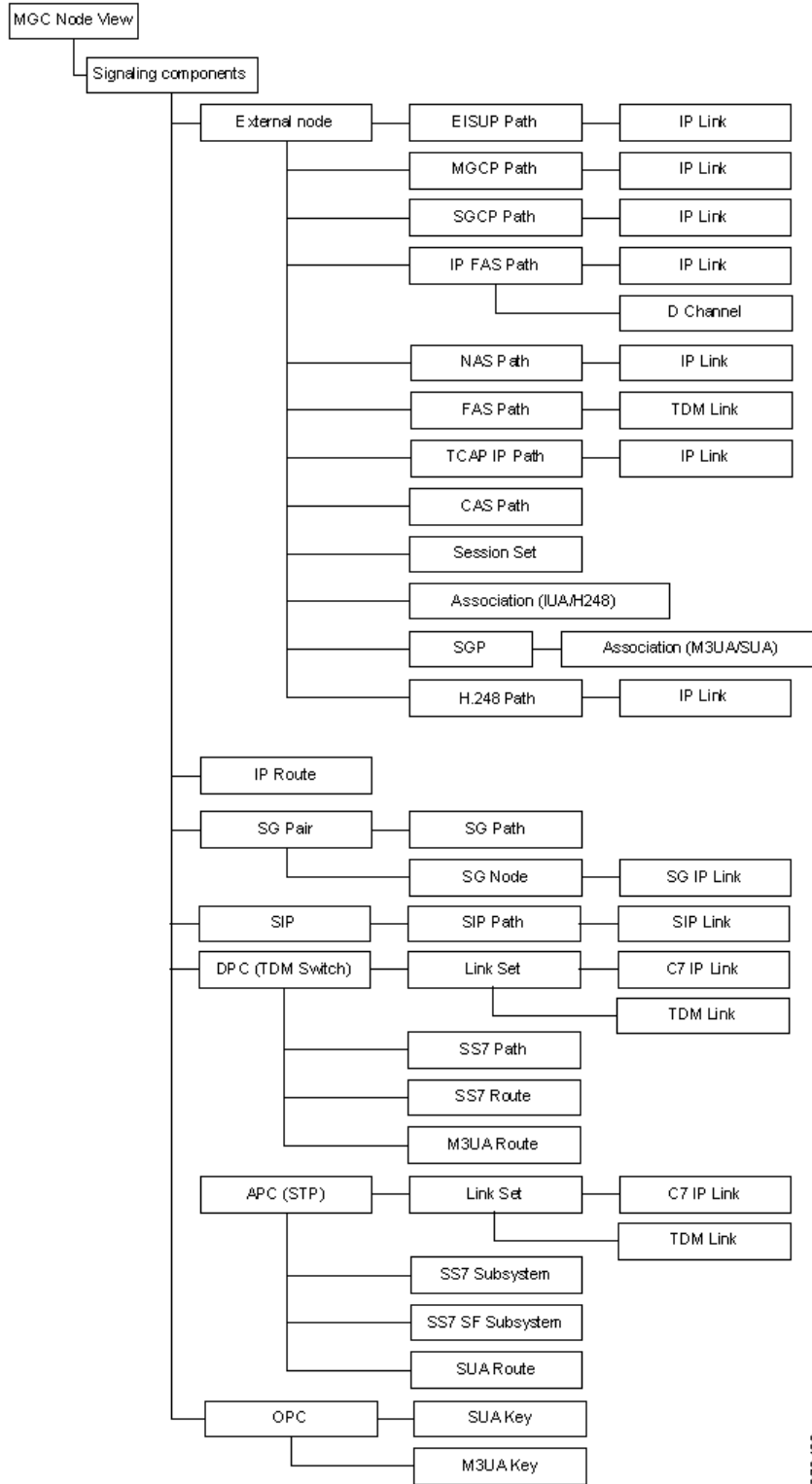
In the MML file, the destination point code (DPC) component represents a switch. The adjacent point code (APC) component represents an STP.

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

- Cisco CallManager
- Connected Cisco PGW 2200 Softswitches
- Interfaces of the Cisco PGW 2200 Softswitch (Cisco HSI)
- Media gateways
- RADIUS servers
- SS7 Service Control Points

Cisco PGW 2200 Softswitch Host Trunking Components

Cisco MNM models all of the trunk groups on the active Cisco PGW 2200 Softswitch host and makes trunk information available to northbound systems. Trunks represent the physical bearer channels, and trunk groups provide a higher-level grouping of trunks.

Trunk group components are stored in a separate logical folder, the Trunking Components folder. When the Cisco PGW 2200 Softswitch host is using switched trunks, each trunk group is shown in the folder. In the case of nailed trunks, the Cisco PGW 2200 Softswitch host does not have any trunk groups, and so no folder is created.

Cisco MNM defines a different class for each type of trunking 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 trunking components in Cisco MNM are described in Table 1-3.

Table 1-3   Classes Representing Trunking Components

MML Type	Description
nailedtrnk	Nailed trunk component (signaling mode)
switchtrnk	Switched trunk component (call control mode)
trnkgrp	Trunk group component

Containment Hierarchy of the Trunking Components

When Cisco MNM retrieves the current configuration from the active Cisco PGW 2200 Softswitch host, it establishes the containment hierarchy of the trunking components. See Figure 1-8.

Figure 1-8   Hierarchical Model Example of Trunking Components
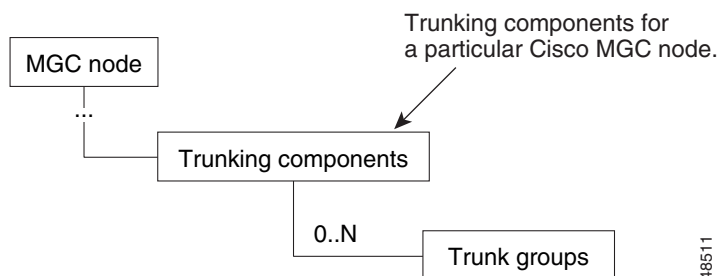
Host View

The Host View displays all of the Cisco PGW 2200 Softswitch host devices along with their associated interfaces and system components, as illustrated in Figure 1-9.

Figure 1-9   Host View
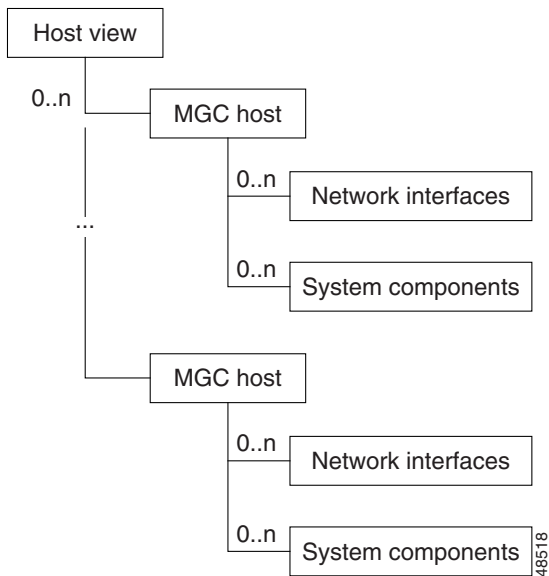
This view collects all Cisco PGW 2200 Softswitch hosts in a single location from which functions can be opened.

ITP-L View

The ITP-L View displays all of the Cisco ITP-L devices in the network along with their associated interfaces, as illustrated in Figure 1-10.

Figure 1-10   ITP-L View
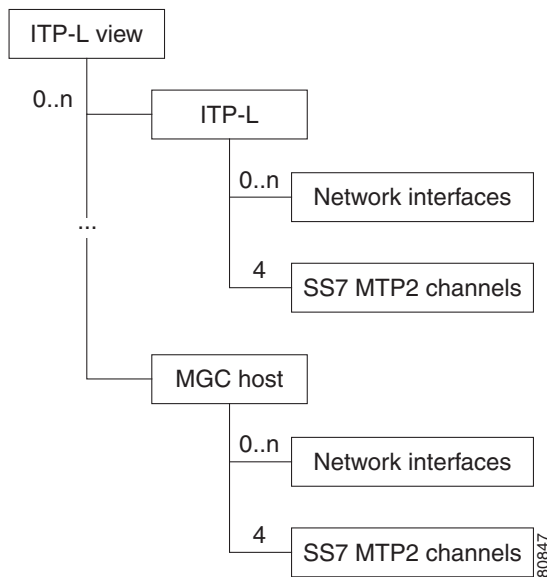
This view is used to collect all Cisco ITP-Ls in a single location.

Note   Cisco MNM 2.3(2) and later releases support ITP-L functions integrated in the Cisco AS5350 and AS5400 access servers. When Cisco MNM is the only element manager managing the server, the functionality is referred to as an integrated ITP-L. In previous releases, the ITP-L functionality was referred to as an integrated ITP-L for coresident EMs, but there are no longer any co-resident EMs for AS5x00. Unless otherwise noted, the term ITP-L describes any of these configurations.

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 1-11.

Figure 1-11   LAN Switch View
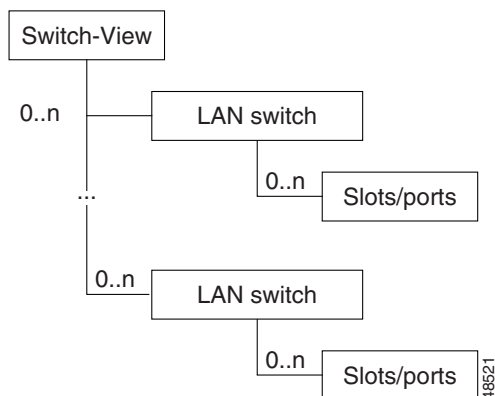
This view is used to collect all LAN switches in a single location for viewing events or starting functions.

BAMS View

The BAMS View displays all of the Cisco BAMS servers in the network. For each Cisco BAMS, the network interfaces of the BAMS are displayed. In addition, each Cisco PGW 2200 Softswitch host that is communicating with the Cisco BAMS is shown, as illustrated in Figure 1-12.

Figure 1-12   BAMS View
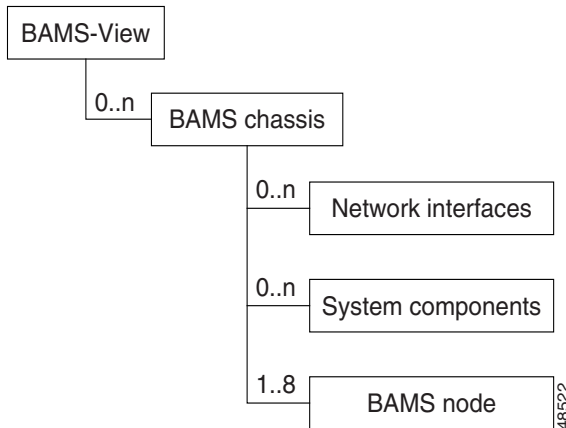
Each Cisco BAMS in the network is displayed, along with its network interfaces and system components. This view is used to collect all Cisco BAMSes in a single location from which functions can be opened.

HSI View

The HSI View displays all Cisco HSIs in the network. For each Cisco HSI, the network interfaces and the associated IP addresses and system components are displayed. This view is used to observe faults and start services.

Figure 1-13   HSI View
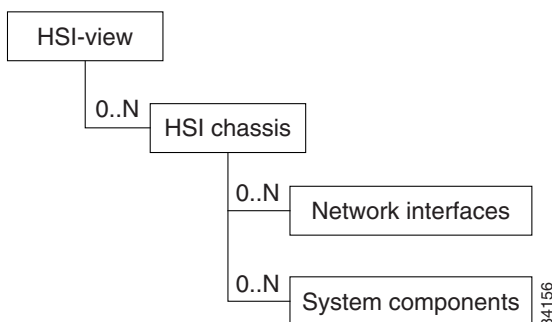
Physical View

Cisco MNM uses the Physical View to represent the physical location of devices. You can set up different types of groupings based on the physical layout of your network.

You can create sites and regions to represent the physical locations of devices in your network. When Cisco PGW 2200 Softswitch node devices are deployed, you can specify the physical location of these devices in one of the predefined regions or sites. The Physical View can be used to quickly see which network elements are at a given location. If a device fails, NOC operators can easily see where personnel should be dispatched.

An example of the Physical View is shown in Figure 1-14.

Figure 1-14   Physical View
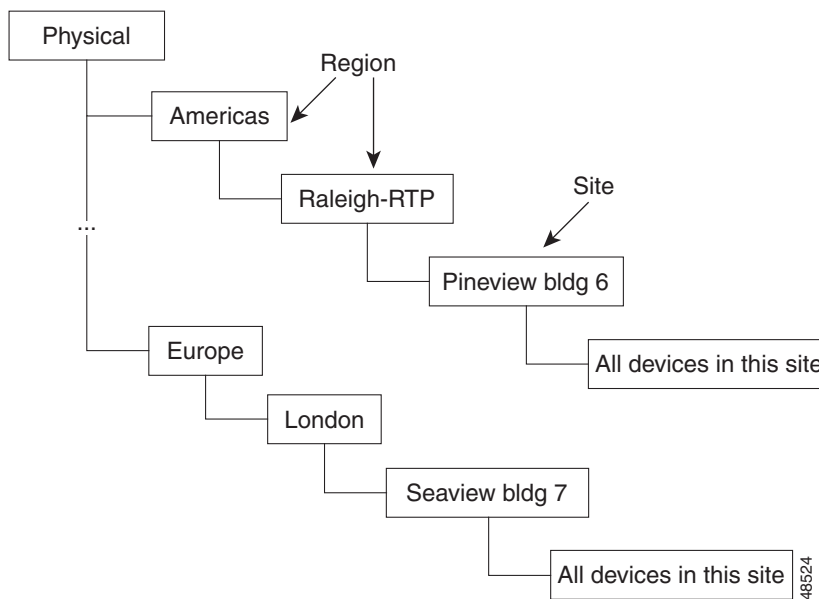
During deployment, devices are placed in each region or site. Relationships between objects at a given site are not shown (these relationships are shown in other views); all devices in a given site are at the same level. Because the Cisco PGW 2200 Softswitch node is not a physical device, it is not represented in this view.

Network View

The Network View groups all IP-enabled devices in containers based on their subnet address, as illustrated in Figure 1-15. This view represents a standard Cisco EMF that is not controlled by Cisco MNM.

Figure 1-15   Network View
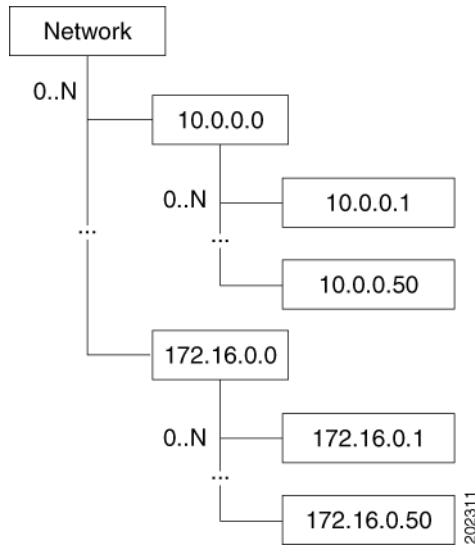
Configuring Network Devices for Management

Revised: December 15, 2009, OL-18339-03

After a short overview, this chapter describes how to configure the various devices in the
Cisco PGW 2200 Softswitch node. This task is typically done by the system administrator.

Note Take precautions to avoid more than one user simultaneously accessing and modifying the same network
device or any of its components. Establish access schedules for all your users.

Overview of Configuration

In Cisco Media Gateway Controller (MGC) Node Manager (MNM), device configuration means setting
up devices that are in the Cisco PGW 2200 Softswitch node to forward alarms (Simple Network
Management Protocol [SNMP traps] from the point of view of the device) to Cisco MNM. For
Cisco MNM to be able to receive and manage alarms, the devices must be configured to send them.
Configuration involves editing the SNMP configuration file on the device to specify the following:

- The Cisco MNM management server's IP address as the SNMP trap destination

- Depending on the device, the severity level of traps to be forwarded, the configuration of SNMP
  community strings, and the SNMP trap source

Note
- The other task in setting up the management of your network is deploying the network devices and
  adding them to the Cisco MNM network model. Deployment tells Cisco MNM how to communicate
  with the managed devices; configuration tells the devices how to communicate with Cisco MNM.
  Deployment is typically performed by users, and the configuration is typically performed by the
  system administrator. See Chapter 5, "Deploying Your Network in Cisco MNM" for details of
  deployment.

- For information on configuring trap forwarding from Cisco MNM to northbound management
  systems, see Chapter 6, "Managing Faults with Cisco MNM," "Forwarding Traps to Other Systems"
  section on page 6-24.

- Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal
  (SLT). Over time, ITP-L will replace SLT in publications and the product.

The Cisco PGW 2200 Softswitch host, Cisco Billing and Measurements Server (BAMS), Cisco ITP-L, Cisco H.323 Signaling Interface (HSI) server, and the Cisco LAN Switch are configured by opening a Telnet session with the device and entering the prescribed SNMP configuration settings. You can initiate the Telnet session at the UNIX command prompt, or, if the device has been deployed in Cisco MNM, you can use Cisco MNM to initiate the Telnet session.

If you deploy firewalls between Cisco MNM and other network elements, configure the firewalls to open the following ports,

- 22 for SSH
- 23 for Telnet
- 161and 162 for SNMP

Information Needed for Configuration

Have the following information available:

- For the Cisco PGW 2200 Softswitch, the Cisco BAMS, and the Cisco HSI server, the superuser password.
- For the Cisco ITP-L and the Cisco LAN switch, the login and enable passwords for the device.
- The IP address of the Cisco MNM server (standalone server or management server in a distributed configuration), to be used as the SNMP trap destination. If multiple IP addresses and host names are configured on your server, choose the IP address that is in the same LAN as the devices.
- For the Cisco ITP-L and Cisco LAN Switch, the IP address of the device (this is the same address that is entered when the device is deployed in Cisco MNM).

Configuring the Cisco PGW 2200 Softswitch

For the procedure of configuring the Cisco PGW 2200 Softswitch for network management, see the section, "Configuring SNMP Support Resources", of the *Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide* at the following link

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9.8/Installation/Guide/Install98.html

Configuring the Cisco ITP-L

Use the following procedure to configure the Cisco ITP-L for network management:

Step 1   Access the Cisco ITP-L in either of the following ways:

- Enter the command:

    telnet *Cisco-ITP-L-IP-address*

- If the device has been deployed in Cisco MNM, in the Map Viewer, right-click the device and choose **Tools > Connection Service**.

    A Telnet window opens and the `password` prompt displays.

Step 2   Enter the login password for the Cisco ITP-L.

The `itp-l` prompt displays.

Step 3   Enter the command **enable**.

The `password` prompt displays.

Step 4   Enter the enable password for the Cisco ITP-L.

The `itp-l` prompt displays.

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

The `itp-l (config)` prompt displays.

Community strings can be found at snmpCommunityEntry. The following are default community entries:

```
snmpCommunityEntry  admin mgcusr mgcusr localSnmpID - - nonVolatile
snmpCommunityEntry  readonly public public localSnmpID - - nonVolatile
snmpCommunityEntry  user private private localSnmpID - - nonvolatile
```

> **Note**   Do not change the default values or attempt to add more entries.

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 Cisco MNM.

a.   To configure the Cisco ITP-L to send all types of traps, enter the command

```
snmp-server enable traps
```

b.   To configure the Cisco ITP-L 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
```

c.   To configure the IP address of Cisco MNM to which traps are sent, enter the command (in this example the IP address of the Cisco MNM is 10.1.1.1)

```
snmp-server host 10.1.1.1 public
```

By default, this trap will send out SNMP v1 traps. To send SNMP v2c traps, use the following command:

```
snmp-server host 10.1.1.1 version 2c public
```

Step 8   Set the SNMP trap source, which specifies the Cisco ITP-L interface from which traps are sent. The SNMP trap source should be the interface with the IP address that the Cisco MNM 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 ITP-L. If Cisco MNM is configured to communicate with the Cisco ITP-L using IP address 10.2.2.2 (the address given when the device is deployed in Cisco MNM), then the trap interface on the Cisco ITP-L 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 2KB by entering the command

```
snmp-server packetsize 2048
```

Step 10 To exit the configuration mode, press **Ctrl-Z**, and then enter the **write** command to write the configuration to Flash memory.

Configuring the Cisco LAN Switch Catalyst 2900XL

Use the following procedure to configure the Cisco Catalyst 2900XL LAN switch for network management:

Step 1 Access the Cisco LAN Switch in either of the following ways:

- Enter the command

  telnet *Cisco-LAN-switch-IP-address*

- If the device has been deployed in Cisco MNM, in the Map Viewer, right-click the device and choose **Tools > Connection Service**.

  A Telnet window opens and the `password` prompt.

Step 2 Enter the login password for the LAN switch.

The `2900xl` prompt displays.

Step 3 Enter the command **enable**.

The `password` prompt displays.

Step 4 Enter the enable password for the LAN switch.

The `2900xl` prompt displays.

Step 5 Enter the command and press Enter:

configure terminal

The `2900xl(config)` prompt displays.

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 Cisco MNM.

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 Cisco MNM to which traps are sent, enter the command (in this example the IP address of the Cisco MNM is 10.1.1.1)

snmp-server host 10.1.1.1 public

c. By default, this trap will send out SNMP v1 traps. To send SNMP v2c traps, use the following command:

snmp-server host 10.1.1.1 version 2c 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 Cisco MNM is configured to use for SNMP communications.

For example, let's assume that the IP address 10.2.2.2 is assigned to interface VLAN1 on the LAN switch. If Cisco MNM is configured to communicate with the LAN switch using IP address 10.2.2.2 (the address given when the device is deployed in Cisco MNM), 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 2KB by entering the command

```
snmp-server packetsize 2048
```

Step 10 To exit the configuration mode, press **Ctrl-Z**, and then enter the **write** command to write the configuration to Flash memory.

Configuring the Cisco Catalyst 5500 or 6509 LAN Switch

Use the following procedure to configure the Cisco Catalyst 5500 or 6509 LAN switch for network management:

Step 1 Access the Cisco LAN Switch in either of the following ways:

- Enter the command:

  ```
  telnet Cisco-LAN-switch-IP-address
  ```
- If the device has been deployed in Cisco MNM, in the Map Viewer, right-click the device and choose **Tools > Connection Service**.

  A Telnet window opens and the `password` prompt displays.

Step 2 Enter the login password for the LAN switch.

The `cat` prompt displays.

Step 3 Enter the command **enable**.

The `password` prompt displays.

Step 4 Enter the enable password for the LAN switch.

The `cat(enable)` prompt displays.

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
```

Community strings can be found at snmpCommunityEntry. The following are default community entries:

```
snmpCommunityEntry  admin mgcusr mgcusr localSnmpID - - nonVolatile
snmpCommunityEntry  readonly public public localSnmpID - - nonVolatile
snmpCommunityEntry  user private private localSnmpID - - nonvolatile
```

Do not change the default values or attempt to add more entries.

Step 6 Configure traps to be sent to Cisco MNM.

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

   `set snmp trap enable`

   b. To configure the IP address of the Cisco MNM to which traps are sent, enter the command (in this example the IP address of the Cisco MNM is 10.1.1.1):

   `set snmp trap 10.1.1.1 public`

✎
Note Currently, Catalyst 5500 and 6500 LAN switches only send snmp v1 traps, not snmp v2c or v3.

Step 7 To exit enable mode, enter **exit**.

Configuring a Cisco BAMS

Use the following procedure to configure a BAMS for network management:

Step 1 Access the BAMS in either of the following ways:

   • Enter the command:

   `telnet Cisco-<BAMS server>-IP-address`

   • If the device has been deployed in Cisco MNM, in the Map Viewer, right-click the device and choose **Tools > Connection Service**.

   A Telnet window opens.

Step 2 Use the following command to become the root user:

`su - root`

Step 3 Use the following command to change the directory:

`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 host name of the BAMS. The entry should be

`sysName <BAMS-server-hostname>`

Step 6 Enter the following lines after the existing snmpNotifyEntry lines:

```
snmpNotifyEntry 31 Console trap nonVolatile
snmpNotifyEntry 32 TrapSink trap nonVolatile
```

✎
Note The second field on each line (31 and 32 in the example) must be a value that is unique in the snmpNotifyEntry section.

Step 7 Enter the following lines after the existing snmpTargetAddrEntry lines:

```
snmpTargetAddrEntry 33 snmpUDPDomain 127.0.0.1:0 100 3 Console
\ v1ExampleParams nonVolatile 255.255.255.255:0 2048
```

```
snmpTargetAddrEntry 34 snmpUDPDomain 127.0.0.1:0 100 3 Console
\ v2cExampleParams nonVolatile 255.255.255.255:0 2048
```

- To send SNMP v1 traps, add the following lines:

```
snmpTargetAddrEntry 35 snmpUDPDomain 10.1.1.1:0 100 3 TrapSink
\ v1ExampleParams nonVolatile 255.255.255.255:0 2048
```

- To send SNMP v2c traps, add the following lines:

```
snmpTargetAddrEntry 36 snmpUDPDomain 10.1.1.1:0 100 3 TrapSink
\ v2cExampleParams nonVolatile 255.255.255.255:0 2048
```

Note
- In the example above, the IP address for Cisco MNM is 10.1.1.1, and the \ character entered at the end of the first line indicates that the entire command should be entered on one line.

- The second field on each line (33, 34, 35 and 36 in the example) must be a value that is unique in the TargetAddrEntry section.

Step 8 Verify that you have entered the exact information specified. UNIX is case-sensitive, so make sure that commands are entered in the same case each time they are entered.

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

Step 10 Determine the process ID of the SNMP daemon. From the Sun Solaris command line, enter the command

`# ps -ef | grep snmpdm`
The information that displays 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 11 Enter the following command to terminate the SNMP daemon:

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

Note The SNMP daemon restarts automatically after termination.

Configuring a Cisco HSI Server

Use the following procedure to configure an HSI server for network management:

Step 1 Access the Cisco HSI server in either of the following ways:

- Enter the command

`telnet Cisco-<HSI-server>-IP-address`
- If the device has been deployed in Cisco MNM, in the Map Viewer, right-click the device and choose **Tools > Connection Service**.

A Telnet window opens.

Step 2 Use the following command to become the root user:

```
su - root
```

Step 3   Enter the following command and press Enter:

```
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 host name of the HSI server. The entry should be

```
sysName <HSI-server-hostname>
```

Step 6   Community strings can be found at snmpCommunityEntry. Verify that the following default community strings are present:

```
snmpCommunityEntry  t0000000 public public localSnmpID - - nonVolatile
snmpCommunityEntry  t0000001 sysadmin sysadmin localSnmpID - - nonvolatile
```

✎
Note   Do not change the default values or attempt to add more entries.

Step 7   Enter the following line after the existing snmpNotifyEntry lines:

```
snmpNotifyEntry 32 rambler trap nonVolatile
```

Step 8   Enter the following line after the existing snmpTargetAddrEntry lines:

```
snmpTargetAddrEntry stae3 snmpUDPDomain 10.1.1.1:0 100 3 mgr1 stpe2 \
nonVolatile 255.255.255.255:0 2048
```

✎
Note   • In the example above, the IP address for Cisco MNM is 10.1.1.1, and the \ character entered at the end of the first line indicates that the entire command should be entered on one line.

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

Step 9   Verify that you have entered the exact information specified. UNIX is case-sensitive, so make sure that they are entered in the same case each time they are entered.

Step 10   Save the changes you made to the snmpd.cnf file.

Step 11   Determine the process ID. From the Sun Solaris command line, enter the command

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

Information displays that resembles the following:

```
root 565 1 0 Mar 20 ? 0:01 /opt/<HSI>/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 12   Enter the following command to terminate the SNMP daemon:

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

Note   The SNMP daemon restarts automatically after termination.

Getting Started with Cisco MNM

Revised: December 15, 2009, OL-18339-03

This chapter describes the basics of working with Cisco Media Gateway Controller (MGC) Node Manager (MNM). Topics include:

Starting and Quitting a Cisco MNM Session

This section describes how to start and quit a Cisco MNM session.

> **Note** If you are using VNC on Solaris 10 to access Cisco MNM, see the following URL for instructions on installing and configuring the VNC on the Solaris 10 platform from the Sun Microsystems website
>
> http://www.sun.com/bigadmin/jsp/descFile.jsp?url=descAll/install_and_configu
>
> In the configuration procedure described in the above URL, use the following line to replace the corresponding line when you are editing /etc/dt/config/Xservers.
>
> **:1   Local local_uid@console root /opt/sfw/bin/Xvnc :1 -httpd /opt/sfw/vnc/classes -depth 24 -geometry 1024x768 -r fbwait 120000 -rfbauth /opt/sfw/vnc/.vnc/passwd -rfbport 5901 -httpport 5801 -fp tcp/localhost:7100 -alwaysshared -co /usr/openwin/lib/X11/rgb -fp /usr/openwin/lib/X11/fonts/misc/, /usr/openwin/lib/X11/fonts/75dpi/**

Starting a Cisco MNM Session

You can start a Cisco MNM session when Cisco EMF is running. Use the following steps to start a Cisco MNM session:

Step 1 Log in as root.

Step 2 From the command line on the terminal window enter

cd <CEMF_ROOT>/bin

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

Note Because Cisco EMF is the element management framework upon which Cisco MNM is built, you need go into the <CEMF_ROOT> directory to start a Cisco MNM session.

Step 3 Verify that Cisco EMF is running.

Step 4 Enter

cemf query

You should see CEMF Manager 3.2 initialized followed by a list of running Cisco EMF processes.

Step 5 If Cisco EMF is not running, start it by entering the following command:

cemf start

Step 6 From the command line on the terminal window, enter

<CEMF_ROOT>/bin/cemf session

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

The Cisco EMF Login window displays, as shown in Figure 3-1.

Figure 3-1   *Cisco EMF Login Window*
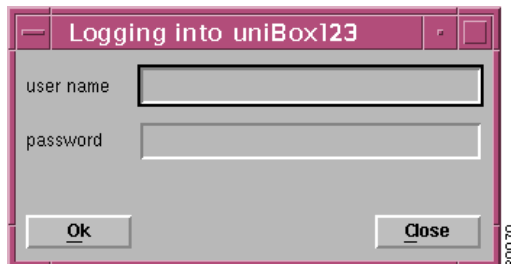
Step 7 Enter your user name and password, and click **OK**.

Note • The default user name and password is admin.

• If an unknown user name or password is entered, an error message displays. You are given three attempts to enter a valid user name and corresponding password. After three invalid entries, the session does not start and the Login window closes.

When a valid user name and password is entered, the session starts and the Cisco EMF Launchpad window displays, as shown in Figure 3-2.

Step 8 Continue to the "Opening an Application" section on page 3-4.

Quitting a Cisco MNM Session

You can quit a Cisco MNM session at any time. Quitting Cisco MNM closes any open applications or dialog boxes, but does not stop Cisco EMF. Use the following procedure to quit a Cisco MNM session:

Step 1   Do one of the following:

- From the File menu, select **Quit**.

- Press **Ctrl-Q**.

- Click the **Close** tool on the toolbar.

You are asked if you want to quit the Cisco EMF Manager system.

Step 2   Click **Yes** to quit the session.

All active applications are closed and the session terminates. Cisco EMF continues to run.

> **Note**   To stop Cisco EMF, you must be the root user.

Opening, Closing and Switching Cisco MNM Applications

Cisco MNM applications are the major groupings of network management functions. They include:

- Map Viewer—You can view, build, and monitor a network with Map Viewer. You can monitor the networks using network object connections.

- Object Group Manager—You can organize network elements into object groups with the Object Group manager. You can create, delete, and modify object groups.

- Access Manager—The Access menu allows an administrator to set up users and user groups, assign passwords, and define access parameters.

- Event Browser—Clicking the Events button initiates the Event Browser and Query Editor. You can create object groups or browse events from these windows.

- Discovery—Because Cisco MNM requires a log in and password to communicate with a device, the Cisco EMF Automatic Discovery feature is not supported by Cisco MNM. Cisco MNM discovers (and can automatically rediscover) device components and configurations once the device has been deployed: IP address, host name, and login information entered into Cisco MNM, as described in Chapter 5, "Deploying Your Network in Cisco MNM."

- Cisco MNM Manuals—Opens a Mozilla browser window and displays links to the following documents:

  - Cisco Media Gateway Control Node Manager End-User Guides
    You can also see these documents at
    http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/products_user_guide_list.html.

> **Note**   If the Cisco MNM is installed co-resident with another CEMF element manager, a button for that product's manual also displays.

- Event Manager

- 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 Groups—You can filter and organize events based on specified criteria, such as severity, state, or type of network element, and then create a scoreboard to show the state of the group at a glance.

- PreFilter—Pre-filter some messages collected in Cisco MNM according to the defined rules.

- Version—Display the version and patch information for Cisco MNM and Cisco VSPT (if installed together with Cisco MNM).

Once you have started a Cisco MNM session, you can open, close, and switch between applications.

Opening an Application

The Cisco EMF Launchpad (shown in Figure 3-2) is used to access Cisco MNM applications. You can open multiple applications, and you can open more than one instance of an application.

Figure 3-2   Cisco EMF Launchpad
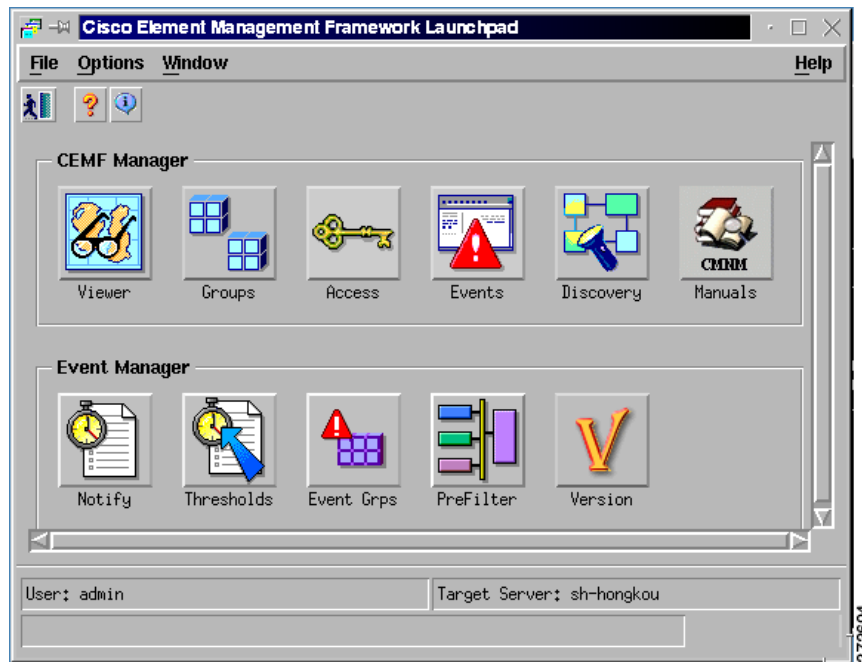
Use the following procedure to open an application:

On the Launchpad, click the icon to open the desired application. A busy icon and a message in the status bar displays while it is opening.

> **Note** If an application is already open, it displays in the drop-down menu on the Window toolbar. Click **Window**, and choose the desired application.

Closing an Application

Closing an application closes only the current instance of the application. Other instances of the application are unaffected. For example, if you separately opened an Event Browser for a Cisco BAMS and an Event Browser for a Cisco PGW 2200 Softswitch host, closing the Cisco PGW 2200 Softswitch host Event Browser window does not close the Cisco BAMS Event Browser window.

Use one of the following procedures to close an application:

- Choose **File > Close**.
- Click the window **Close** button.
- If the window has a toolbar, click the **Close** tool .
- Press **Alt-F4**.

Switching Between Open Application Windows

Working in Cisco MNM often involves having several windows open at the same time. You can view the list of open windows and switch between them from the drop-down menu on the Window toolbar, as shown in Figure 3-3.

Use the following steps to switch between windows:

Step 1 Click **Window** on the toolbar. The drop-down menu displays and lists all open windows.

Figure 3-3   Window Pull-Down Menu
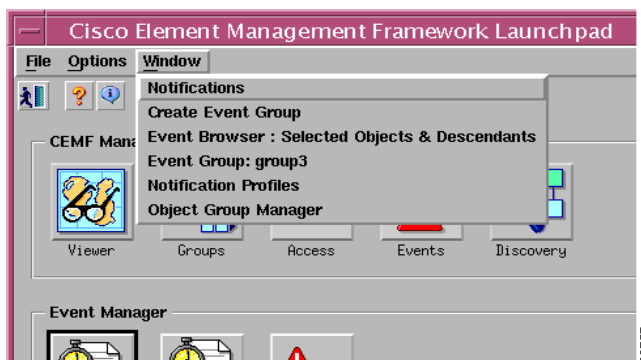
Step 2 Choose the desired window.

Basic Operations in Cisco MNM

This section describes basic operations that apply to Cisco MNM:

- Using the mouse, shortcut keys, or toolbar to access Cisco MNM features
- Selecting items in lists
- Printing the contents of a window
- Viewing Cisco MNM status information

> **Note** If you have problems printing the contents of a window, consult your system administrator to verify that your operating system is configured for printing.

Using the Mouse

The left, middle, and right mouse buttons are used for the following Cisco MNM functions:

- Click the left mouse button to
    - Select.
    - Activate.
    - Set the location of the cursor.
- Click the middle mouse button to
    - Copy.
    - Move.
    - Drag.
- To access context menus, click the right mouse button on a managed object within an application such as the Map Viewer, the Object Group Manager, and events in the Event Browser.

Using Shortcut Keys

Ctrl-Key

Standard Cisco MNM menus are available on the toolbar. You can click to select items from the menus or you can enter shortcut keys, as shown in Table 3-1 and Table 3-2.

Table 3-1   File Menu Shortcut Keys

Key Sequence	File Menu Function
Ctrl-Q	Quit
Ctrl-W	Close
Ctrl-P	Print
Ctrl-S	Save

Table 3-1   File Menu Shortcut Keys (continued)

Ctrl-N	New
Ctrl-O	Open

Table 3-2   Edit Menu Shortcut 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-Key

Items in the Cisco MNM menus and dialog boxes may be displayed with the first (initial) letter underlined (for example, Actions.) This means that you can either select this option by clicking the mouse, or you can press **Alt**-**A**.

Tip   You can use the X windows standard **Alt-4** to close the current window.

Using the Toolbar

In Cisco MNM application windows, a toolbar contains tool buttons for commonly used menu options. You can toggle the toolbar on or off and choose to display or hide tooltips.

In Figure 3-4, the toolbar contains tool buttons for the following functions common to many dialog boxes:

- Close the current window.
- Print the contents of the window.

Figure 3-4   Example Toolbar

Note   If you have problems printing the contents of a window, consult your system administrator to verify that your operating system is configured for printing.

- Toggle dynamic update mode to allow viewing or not viewing real-time changes.
- Refresh the window to update the information when dynamic update mode is off.
- Acknowledge that you have seen dynamically updated dialog box changes.

Hiding or Showing the Toolbar

To toggle the display of the toolbar for the current window, choose **Options > Show Toolbar**.

Hiding or Showing Tooltips

Tooltips provide a brief description 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.

To toggle the display of tooltips for the toolbar in the current window, choose **Options > Enable Tooltip**.

Selecting from Lists

To perform an operation on more than one item, you can select:

- A block of items
- Multiple items in different areas of a list
- All items

You can also deselect all items. For instructions, see the "Use the following steps to deselect all items:" task on page 3-9

Use the following steps to select a block of items:

Step 1	Click the first item in the block.
	The item is highlighted.
Step 2	Press and hold the **Shift** key.
Step 3	Click the last item in the block.
Step 4	Release the **Shift** key.
	All items between the first and last item are highlighted.

Use the following steps to select multiple items in different areas of a list:

Step 1	Click the first item.
	The item is highlighted.
Step 2	Press **Ctrl** and click the next item you want to select.
	The item is highlighted.
Step 3	Repeat Step 2 and Step 3 until all the desired items are highlighted.

Use the following steps to select all items:

Step 1   Place the cursor anywhere in the window.

Step 2   Press and hold the right mouse button.

A context menu displays.

Step 3   Choose **Select All**.

> ✎
>
> **Note**   This option is not available in all windows.

All items in the list are highlighted.

Use the following steps to deselect all items:

Step 1   Place the cursor anywhere in the window.

Step 2   Press and hold the right mouse button.

A context menu displays.

Step 3   Choose **Deselect**.

> ✎
>
> **Note**   This option is not available in all windows.

All items in the list are deselected.

Printing the View Displayed in the Window

In most windows you can print the contents.

> ✎
>
> **Note**   If you have problems printing the contents of a window, consult your system administrator to verify that your operating system is configured for printing.

To print the contents of the current window, do one of the following:

- From the File menu, choose **Print**.
- Press **Ctrl-P**.
- Click the **Print** tool on the toolbar.

The current view is printed.

Viewing Cisco MNM Status Information

The status bar at the bottom of most windows displays status information about the current Cisco MNM application status (not about network status).

To view previous status messages, double-click in the status bar. The Status Dialog displays, as shown in Figure 3-5.

Figure 3-5   Status Dialog

Using the Map Viewer

The Map Viewer organizes the network display into various views and is the starting point for most Cisco MNM network management operations. Each view represents a different way of containing and grouping the network elements, such as device type, Cisco PGW 2200 Softswitch node, and physical or network view.

In the Map Viewer you can

- Deploy an entire network or a single new device.
- See at a glance which devices have generated alarms. Because the alarm display is propagated from the originating object up through the containing objects, you can quickly drill down to find the source of the problem.

Note Propagation applies to the node and physical views. Alarms are not propagated in device views.

- Identify information about a device by its graphical representation. State icon, color, cross-hatching pattern are some of the indicators that give you a quick graphical read of the network condition.
- Access network devices by navigating through one of the views to the desired object and then right-clicking to open any of the Cisco MNM services relevant to that device.
- View the network in different ways. For example, you can use the physical view to see where devices are located, the device view to perform an operation on all devices of a particular type, and the node view to see node-specific elements such as signaling components.

Note The term "object" refers to the graphical representation of a network element in Cisco MNM and the term "device" refers to the real-world counterpart that is represented and manipulated by the object.

This section describes the basics of how to use the Map Viewer. The Map Viewer display is based on the Cisco MNM object model of the network. For an explanation of the concepts and some of the technical details behind the Map Viewer, see Chapter 1, "Overview of Cisco Media Gateway Controller Node Manager," "How Cisco MNM Models the Network" section on page 1-9.

This section describes:

- The Map Viewer window and views.

- How to expand a view, to get to an object, and collapse a view.

- How to read the visual symbols associated with objects in the Map Viewer.

- How to use the context menu to open a Cisco MNM service for the current object. (This is your entry point to most network management functions.)

For more information on the Map Viewer, refer to "Map Viewer" in the Cisco EMF online help.

Map Viewer Window

Until you have deployed a network in Cisco MNM, the Map Viewer displays only empty container objects.

Figure 3-6   Map Viewer Before a Network Is Deployed
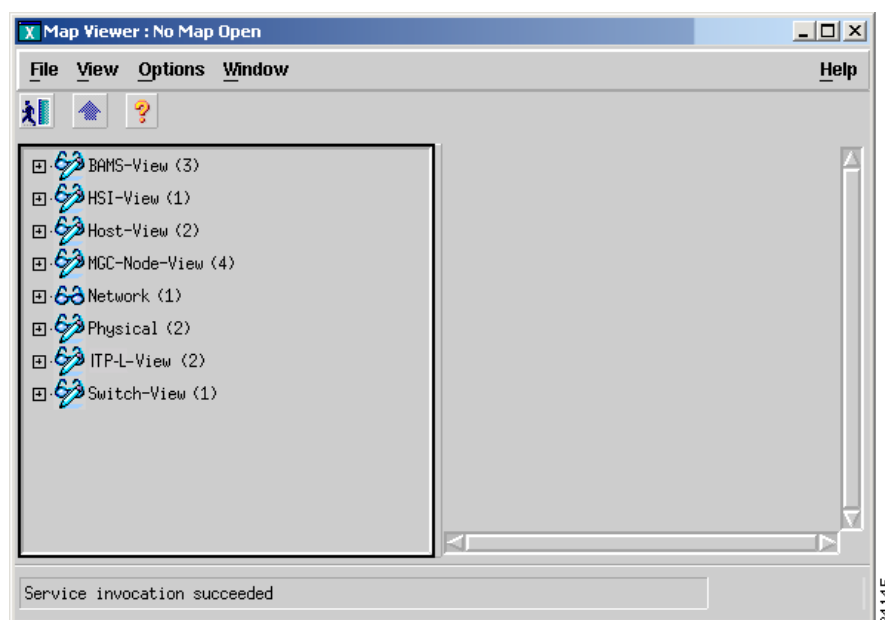
When you deploy a network, (see Chapter 5, "Deploying Your Network in Cisco MNM") the views are populated with the graphical objects that represent your network devices. Initially, the view is collapsed, as shown in Figure 3-7.

Figure 3-7   Map Viewer After Deployment
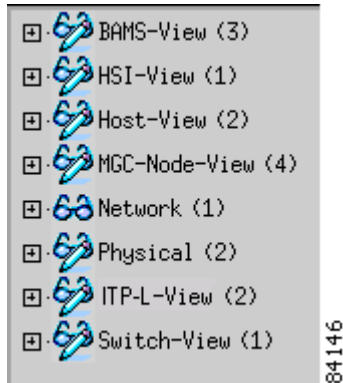
When a view is expanded, the Map Viewer looks similar to the illustration shown in Figure 3-8.

Figure 3-8   Typical Appearance of the Map Viewer
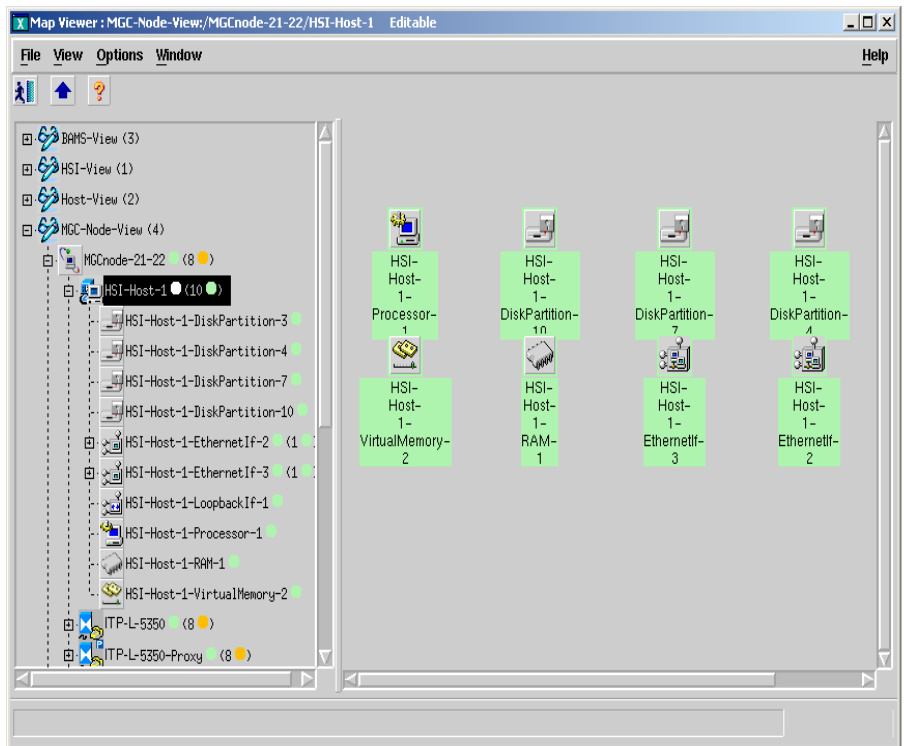
- The Map Viewer window is divided into two panes. The left pane is a hierarchy browser. The right pane displays a map of the object selected in the right pane. The map is a detailed depiction of the selected device or site.

- Resize the hierarchy browser pane and map pane by positioning your cursor over the boundary and dragging.

- Use the scroll bars to view all information in the left and right panes.

- You can open a service on a device object by right-clicking the object and choosing the service from the context menu. To open a service on multiple devices, select the devices, and then right-click.

Note   The context menu displays the list of services available for the selected device or devices. Services available depend on your access privileges. If multiple objects are selected, only services common to all selected objects are available.

Map Viewer Views

This section describes the various Map Viewer views.

Node View

The node view shows all the devices in the node, as well as the Cisco PGW 2200 Softswitch host signaling, dial plan, and trunking components.

Use the node view to:

- Deploy a node and devices within a node. In a conventional node, you deploy one or a pair of Cisco PGW 2200 Softswitch hosts under the node. In a farm, you deploy a farm under the node, and then deploy one or a pair of Cisco PGW 2200 Softswitch hosts under the farm, as shown in Figure 3-12.
- View alarm propagation. Alarms are propagated from child devices to parent devices anywhere in the node, and you can drill down through the tree to find the element raising the alarm.
- View signaling, trunking, and dial plan information.
- Open applications for signaling, trunking, and dial plan components.

Figure 3-9 shows an example of the node view. Figure 3-10 and Figure 3-11 show expansions of the signaling and trunking folders. Figure 3-12 shows an example of a farm folder.

Figure 3-9   Node View
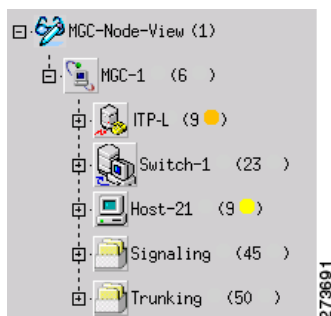
Figure 3-10   Signaling Folder
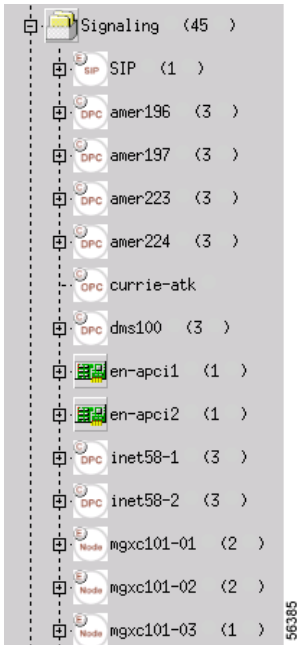
Figure 3-11   Trunking Folder
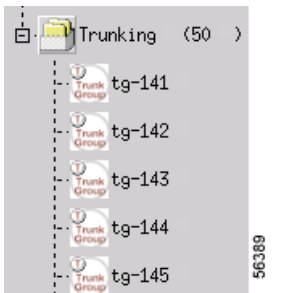
Figure 3-12   Farm Folder
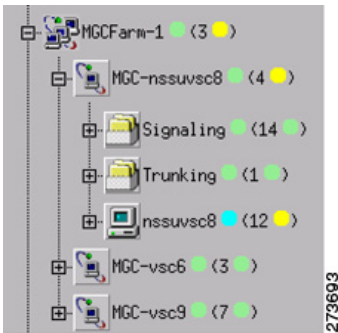
Device Views

The device views group devices by their type. Use device views to view and manage all the devices of a particular type.

✎ **Note** Alarms are not propagated in device views. Use the node view or physical view to propagate alarms.

🔍 **Tip** To open a Cisco MNM service for a group of devices, open the service from the device view. The dialog box lists all the devices. You can select each desired device in turn.

Cisco PGW 2200 Softswitch Host View

This view shows all Cisco PGW 2200 Softswitch hosts. Use host view to:

- View and manage all hosts
- View and manage host system components, such as disk, RAM, memory, processor, and interfaces

Figure 3-13   Cisco PGW 2200 Softswitch Host View
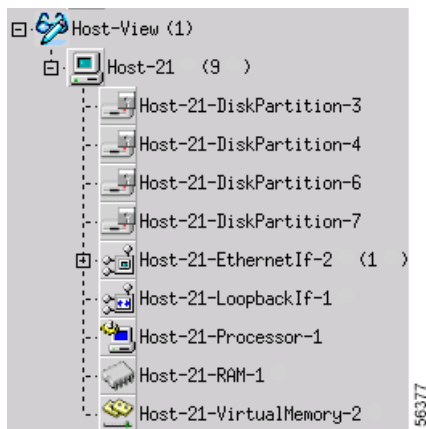
Cisco ITP-L View

✎ **Note** Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, ITP-L will replace SLT in publications and the product.

This view shows all the Cisco ITP-Ls, integrated ITP-Ls and integrated ITP-L coresident EMs. Use Cisco ITP-L view to:

- View and manage all of the Cisco ITP-Ls
- View and manage ITP-L interfaces, including TDM interfaces

Different icons are used for different types of ITP-Ls, as shown below.

Type of ITP-L	Icon
Standalone ITP-L	
Integrated ITP-L	

Figure 3-14   Cisco ITP-L View
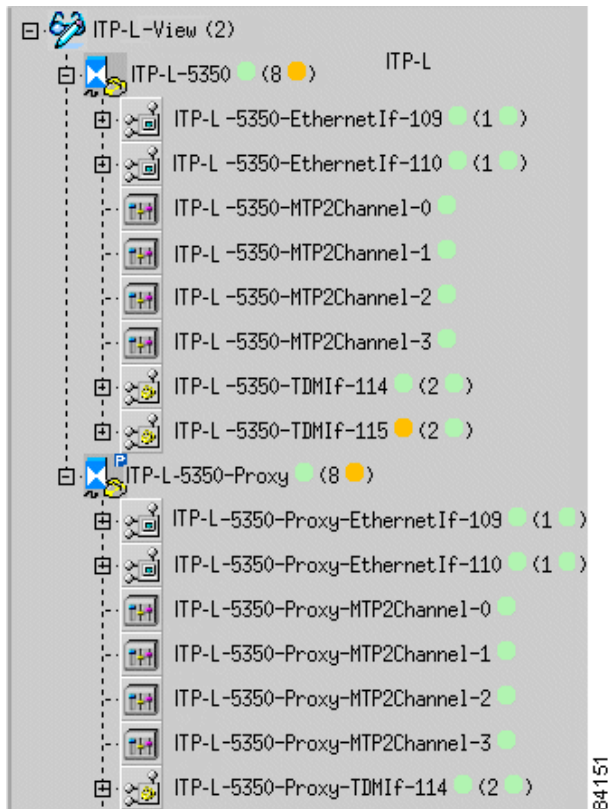
Cisco LAN Switch View

This view shows all Cisco LAN switches. Use this view to:

- View and manage all Cisco LAN switches
- View and manage switch components, such as interfaces, modules, and ports

Figure 3-15   LAN Switch View
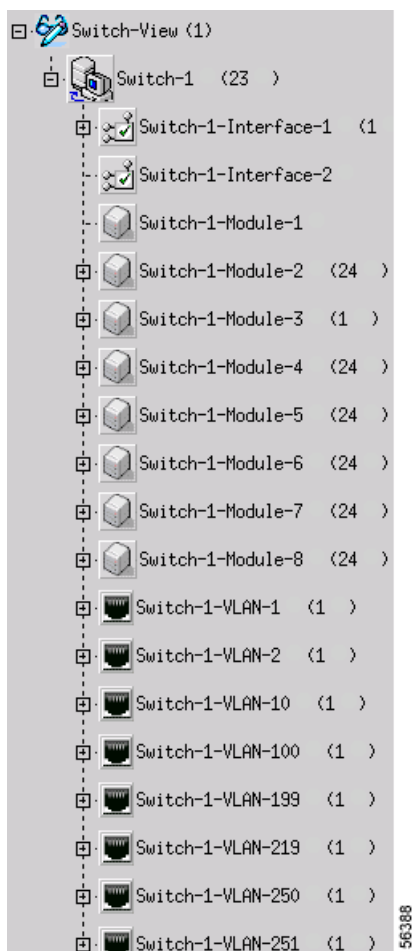
BAMS View

This view shows all Cisco BAMS machines. Use BAMS view to:

- View and manage all Cisco BAMS machines
- View and manage Cisco BAMS system components, including disk, RAM, memory, and interfaces

Figure 3-16   BAMS View
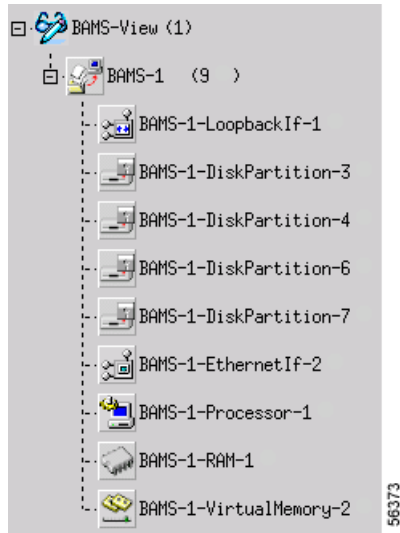
HSI View

This view shows all Cisco HSI servers. Use this view to:

- View and manage all Cisco HSI servers
- View and manage Cisco HSI system components, including disk, RAM, memory, and interfaces

Figure 3-17   HSI View

Physical View

This view organizes the network by physical location. You can define a hierarchy of regions and sites, such as cities, buildings, and floors (see Figure 3-18). When you deploy the network, you can identify the physical region or site associated with each network device.

Use the physical view to:

- Deploy regions and sites—Select the container object for the level you want to deploy. For example, select a Southeast region object to deploy an Atlanta site.

- View alarm propagation—Alarms are propagated from child devices to parent devices. Drill down through the tree to find the element raising the alarm.

- Identify where a problem device is located—For example, in Figure 3-18, a problem is indicated in the Stonybrook building, which is propagated upward to the Raleigh and Southeast sites.

- Visualize the physical network.

Figure 3-18   *Physical View*

Network View

This view shows the IP addresses of the network devices.

Figure 3-19   *Network View*
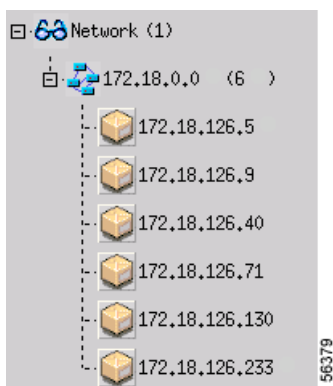
Expanding or Collapsing a View

In the left hierarchy browser pane, a plus sign (+) next to an object means it contains other objects and can be expanded. A minus sign (-) means that the object is fully expanded.

- To expand a view, click the + next to the object, as shown in Figure 3-20.

- To drill down to an object, continue expanding the view until you see the desired object.
- To collapse a view, click the - next to the object.

Tip When you see an alarm symbol next to an object, drill down to find the object generating the alarm.

Figure 3-20   Expanding a View in the Map Viewer
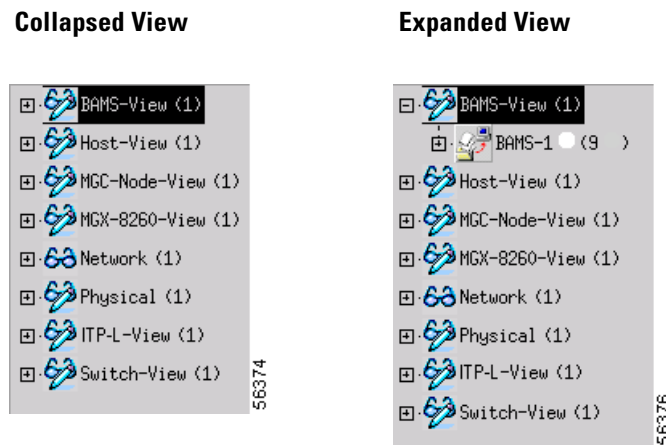
Understanding Map Viewer Symbols

Indicators in the Map Viewer reflect the status of the associated object and the occurrence of alarm events. For example, a polling icon indicates that a device or its child is being polled. In this way, the states of the Cisco PGW 2200 Softswitch subobjects are propagated up to the Cisco PGW 2200 Softswitch node object.

Similarly, alarm events, indicated with a color-coded circle in the left pane and a balloon in the right pane, are propagated up in the physical and node view.

For some states, a small symbol is placed near the top of the icon. Cross-hatching is used to indicate state information.

Table 3-3 lists and describes status and event symbols. Table 3-4 displays the color-coding used for alarm events. For more information about alarm events, see Chapter 6, "Managing Faults with Cisco MNM."

Table 3-3   Status and Event Symbols

Symbol	Description
	(In the left pane) Indicates the number of child devices. In the physical and network views, a circle indicates an event on one or more child devices, color-coded to severity. The highest severity is displayed.
	(In the right pane) A balloon indicates events, color-coded to severity. The number indicates the number of the most severe events in the category. The letter indicates the highest unacknowledged event severity in the category.

Table 3-3   Status and Event Symbols (continued)
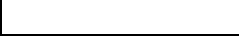
Symbol	Description
	Indicates that the device has not been discovered. (This is the icon that displays when the device is initially deployed.)
	Indicates that the device is in the process of discovering or rediscovering. The object icon itself has a hatch pattern.
	Indicates that the device has some 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.

Table 3-4   Colors Used to Indicate Event Severity

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

Use the Map Viewer to open a function, such as the Performance Manager or a Properties dialog box, for a device or group of devices.Use the following steps to open a function for a device:

Step 1   In the Map Viewer, navigate to the desired object.

> **Note** To open a Cisco MNM service for a group of devices, open the service from the device view. The dialog box contains a list box of all the devices. You can select each desired device in turn.

Step 2 Right-click the object. The context menu displays showing the functions available for the selected object or objects.

Step 3 Choose the desired option. Table 3-5 summarizes how to access various services.

A window opens for the service. For example, if you choose **Properties**, a Properties dialog box displays the properties of the selected device.

> **Note** • Some functions can be opened from the Event Browser as well as the Map Viewer.
>
> • If SSH is enabled, functions that normally invoke Telnet or ftp instead invoke their SSH counterparts, ssh or sftp.

Table 3-5   Opening Cisco MNM Functions

Function	Select This View or Object	Command: Right-Click and Choose...	Description
Cisco PGW 2200 Softswitch Node Deployment	MGC-Node-View	**Deployment > Deploy MGC Node**	Deploys a new Cisco PGW 2200 Softswitch node
Cisco PGW 2200 Softswitch Host Deployment	Host-View Cisco PGW 2200 Softswitch Node	**Deployment > Deploy MGC Host** **Deployment > Deploy MGC Node Component**	Deploys a new Cisco PGW 2200 Softswitch host
ITP-L Deployment	ITP-L-View Cisco PGW 2200 Softswitch Node	**Deployment > Deploy ITP-L** **Deployment > Deploy MGC Node Component**	Deploys a new Cisco ITP-L or integrated ITP-L
LAN Switch Deployment	Switch-View Cisco PGW 2200 Softswitch Node	**Deployment > Deploy LAN Switch** **Deployment > Deploy MGC Node Component**	Deploys a new Cisco LAN switch
BAMS Deployment	BAMS-View Cisco PGW 2200 Softswitch Node	**Deployment > Deploy BAMS** **Deployment > Deploy MGC Node Component**	Deploys a new Cisco BAMS
HSI Deployment	HSI-View Cisco PGW 2200 Softswitch Node	**Deployment > Deploy HSI** **Deployment > Deploy MGC Node Component**	Deploys a new Cisco HSI host device
Seed File Deployment	Any view icon (action applies to entire network)	**Deployment > Deploy Network Seed File**	Displays Seed File deployment dialog

Table 3-5   Opening Cisco MNM Functions (continued)

Function	Select This View or Object	Command: Right-Click and Choose...	Description
Performance Manager	Cisco PGW 2200 Softswitch Node, BAMS, HSI, ITP-L, or LAN Switch at level of managed element	**Tools > Performance Manager**	Opens Performance Manager application to monitor performance measurements
Cisco PGW 2200 Softswitch Node States	MGC-Node-View, Cisco PGW 2200 Softswitch Node	**MGC Node States**	Opens MGC Node States dialog
Cisco PGW 2200 Softswitch Host Properties	Host-View or Node View, Cisco PGW 2200 Softswitch Host	**Properties**	Opens Host Properties dialog
Cisco PGW 2200 Softswitch Host File System Properties	Host-View or Node View, Cisco PGW 2200 Softswitch Host	**File Systems**	Opens Host File System properties dialog
Cisco PGW 2200 Softswitch Host System Component Properties	Cisco PGW 2200 Softswitch Host	**Devices**, then the desired component: **Disk Partition, Processor, RAM, or Virtual Memory**	Opens the properties dialog for the selected system component
Cisco PGW 2200 Softswitch Host States	Host-View or Node View, Cisco PGW 2200 Softswitch Host	**States**	Opens Host States dialog
Cisco PGW 2200 Softswitch Host Accounts	Host-View or Node View, Cisco PGW 2200 Softswitch Host	**Accounts**	Opens Host Accounts dialog
Cisco PGW 2200 Softswitch Host Diagnostics	Host-View or Node View, Cisco PGW 2200 Softswitch Host	**Tools > MGC Host Diagnostics**	Opens Host Diagnostic dialog
ITP-L Properties	ITP-L-View or Node View, ITP-L	**Properties**	Opens ITP-L Properties dialog
ITP-L States	ITP-L-View, ITP-L	**States**	Opens ITP-L States dialog
ITP-L Accounts	ITP-L-View, ITP-L	**Accounts**	Opens ITP-L Accounts dialog
ITP-L Diagnostics	ITP-L-View, ITP-L	**Tools > ITP-L Diagnostics**	Opens ITP-L Diagnostic dialog

Table 3-5   *Opening Cisco MNM Functions (continued)*

Function	Select This View or Object	Command: Right-Click and Choose...	Description
LAN Switch Properties	Switch-View or Node View, LAN Switch	**Properties**	Opens LAN Switch Properties dialog
LAN Switch States	Switch-View or Node View, LAN Switch	**States**	Opens LAN Switch States dialog
LAN Switch Accounts	Switch-View or Node View, LAN Switch	**Accounts**	Opens LAN Switch Accounts dialog
LAN Switch Diagnostics	Switch-View or Node View, LAN Switch	**Tools > LAN Switch Diagnostics**	Opens LAN Switch Diagnostic dialog
BAMS Properties	BAMS-View or Node View, BAMS	**Properties**	Opens BAMS Properties dialog
BAMS File System Properties	BAMS-View or Node View, BAMS	**File Systems**	Opens BAMS File System properties dialog
BAMS System Component Properties	BAMS	**Devices**, then the desired component: **Disk Partition, Processor, RAM, or Virtual Memory**	Opens the properties dialog for the selected system component
BAMS States	BAMS-View or Node View, BAMS	**States**	Opens BAMS States dialog
BAMS Accounts	BAMS-View or Node View, BAMS	**Accounts**	Opens BAMS Accounts dialog
BAMS Diagnostics	BAMS-View or Node View, BAMS	**Tools > BAMS Diagnostics**	Opens BAMS Diagnostic dialog
BAMS Node Properties	BAMS-View or Node View	**Properties**	Opens BAMS Node Properties dialog
BAMS Node Diagnostics	BAMS-View or Node View	**Tools > BAMS Diagnostics**	Opens BAMS Node Diagnostic dialog
Trunking Configuration Audit	BAMS	**Tools > BAMS Diagnostics > Audit**	Opens the Configuration Audit dialog
H323 Properties	HSI-View, HSI Host	**Properties**	Opens the H323 Properties dialog
H323 File Systems	HSI-View, HSI Host	**File Systems**	Opens the H323 File Systems dialog
H323 States	HSI-View, HSI Host	**States**	Opens the H323 States dialog
H323 Accounts	HSI-View, HSI Host	**Accounts**	Opens the H323 Accounts dialog

Table 3-5   Opening Cisco MNM Functions (continued)

Function	Select This View or Object	Command: Right-Click and Choose...	Description
H323 Diagnostics	HSI-View, HSI Host	**Tools > Diagnostics**	Opens the H323 Diagnostics dialog
H323 Administration Tool	HSI-View, HSI Host	Administration Tool	Opens the H323 Administration Tool dialog
Signaling Dialogs	Signaling folder, all signaling components	**Properties**	Opens the various signaling component property dialogs, one for each type of signaling component
Trunking Dialogs	Trunking folder, all trunk group components	**Properties**	Opens the various trunking component property dialogs, one for each type of component
Dial Plan Properties Dialogs	Dial plan folder, all routing components	**Properties**	Opens the various dial plan component property dialogs, one for each type of routing component
Network Interface or Component Properties	The individual interface or component under a device	**Properties**	Opens the properties dialog for the selected network interface or component (interface, port, slot, and so forth)
Network Interface or Component Properties, a set of components	The device	**Component Type > Component Properties**, for example, **Interfaces > TDM Properties**	Opens the properties dialog for all components of that type on the selected device
Event Browser (can also be opened from Launchpad)	Any device that forwards traps to Cisco MNM	**Tools > Open Event Browser**	Opens Event Browser for the selected device(s)
Performance Manager	Any device that collects performance data and is in polling state	**Tools > Performance Manager**	Opens Performance Manager for the selected device(s)
Voice Services Provisioning Tool	Cisco PGW 2200 Softswitch Host, BAMS	**Tools > Voice Services Provisioning Tool**	Starts Cisco Voice Services Provisioning Tool application (detects correct release for Cisco PGW 2200 Softswitch software and correct level of user privileges).

Table 3-5   Opening Cisco MNM Functions (continued)

Function	Select This View or Object	Command: Right-Click and Choose...	Description
Cisco PGW 2200 Softswitch Toolbar	Cisco PGW 2200 Softswitch Host	**Tools > MGC Host Toolbar**	Opens MGC Host toolbar applications
HSI Alarm Viewer	HSI Host	**Tools > HSI Alarm Viewer**	Launches HSI Alarm Viewer application
HSI Log Viewer	HSI Host	**Tools > HSI Log Viewer**	Launches HSI Log Viewer application
XTerm	Cisco PGW 2200 Softswitch Host, BAMS, HSI server	**Tools > Xterm**	Opens an XTerm window
CiscoView	LAN Switch, ITP-L	**Tools > CiscoView**	Opens CiscoView application
Connection Service	Cisco PGW 2200 Softswitch Host, BAMS, HSI server, ITP-L, LAN Switch	**Tools > Connection Service**	Opens UNIX Telnet application or SSH, depending on whether SSH is enabled on both Cisco MNM and the device its connecting to
Web Browser (Mozilla)	ITP-L, Catalyst 2900XL	**Tools > Web Browser**	Opens a web browser, pointing to the internal web server on Cisco ITP-Ls and Catalyst 2900XLs
Administration tool (system administrators only)	Cisco PGW 2200 Softswitch Host, BAMS, HSI server, ITP-L, LAN Switch, or device view for all devices of the same type	**Tools > Administration Tool**	Opens the device administration dialog box to allow rebooting or shutting down the device

Understanding Cisco MNM Dialog Boxes

Cisco MNM dialog boxes are summarized below:

- Many dialog boxes display popup field descriptions when you pass your pointer over a field name.

- If a container object is selected when the dialog box is opened, the dialog box can be used to view or manipulate properties for any of the selected devices.

- Because Cisco MNM supports multiple releases of the Cisco PGW 2200 Softswitch software, some fields in property dialog boxes may not apply to your release.

- Some dialog boxes display information received from a managed device and others display information about that device residing in the Cisco MNM database. Toolbar buttons in the dialog box can help you recognize the difference and how the information can be updated.

The features of Cisco MNM dialog boxes are described in the following sections.

Displaying Field Descriptions

In many dialog boxes, you can view a description of the current field by slowly passing the cursor across the field name, as shown in Figure 3-21.

Figure 3-21   *Context Help*
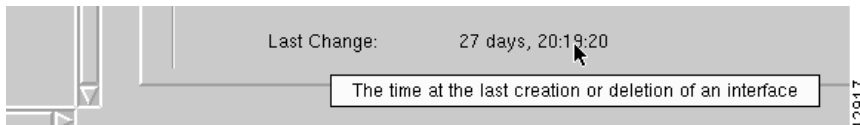
Displaying Information for Multiple Devices

You can open a dialog box on multiple devices of the same type. For example, you can:

*   Select a device view to open a service on all devices of that type.
*   Select a device chassis to open a Properties dialog box on all subcomponents of a particular type.

Use the following steps to display information for multiple devices:

Step 1   Select the devices. See the "Selecting from Lists" section on page 3-8 for details on selecting multiple objects.

Step 2   Right-click, and choose the desired option.

✎ **Note**   If an option is not available for the multiple devices you have selected, the option name is dimmed.

The dialog box opens. A list box in the left pane lists the selected devices. Figure 3-22 shows an example (properties for all TDM interfaces of a Cisco ITP-L).

Step 3   To view or manipulate information for a particular device, select the device in the list box. The information on the right changes to reflect the current selection.

Figure 3-22   *Dialog Box with Information on Multiple Devices*
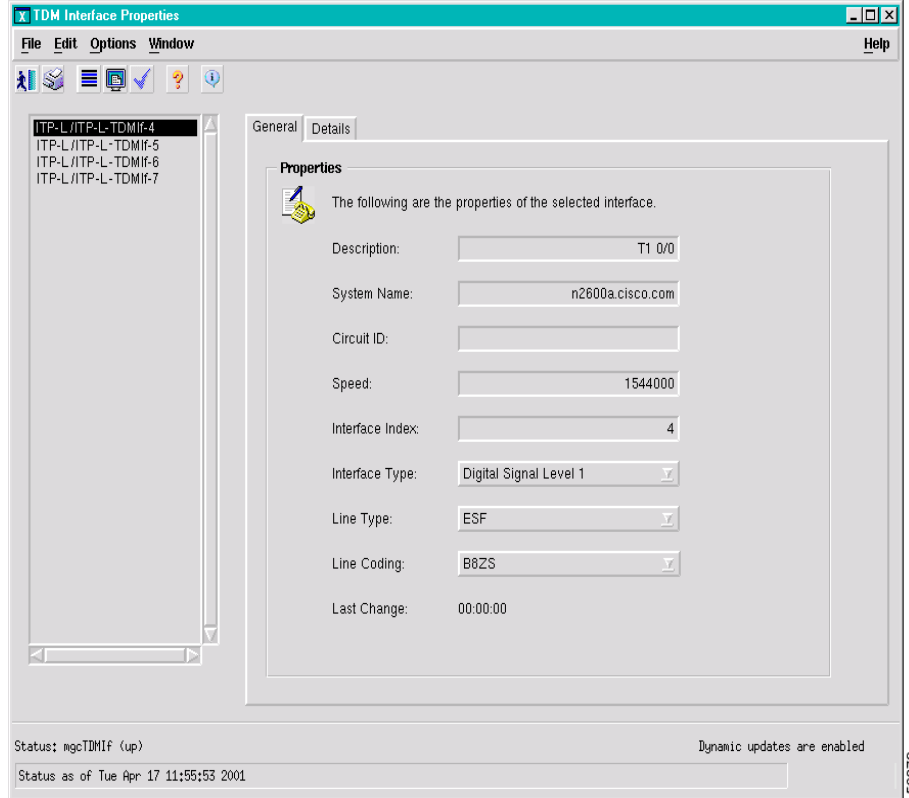
Properties for Multiple Releases of the Cisco PGW 2200 SoftswitchSoftware

Each new release of the Cisco PGW 2200 Softswitch software supports additional properties of the Cisco PGW 2200 Softswitch node elements.

Because Cisco MNM supports multiple Cisco PGW 2200 Softswitchsoftware releases, some dialog boxes may display some fields that might not be applicable to your release of the Cisco PGW 2200 Softswitch software. For example, the H.248 Path Properties dialog box includes the property, Label, for Cisco PGW 2200 Softswitch software Release 9.8. If you are using Cisco PGW 2200 Softswitch software Release 9.7, this field is empty.

In general, Cisco MNM is tested and supported only on Cisco PGW 2200 Softswitch Releases 9.8(1), 9.7(3), and 9.6(1).

Figure 3-23   *A Dialog Box with Properties for Multiple Cisco PGW 2200 Softswitch Releases*
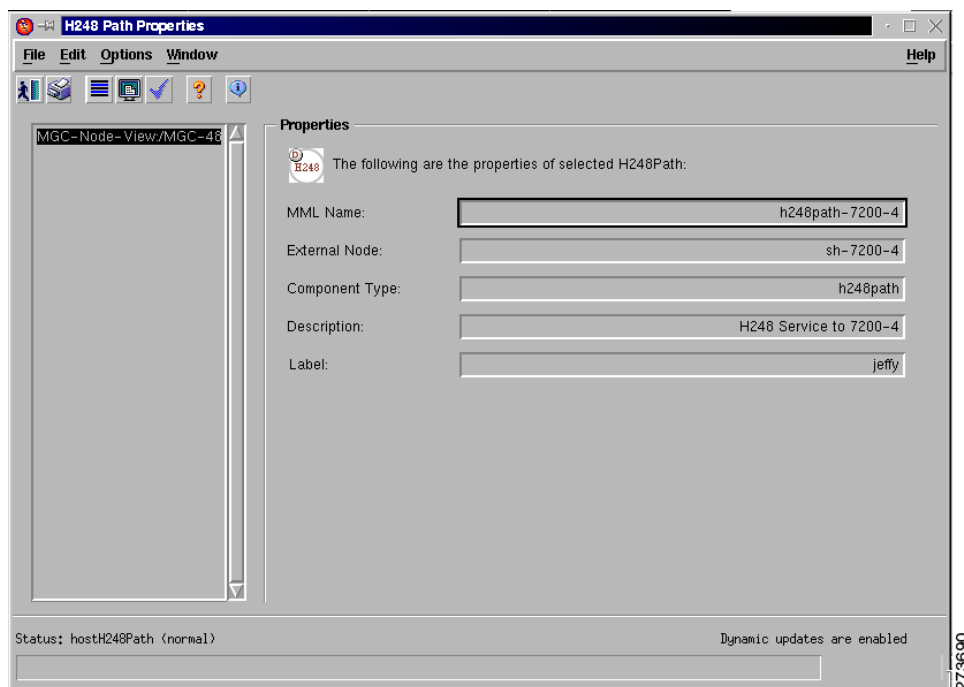
Working with Various Types of Dialog Box Information

Cisco MNM dialog boxes display two kinds of information about network devices:

- Information that comes from the device itself, such as properties or alarm events, or from Cisco MNM interaction with the device, such as state information

- Information that resides in the Cisco MNM database and is used by Cisco MNM to communicate with the device, such as account information

Information that comes from the device is display-only and cannot be edited or modified. To turn on "Dynamic Update" mode for real-time monitoring of the device, see the "Monitoring Dynamically-Updated Information" section on page 3-30.

✍

Note   Information that resides in the Cisco MNM database can typically be changed. However, you are changing only the Cisco MNM database and not information stored on the device itself.

This section describes

- How to recognize and work with a dialog box that displays dynamically updated information

- How to recognize and use field changes that are applied to the device from a dialog box where information is display only

Monitoring Dynamically-Updated Information

Many dialog boxes display in near real-time information received from a managed device. With dynamic update on, incoming changes from a device are highlighted in blue (see Figure 3-24). The status bar indicates whether dynamic updating is on or off. This kind of information is display only; it cannot be changed.

Figure 3-24   Dialog Box with Dynamic Updating
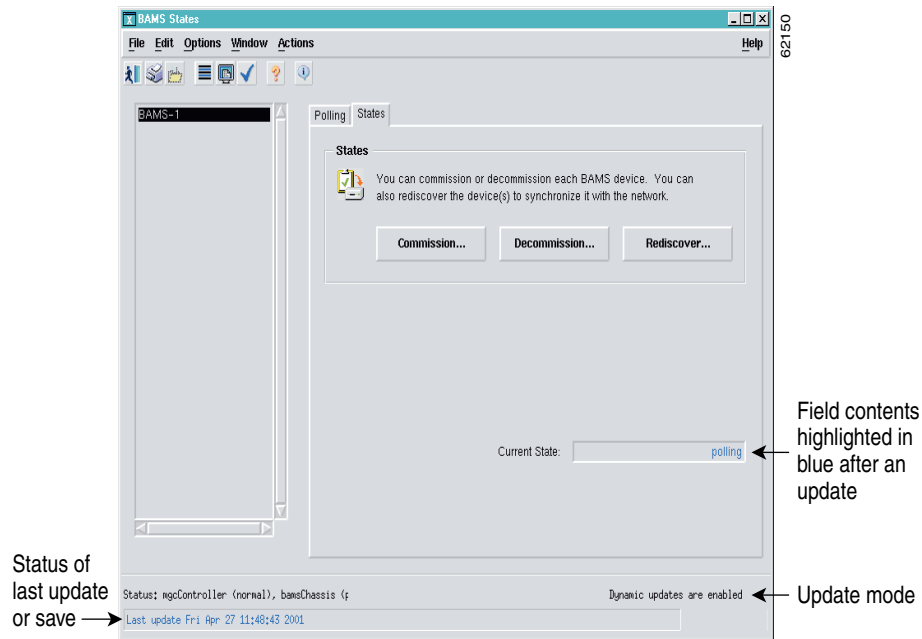
The toolbar in these dialog boxes includes the three tool buttons in Figure 3-25 used for managing updates:

- Toggle dynamic update mode, to allow viewing of real time changes.
- Refresh the window, to update the information manually when dynamic update mode is off.
- Acknowledge that you have seen dynamically updated dialog box changes. When clicked, the blue highlighting is removed.

Note   Some dialog boxes include both dynamically updatable information from managed devices and information about the network maintained in the Cisco MNM database. The toolbar in Figure 3-25 also includes a Save tool used for saving changes to database information, as described in the "Making Changes to Cisco MNM Device Information" section on page 3-31.

Figure 3-25   Dialog Box Toolbar with Dynamic Update and Database Save Functions
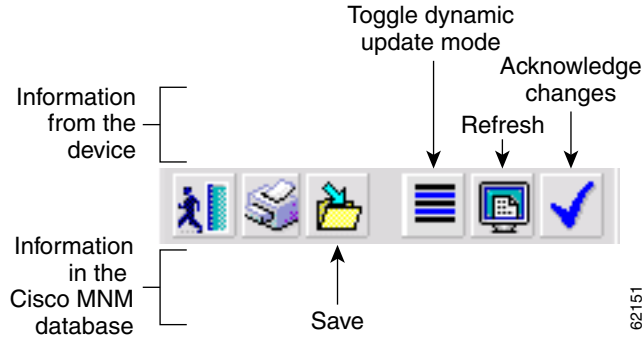
Making Changes to Cisco MNM Device Information

Some dialog boxes display information that you can edit. For example, if the login ID for a device changes, you can use the Accounts dialog box for that device to update the information in the Cisco MNM database. In dialog boxes that include editable information, the toolbar includes a **Save** tool button, as shown in Figure 3-25.

To make changes to the Cisco MNM database, enter the new information, and click the **Save** tool button.

Note   If you try to make a change but the **Save** tool button remains dimmed, the field is not editable.

Navigating between Dialog Boxes for a Given Component

For most Cisco PGW 2200 Softswitch node components, you can navigate from one dialog box to another without having to reselect the component in the Map Viewer and right-click. For example, from the File Systems dialog box for a given Cisco BAMS, you can navigate to the Properties, Accounts, States, or Diagnostics dialog box for that Cisco BAMS.

Perform the following steps to navigate from one dialog box to another not-yet-open dialog box for a given component:

Step 1   In the open dialog box, choose **Navigation**. A menu appears listing options to open other dialog boxes for this component. See Table 3-6 for a list of components and dialog boxes that provide the Navigation menu.

Step 2   Choose the desired menu option. The selected dialog box opens.

Note   Once a dialog box is open, use the Window menu on the toolbar to navigate between windows.

Table 3-6   *Components with Dialog-Box Navigation Menus*

Component	Dialog Boxes with the Navigation Menu
Cisco PGW 2200 Softswitch Host	Properties, Accounts, File Systems, States, Diagnostics.
Cisco BAMS	Properties, Accounts, File Systems, States, Diagnostics.
Csico HSI server	Properties, Accounts, File Systems, States, Diagnostics.
Cisco ITP-L	Properties, Accounts, States, Diagnostics.
Cisco LAN switch	Properties, Accounts, States, Diagnostics.
All components that have Properties dialog boxes	Properties: You can navigate from any Properties dialog box for the component to any other valid Properties dialog box for that component. **Note** The Navigation menu may display options that are not valid for the current component. Service invocation fails if you select an invalid properties dialog box.

Setting Up Cisco MNM Security

Revised: December 15, 2009, OL-18339-03

This chapter is designed for system administrators. It provides an overview of Cisco Media Gateway Controller (MGC) Node Manager (MNM) security capabilities and describes the following:

- Setting Up Security, page 4-5
- Modifying Security Settings, page 4-10

Note This chapter describes managing security as it applies to users of Cisco MNM; it does not cover the use of SSH or the Security Policy attribute in communicating with managed components. For information on installing SSH, see the *Cisco Media Gateway Controller Node Manager Installation Guide* at: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/prod_installation_guides_list.html. Information on using SSH-enabled functions is covered under the relevant functions in this guide. To define a component's security policy at deployment, see Chapter 5, "Deploying Your Network in Cisco MNM". To change the security policy of an existing component using the Accounts dialog box, see Chapter 8, "Other Network Management Tasks," "Viewing or Modifying Account and SNMP Information" section on page 8-6.

Overview of Cisco MNM Security

Cisco MNM provides user access control, which allows you as a system administrator to control the operations that different users can perform. Each user has a different login name and password and 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. Do not edit the administrator user except to change the password.

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

Within Cisco MNM, 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 resides. 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 in the following sections.

User Groups

Cisco MNM 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.

Cisco MNM applies access control based on user groups. The Cisco MNM administrator configures access control by assigning access specifications to the relevant user groups.

Feature Lists

All features 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. A feature may appear in more than one feature list. Permissions are:

- R—Read only. Available to all users. Useful for new users finding their way around the system.
- RW—Read-Write. Normal level, allowing the user to make modifications, such as acknowledging and clearing events or deploying the network. Operators typically have Read-Write access to the features they need for day-to-day tasks.
- RWA—Administrator. Administration level, allowing the user Read-Write access to all features at all times. This is available to administrators only.

Table 4-1 describes feature lists available in Cisco MNM.

Table 4-1   Feature Lists in Cisco MNM

Feature List	Permissions[1]	Description
AccessManagement	RWA	Set up users, user groups, assign passwords, and define access parameters.
AutoDiscovery	RW	Launch the auto-discovery services.
Change Password	RWA	Change passwords.
Deployment	RW	Deploy sites, regions, and networks (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	Clear and acknowledge events.
GenericConfigApplication	RWA	Launch the object configuration utility.
Help	R	Launch online help.
Host-Dialplan-Properties	R	View properties of Cisco PGW 2200 Softswitch host dial plan components.
Host-Signaling-Performance	RW	View performance statistics for signaling components.
Host-Signaling-Properties	R	View properties of Cisco PGW 2200 Softswitch host signaling components.
Host-Trunking-Properties	R	View properties of Cisco PGW 2200 Softswitch host trunking components.

Table 4-1   Feature Lists in Cisco MNM (continued)

Feature List	Permissions[1]	Description
Launchpad	R	Use the CEMF LaunchPad (start a CEMF session).
MGC-Node-Accounts	RWA	Change passwords, login IDs, and SNMP community strings.
MGC-Node-Admins	RWA	Use the Cisco MNM Administration Tool to start, stop, or reboot a device.
MGC-Node-Diagnostics	RW	Run diagnostic tools on Cisco PGW 2200 Softswitch node components.
MGC-Node-Filesystems	RW	View file system information on BAMS, HSI server, and Cisco PGW 2200 Softswitch host devices.
MGC-Node-Properties	R	View properties of Cisco PGW 2200 Softswitch node components.
MGC-Node-Provisioning	RWA	Deploy all Cisco PGW 2200 Softswitch node components (either manually or through a seed file).
MGC-Node-States	RW	Change the states of Cisco PGW 2200 Softswitch node components.
MGC-Node-Tools	RW	Launch Cisco PGW 2200 Softswitch node component tools.
MGC-Node-Transfer	RW	Configure performance.
MGC-Node-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	Define and edit thresholds.
ThresholderViewFeatureList	R	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 which features are appropriate for various types of users. For more information, see the "Setting Up Security for Typical User Roles" section on page 4-10.

Note   In Cisco MNM, features are preassigned to feature lists and cannot be modified.

Access Specifications

Access specifications define the features that can be invoked by a group of users and the objects upon which these features can be invoked.

Cisco MNM provides a number of access specifications. As a system administrator, you can create additional access specifications tailored to your needs.

Each access specification can include the following components:

- Feature lists—Lists the Cisco MNM features in the access specification. A feature list can appear in more than one access specification. Cisco MNM feature lists are shown in Table 4-1.

- User groups—Cisco MNM user accounts can be collected by an administrator into groups that correspond to user roles at your site. By associating user groups with access specifications, you can apply access control.

- A permission level—For example, read-only, read-write (view and modify information), and read-write-administrator (read and write all functions at all times).

- An optional object group—Where an object group is supplied, users have access to the features included in 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. You might use this option to grant the administrative user group for a site read-write access to the objects on that site, while another access specification would be used for read-only access for non administrative users.

Table 4-2 lists access specifications predefined in Cisco MNM.

Table 4-2   Predefined Access Specifications in Cisco MNM

Access Specification	Permissions	Feature Lists Included
Full_User_Access_Control	RWA	AccessManagement
Generic_Config_Application	RWA	GenericConfigApplication
Deployment	RWA	Deployment
AutoDiscovery	RWA	AutoDiscovery
Full_Event_Browser_Access	RWA	EventsView
		EventsClear_Acknowledge
EventManagerAccessSpec	RWA	ThresholderEditFeatureList
		ThresholderViewFeatureList
		NotificationEditFeatureList
		NotificationViewFeatureList
		EventGroupEditFeatureList
		EventGroupViewFeatureList
MGCHostServices	R	HostSignalingProperties
		HostDialplanProperties
		HostTrunkingProperties
		HostSignalingPerformance
Launchpad	RWA	Launchpad
MGCNodeServices	RWA	MGCNodeProvisioning
		MGCNodeTrapForwarding
		MGCNodeStates
		MGCNodeAdmin

Table 4-2   Predefined Access Specifications in Cisco MNM (continued)

Access Specification	Permissions	Feature Lists Included
		MGCNodeAccounts
		MGCNodeFilesystems
		MGCNodeProperties
		MGCNodeTransfer
		MGCNodeDiagnostics
		MGCNodeTools
Full_Object_Group_Access	RWA	ObjectGroupsView
		ObjectGroupsEdit
Full_Viewer_Access	RWA	ViewerEdit
		ViewerView
PerformanceManager	RWA	PerformanceManager
All_Standard_Features	RWA	Launchpad
		ChangePassword
		AccessManagement
		GenericConfigApplication
		EventsView
		EventsClear_Acknowledge
		FilterEditor
		ObjectGroupsEdit
		ObjectGroupsView
		ViewerEdit
		ViewerView
		Help
		Deployment
		AutoDiscovery
		PerformanceManager
		ThresholderEditFeatureList
		ThresholderViewFeatureList
		NotificationEditFeatureList
		NotificationViewFeatureList
		EventGroupEditFeatureList
		EventGroupViewFeatureList

Setting Up Security

To set up security, define the following:

- User accounts—Assign login IDs and passwords to individuals and optionally place them in user groups.

- User groups—Assign access specifications to a named group and assign users to user groups.

You can add new access specifications to define new groupings of features tailored to specific user roles in your system.

These tasks may be done in any order. They are interrelated—user groups have associated access specifications and users, and access specifications are linked to user groups. Before beginning, think through the types of users working with your system and the kinds of tasks they need to perform. Use this to plan user groups and access specifications on paper before you create user accounts, user groups, and access specifications. For examples, see the "Setting Up Security for Typical User Roles" section on page 4-10.

Setting Up New Accounts

You must set up new accounts for all users. Use the following procedure to create a new account for a user and assign a password:

Step 1 Click the **Access** icon on the Cisco EMF LaunchPad.

The Access Manager window opens.

Step 2 Choose **Edit > Create > User**.

The Create User window opens.

Step 3 Enter the login information for the new user. The login name must contain 5 to 32 characters; only alphanumeric characters and underscores are valid, and the first character must be a letter. Click **Forward**.

The Copy From Existing User window opens. If user groups have been defined and one or more user is already assigned to a group, "Copy from existing user" copies the user group assignment of the selected user.

Step 4 If you do not want to copy the assignment of an existing user or none exists, click **No**, and then click **Forward**.

To automatically place this user in the same user group as another user, click **Yes**. The list of users displays.

Step 5 Select the user whose assignment you want to copy, and click **Forward**.

The Select User Groups window opens.

Step 6 Select a user group, click the right arrow to move the group to the Selected User Groups list, and click **Forward**.

If no user groups are defined, click **Forward**. 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 a User Group" section on page 4-7.

The User Password Entry window opens.

Step 7 Enter a password for the user and confirm it.

The Summary Details for User window opens.

Note Passwords must contain 8 to 32 alphanumeric characters and at least one punctuation character such as _, %, (, or ^. Click **Forward**.

Step 8   If you are satisfied with the user definition, click **Finish**. If not, click **Back** to make modifications.

When you click **Finish**, the user is added and the Access Manager window closes. You are returned to the Launchpad window.

Creating a User Group

Use the following procedure to define an access privilege user group to which you can assign users:

Step 1   Click the **Access** icon on the Cisco EMF Launchpad.

The Access Manager window opens.

Step 2   Choose **Edit > Create > User Group**.

The Create User Group window opens.

Step 3   Enter the name for the new group.

The Copy From Existing User Group window opens. If user groups have been defined and one or more user is already assigned to a group, "Copy from existing user group" copies the access specifications and user membership of the selected group. Use this to base a group on an existing group, and then click the **Modify > User Groups** menu option to add or remove access specifications or users.

Step 4   If you do not want to copy an existing user or none exists, click **No**, and then click **Forward**.

If you want to base this user group on another, click **Yes**. The list of groups displays. Select the group you want to copy, and then click **Forward**.

The Select Users window opens listing existing users.

Step 5   Select each user you want in the new group, and then click the right arrow to move the user to the Selected Users list. Press Ctrl-click to select multiple users. When you are finished, click **Forward**.

The Select Access Specifications window opens, listing available access specifications. See Table 4-2 for the list of predefined Cisco MNM access specifications.

Step 6   Select each desired access specification, and then click the right arrow to move the specification to the Selected Access Specs list. Press Ctrl-click to select multiple specifications. When you are finished, click **Forward**.

The Summary Details for User Group window opens listing the user group name, members, and selected access specifications.

For details on access specifications, see the "Creating a New Access Specification" section on page 4-8.

✎
Note   Giving a user group Full User Access Control allows each user in the user group to add or delete other users to or from the group and to change specifications for all other users.

Step 7   If you are satisfied with the user group definition, click **Finish**. If not, click **Back** to make modifications.

When you click **Finish**, the user group is added and the Access Manager closes. You are returned to the Launchpad window.

Creating a New Access Specification

Use the following procedure to create a new access specification:

Step 1   Click the **Access** icon on the Cisco EMF Launchpad.

The Access Manager window opens.

Step 2   Choose **Edit > Create > Access Spec**.

The Create Access Specification window appears.

Step 3   Enter the name for the new specification.

The Copy From Existing Access Spec window appears. "Copy from existing access spec" copies the access specification and its user group assignments, if any. Use this to base a specification on an existing specification, and then click the **Modify > Access Specs** menu option to add or remove feature lists or user groups. See Table 4-2 for a list of predefined access specifications.

Step 4   If you want to base this specification on another, click **Yes**. The list of specifications displays. Select the one you want to copy, and then click **Forward**. Skip to Step 9.

If you do not want to copy an existing access specification, click **No,** and click **Forward**. The Select Permission window opens. Continue to Step 5.

Step 5   Select the permission for the new specification:

Read Only (basic level)—Information can be viewed only.

Read-Write (normal level)—Information can be viewed or modified.

Read-Write-Admin (administration level)—Read-Write access to all features at all times. This is available to administrators only.

Click **Forward**.

The Select User Groups window opens listing user groups to which you can assign this specification.

Step 6   Select each user group you want to assign the new specification, and click the right arrow to move it to the Selected User Groups list. Press Ctrl-click to select multiple groups. When you are finished, click **Forward**.

The Select Feature Lists window opens displaying the available feature lists. See Table 4-1.

Step 7   Select each feature you want to include in the specification, and click the right arrow to move the group to the Selected Features list. Press Ctrl-click to select multiple features. When you are finished, click **Forward**.

The Select Object Groups window opens. Each access specification can have one associated object group to limit this specification to a particular type of object.

Step 8   Select the object group, if any, that you want to associate with this access specification, and click **Finish**.

> **Note**   If you do not select a group, the specification is not restricted to a specific object group.

Step 9   The Summary Details for Access Specifications window opens, summarizing the new specification, including:

- The access specification name
- Permissions
- Feature lists included

- The object group associated with the specification
- User groups to which the specification is assigned

If you are satisfied with the new access specification, click **Finish**. If not, click **Back** to make modifications.

When you click **Finish**, the access specification is added to the specification list and the Access Manager closes. You are returned to the Launchpad window.

Setting Up Security for Typical User Roles

Table 4-3 summarizes how to set up security for typical user roles.

Table 4-3   Security for Typical Roles

For This Role	Perform These Steps
Administrator	Use the instructions in the "Setting Up New Accounts" section on page 4-6 to create a new user by copying the existing administrator template. The administrator should have all the features labeled with the permissions R, RW, and RWA in Table 4-1.
Normal user (read permission and ability to deploy and launch tools, but not to use configuration management)	Using the instructions in the "Creating a New Access Specification" section on page 4-8, create a new access specification with the features labeled with the permissions R and RW in Table 4-1, but not including: • AutoDiscovery • ObjectGroups-Edit • ObjectGroups-View Use the instructions in the "Creating a User Group" section on page 4-7 to create a new user group with the access specification you just created. Use the instructions in the "Setting Up New Accounts" section on page 4-6 to create a new account and user, and assign the user to the group you just created.
Novice user or user who only needs to view information	Using the instructions in the "Creating a New Access Specification" section on page 4-8, create a new access specification with the features labeled with the permission R in Table 4-1. Using the instructions in the "Creating a User Group" section on page 4-7, create a new user group with the access specification you just created. Using the instructions in the "Setting Up New Accounts" section on page 4-6, create a new account and user, and assign the user to the group you just created.

Modifying Security Settings

You can do the following using the Access Manager:

- Modify a user account to change the user login, name, or user group membership.

- Modify a user group or access specification:

    - To complete the definition of a new user group or access specification created by copying an existing one.

    - To change properties of an existing group or specification.

- Delete users, user groups, and access specifications.
- Change the administrative password.
- Change user passwords.

Details are provided in the following sections.

Modifying a User Account

Use the following procedure to modify a user login, name, or user group membership:

Step 1   Click the **Access** icon on the Cisco EMF Launchpad.

The Access Manager window opens.

Step 2   Do one of the following:

- Choose **Edit > Modify > User**.
- If the user list is not selected, choose **Users** from the drop-down list. Double-click the user account you want to modify.

The User Editor window opens. In the left, the window includes a list of users. In the right pane, it includes the tabs User Details and Select User Groups. The description pane at the bottom of the window provides details on the current selection.

Figure 4-1   User Editor Window
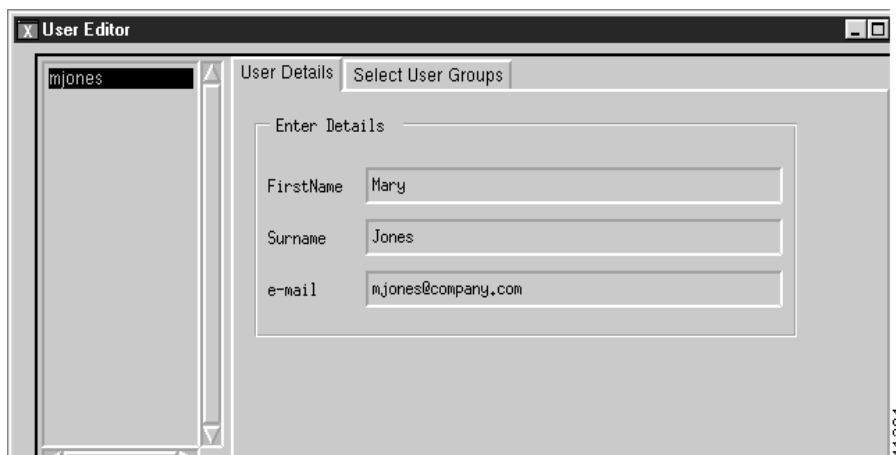
Step 3   Select a user from the list.

Step 4   Make the desired modifications.

Step 5   Click **Apply**. To cancel the changes, click **Revert**.

Step 6   When you are done, click **Close**. You are returned to the Launchpad window.

Modifying User Groups or Access Specifications

Use the following procedure to modify a user group or access specification:

Step 1   Click the **Access** icon on the Cisco EMF Launchpad.

The Access Manager window opens.

Step 2   Do one of the following:

- Choose **Edit > Modify > User Group** or **Access Spec**.
- From the drop-down list, choose **User Groups** or **Access Specifications** to display a list of groups or specifications. Double-click the object you want to modify.

Step 3   The Editor window opens. The left pane includes a list of existing objects, user groups, or access specifications. The right pane includes a tab for each of the windows you used when you created the group or specification. The description pane at the bottom of the window provides details on the current selection. Figure 4-2 shows an example.

Figure 4-2   Access Specification Editor Window

Step 4   Click the object you want to modify.

Step 5   Make the desired modifications.

Step 6   Click **Apply**. To cancel the changes, click **Revert**.

Step 7   When you are done, click **Close**. You are returned to the Launchpad window.

Deleting a User, User Group, or Access Specification

Use the following procedure to delete a user, user group, or access specification:

Step 1   Click the **Access** icon on the Cisco EMF LaunchPad.

The Access Manager window opens.

Step 2   In the drop-down list, choose the users, groups, or specifications you want to delete. Use Ctrl-click for multiple selections.

Step 3   Choose **Edit > Delete**. You are prompted for confirmation.

Step 4   Click **Yes**.

The selections are deleted from the list.

Changing the Administrative Password

Use the following procedure to change the administrative password:

Step 1   Click the **Access** icon on the Cisco EMF Launchpad.

The Access Manager window opens.

Step 2   Choose **Edit > Change Admin Password**.

Step 3   Change the password, and click **OK**.

Changing a User's Password

Use the following procedure to change a user's password:

Step 1   Click the **Access** icon on the Cisco EMF Launchpad.

The Access Manager window opens.

Step 2   Choose **Edit > Change Password**.

Step 3   Change the password, and click **OK**.

CHAPTER **5**

Deploying Your Network in Cisco MNM

Revised: December 15, 2009, OL-18339-03

This chapter provides information about deployment in the following sections:

Note For information on troubleshooting deployment errors, see Appendix C, "Troubleshooting Cisco MNM."

Overview of Deployment

Cisco MNM uses the term *deployment* to refer to the addition of objects to the network model. For Cisco MNM to be able to manage your network, the Cisco PGW 2200 Softswitch node and its devices must first be deployed. When the device is deployed, an object for each device is created automatically. This created object represents a real object in the network and is accessible under the Physical and device-specific views in the Map Viewer.

Note
- The other task in setting up the management of your network is configuration of the managed devices so that they forward alarms to Cisco MNM. Typically, this is done by the system administrator. Deployment tells Cisco MNM how to communicate with the managed devices; configuration tells the devices how to communicate with Cisco MNM. See Chapter 2, "Configuring Network Devices for Management" for details.
- Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, ITP-L will replace SLT in publications and the product.

Deploy an object by giving Cisco MNM the basic information needed to manage the device, such as the IP address and login ID and password. If you are using SSH in your managed network and have installed SSH for Cisco MNM, also specify the security policy of components that can be SSH-enabled:

- Cisco PGW 2200 Softswitch host
- Cisco BAMS
- Cisco HSI server
- Cisco ITP-L
- Cisco Integrated ITP-L
- Cisco Catalyst 5500 and 6509 LAN switches

You can deploy a Cisco PGW 2200 Softswitch node and its devices in two ways:

- Manually, using a deployment template to fill in details for each device individually
- With a seed file, specifying deployment information for a group of devices in an external seed file that is read by Cisco MNM

After you deploy a device, whether manually or with a seed file, Cisco MNM contacts the device and discovers information about its configuration. For example, when a Cisco ITP-L is deployed, Cisco MNM discovers any TDM (DS1) interfaces. When a Cisco LAN Switch is deployed, Cisco MNM discovers ports and modules. When the Cisco PGW 2200 Softswitch host is deployed, Cisco MNM discovers the system components as well as signaling and trunking components.

Note Dial plan components on Cisco PGW 2200 Softswitch are no longer supported on Cisco MNM 2.8(1).

Carry out the deployment for the entire Cisco PGW 2200 Softswitch node or farm when you first set up Cisco MNM. Later, deploy a new device to the network on a device-by-device basis. To keep the Cisco MNM model synchronized with changes in device configurations, define a frequency for auto-rediscovery or manually rediscover device components after making changes. The default frequency for rediscovery is 6 hours.

You can also save a copy of your deployed network model as a seed file to use when adding new devices to the network. The seed file can be modified with a text editor to copy or add new device addresses and passwords, and export the network information in an inventory file. For more information, see the "Exporting Deployment Information to an Inventory or Seed File" section on page 5-22.

Information Needed for Deployment

Whether you are deploying components with a seed file or manually, Cisco MNM needs the same information about the network. Table 5-1 summarizes the information needed. The first column shows the attribute name in the seed file, and the second column shows the field name in the Deployment template.

Table 5-1   Deployment Information

Attribute in Seed File	Attribute in Deployment Template	Applicable Device Types	Description	Seed File Default	Required?
name	Name	All.	A name for the object in Cisco MNM. The name must be unique in the network.	None for Cisco PGW 2200 Soft switch node, HSI server, and BAMS. For node devices: Device type-IP address (for example, Host–10.10.10.0 for a Cisco PGW 2200 Soft switch host).	In manual deployment: Yes for all. In seed file deployment: Yes for Cisco PGW 2200 Softswitch node, HSI server, and BAMS. No for node devices (host, Cisco ITP-L, LAN Switch; default will be used).
ip	IP Address	All except the Cisco PGW 2200 Softswitch node or farm.	IP Address of the network element.	None.	Yes.
read	Read Community	All except Cisco PGW 2200 Softswitch node or farm.	SNMP read-community string.	Public.	In manual deployment: Yes. In seed file deployment, enter this in the file or in the dialog box.

Table 5-1   Deployment Information (continued)

Attribute in Seed File	Attribute in Deployment Template	Applicable Device Types	Description	Seed File Default	Required?
write	Write Community	All except Cisco PGW 2200 Softswitch node or farm.	SNMP write-community string.	Private.	In manual deployment: Yes. In seed file deployment, enter this in the file or in the dialog box.
location	View - Object Relationship	All except farm.	A name for the physical site, used in Cisco MNM to organize objects in the Physical view. The same name should be used for all devices to be grouped in a given Physical view.	Default. **Note** If you omit the name from some devices, devices are placed in two different physical sites; one with the default name and one with the name you supply.	In manual deployment: Yes. In seed file deployment: No (default will be used).
security policy	Security Policy	All except Cisco PGW 2200 Softswitch node and farm, specific devices at end of life that do not support SSH (standalone ITP-L, Catalyst 2900 XL).	The security policy used on the device, either none or SSH. With SSH selected, Cisco MNM determines the correct SSH version for communication with the device.	None.	In manual deployment: Yes. In seed file deployment: No (default will be used).

In seed file deployment, for security reasons the next four attributes should be entered in the Deploy Network dialog box when you deploy the seed file rather than being included in the file.

Table 5-1   Deployment Information (continued)

Attribute in Seed File	Attribute in Deployment Template	Applicable Device Types	Description	Seed File Default	Required?
login	Login	All except Cisco PGW 2200 Softswitch node or farm.	Login ID for the device software. For the Cisco PGW 2200 Softswitch host, for example, this is the login used. (If user id is not configured in the device, leave this field blank).	In seed file— Cisco PGW 2200 Soft switch host: mgcusr. Cisco BAMS: acec. Cisco HSI server: cisco.	Yes.
password	Password	All except Cisco PGW 2200 Softswitch node or farm.	Password to log in to the device software.	None.	Yes.
root	Root Password	Cisco PGW 2200 Softswitch host, BAMS, and HSI server.	Root (super-user) password for the device software.	None.	Yes.
enable	Enable Password	Cisco ITP-L and Cisco LAN Switch.	ITP-L and Catalyst software enable password.	None.	Yes.

Deployment Rules

Cisco PGW 2200 Softswitch Hosts

You can define a maximum of two hosts per Cisco PGW 2200 Softswitch node: the active and standby Cisco PGW 2200 Softswitch hosts. You do not have to specify which host is active or standby; it is determined automatically by Cisco MNM. You must specify the name for each Cisco PGW 2200 Softswitch node.

⚠ **Caution** Although Cisco MNM does not prevent you from deploying more than two hosts per node, the system is not designed to support this configuration.

Cisco PGW 2200 Softswitch Farms

You can define one or more Cisco PGW 2200 Softswitch nodes under a Cisco PGW 2200 Softswitch farm.

Physical Locations and Deployment

When a device is deployed, it is placed into the Physical containment tree for its location. For example, all devices with location=Chicago are placed under a site object named Chicago. If the specified location does not exist, Cisco MNM automatically deploys a site object with the specified location name. If you do not specify a physical location for a device, it is deployed in the same location as its logical parent. If no location is specified for the parent, the objects are deployed to a site called Default.

Cisco PGW 2200 Softswitch node objects and farm objects are not physical devices and, as such, are not deployed into the Physical containment tree. You can specify a location for the Cisco PGW 2200 Softswitch node or farm, however, so that children of the node can, by default, be placed in the specified location. For example, if you specify that a Cisco PGW 2200 Softswitch node is in the site Cincinnati, all of its children that do not specify a location are, by default, placed in the Cincinnati site.

Seed File Deployment

A *seed file* is a text file containing the names and IP addresses of all the devices in the Cisco PGW 2200 Softswitch network, together with the relationship (hierarchy) between the devices. For bulk deployment, use a seed file to deploy an entire Cisco PGW 2200 Softswitch network consisting of one or more Cisco PGW 2200 Softswitch nodes or farms. Using this file, Cisco MNM automatically deploys all the elements in the network.

Note A seed file requires the name and IP address for each device to be deployed, and it can optionally contain the userid and password necessary to log in to the device.

To perform seed file deployment, launch a dialog from an MGC-Node-View node or other type of object in the Map Viewer. This dialog prompts you for the name of the seed file and, if not specified in the seed file, for the login ID and password for each device type. You also specify SNMP read- and write-community strings for the Cisco ITP-L and Cisco LAN Switch.

Note A sample seed file is located at *<CEMF Root>*/samples/seedfile.txt and in Example 5-1.

Seed File Example and Syntax

Sample seed files are shown in Example 5-1 (seed file for Cisco PGW 2200 Softswitch node) and Example 5-2 (seed file for Cisco PGW 2200 Softswitch farm).

The examples are followed by an explanation of the required syntax. You can also view a sample seed file at *<CEMF Root>*/samples/seedfile.txt.

Note By default, Cisco MNM looks for the seed file in the *<CEMF_ROOT>/bin/*.mgcController sysmgr folder. If you place the file elsewhere, note the location. The location needs to be specified in the Deploy Network dialog box.

Seed File Examples

Example 5-1   Sample Seed File for Cisco PGW 2200 Softswitch Node

```
# Sample MGC Network Seed File

MGC (name = mgc-node-1) {
    HOST (name = mgc-host-1, location = Site-1,  ip = 10.1.1.1, securitypolicy = none)
    HOST (name = mgc-host-2, location = Site-1,  ip = 10.1.2.1, securitypolicy = none)
    2600 (name = slt-1,  location = Site-1, ip = 10.1.1.2, securitypolicy = none)
    2600 (name = slt-2,  location = Site-1, ip = 10.1.2.2, securitypolicy = none)
}
2900xl (name = lanswitch-1,  location = Site-1, ip = 10.1.1.3, securitypolicy = none)
5500 (name = lanswitch-2,  location = Site-1, ip = 10.1.2.3, securitypolicy = none)
MGC (name = mgc-node-2) {
    HOST (name = mgc-host-3,   location = Site-1, ip = 10.1.3.1)
    HOST (name = mgc-host-4,   location = Site-1, ip = 10.1.4.1)
    INTEGRATED_SLT (name = slt-3,  location = Site-1, ip = 10.1.1.3, securitypolicy = ssh)
    INTEGRATED_SLT_CORESIDENT (name = slt-4,  location = Site-1, ip = 10.1.2.4,
securitypolicy = SSH)
}
6509 (name = lanswitch-5,  location = Site-1, ip = 10.1.4.3, securitypolicy = ssh)
BAMS (name = bams-1, location = Site-1, ip = 10.10.3.1, securitypolicy = ssh)
HSI (name = gwing-1, location = Site-1, ip = 10.10.3.2, securitypolicy = ssh)
```

Example 5-2   Sample Seed File for Cisco PGW 2200 Softswitch Farm

```
# Sample MGC Seed File including a Farm

BAMS (name = bams-mast, location = bams-mast, ip = 10.18.126.102, securitypolicy = none)
FARM (name=MGCFarm-1)
 {
  MGC (name=MGC-vsc9)
   {
     HOST (name = nssuvsc9, location = nssuvsc9, ip = 10.18.126.59, securitypolicy = none)

   }

 }
BAMS (name = bams-sla, location = bams-sla, ip = 10.18.126.103, securitypolicy = none)
HSI (name = HSI-218, location = HSI-218, ip = 10.18.126.218, securitypolicy = none)
5500 (name = 5509, location = 5509, ip = 10.18.126.5, securitypolicy = none)
MGC (name=MGC-slt)
 {
  2600 (name = slt-b, location = slt-b, ip = 10.18.126.10, securitypolicy = none)
```

Seed File Syntax

The specifications for each Cisco PGW 2200 Softswitch host, Cisco ITP-L, Cisco Integrated ITP-L, and LAN switch are grouped under the relevant Cisco PGW 2200 Softswitch node.

For a Cisco PGW 2200 Softswitch farm, the specifications for each Cisco PGW 2200 Softswitch node in the farm are grouped under the farm specification. The specifications for each Cisco PGW 2200 Softswitch host are grouped under the appropriate node.

> **Note**   A node associated with a farm includes Cisco PGW 2200 Softswitch hosts only.

The specification for each Cisco BAMS or Cisco HSI server must be specified on its own line. The Cisco MNM then determines the node with which the Cisco HSI server or Cisco BAMS is associated at deployment.

For each Cisco PGW 2200 Softswitch node:

```
MGC (name=mgcnodename, location=Physical site) {Values for Cisco MGC node devices}
```

For each Cisco PGW 2200 Softswitch farm:

```
FARM (name=mgcfarmname, location=Physical site) {Values for Cisco MGC node and host}
```

Enclosed in braces under a node, the values for Cisco PGW 2200 Softswitch node devices:

- For each Cisco PGW 2200 Softswitch host:

```
HOST ([name=Cisco MGC host name,] ip=IP address, [read=public,] [write=private,]
[location=Physical site,] [securitypolicy=Securitypolicy])
```

- For each Cisco ITP-L:

```
2600 ([name=Cisco SLT name,] ip=IP address, [read=public,] [write=private,]
[location=Physical site,] [securitypolicy=Securitypolicy])
```

- For each Cisco INTEGRATED ITP-L:

```
INTEGRATED_SLT ([name=Cisco SLT name,] ip=IP address, [read=public,]
[write=private,] [location=Physical site,] [securitypolicy=Securitypolicy])
```

- For each co-resident Cisco INTEGRATED ITP-L:

```
INTEGRATED_SLT_CORESIDENT([name=Cisco SLT name,] ip=IP address, [read=public,]
[write=private,] [location=Physical site,] [securitypolicy=Securitypolicy])
```

- For each Cisco 2900XL LAN Switch, on its own line:

```
2900XL ([name=Cisco LAN Switch name,] ip=IP address, [read=public,]
[write=private,] [location=Physical site,] [securitypolicy=Securitypolicy])
```

- For each Cisco 5500XL LAN Switch, on its own line:

```
5500 (ip=IP address, [name=Cisco LAN Switch name,] [read=public,] [write=private,]
[location=Physical site,] [securitypolicy=Securitypolicy])
```

- For each Cisco 6509XL LAN Switch, on its own line:

```
6509 (ip=IP address, [name=Cisco LAN Switch name,] [read=public,] [write=private,]
[location=Physical site,] [securitypolicy=Securitypolicy])
```

- For each Cisco HSI server, on its own line:

```
HSI ([name=HSI host name,] ip=IP address, [location=Physical site,]
[securitypolicy=Securitypolicy])
```

- For each Cisco BAMS, on its own line:

```
BAMS ([name=BAMS name,] ip=IP address, [location=Physical site,]
[securitypolicy=Securitypolicy])
```

Note If the Cisco BAMS has been configured to collect call detail records (CDRs) for a Cisco PGW 2200 Softswitch host, the Cisco BAMS is deployed in the node containing that host. To appear in that node, it must be actively polling CDRs.

Deploying a Network Using a Seed File

Use the following procedure to deploy a network using a seed file:

Step 1   Create a seed file manually or generate a seed file with the Cisco VSPT. For seed file attributes, see Table 5-1. For seed file syntax, see the "Seed File Example and Syntax" section on page 5-6. Note the location of the seed file.

Step 2   From the Map Viewer screen, click the MGC-Node-View icon.

Step 3   Right-click, and choose **Deployment** > **Deploy Network Seed File**.

The Deploy Network window opens, as shown in Figure 5-1.

Figure 5-1   Deploy Network Window—Seed File Tab

Step 4   In the Filename field, enter the name of the seed file.

✎

Note   If the file is not in the default location, *<CEMF Root>*/bin/.mgcControllerx.sysmgr, include the path.

Step 5   Enter the software login information for each type of device.

Step 6   (Optional) To enter advanced information, such as SNMP configuration parameters, click the **Advanced** tab. Click the **Seed File** tab when you are done.

Step 7   Click **Deploy**. You are prompted to confirm the deployment.

Step 8   Click **Yes**.

The system displays the message "The network has been successfully deployed," and Cisco MNM goes on to discover the device subcomponents. See the "About the Discovery Process" section on page 5-14 for details on what occurs during discovery.

> **Note**   If you receive an error message, see Table C-2 in Appendix C, "Troubleshooting Cisco MNM."

Manual Deployment

Cisco MNM defines a number of templates that allow you to manually configure Cisco PGW 2200 Softswitch nodes and other objects including:

- Cisco PGW 2200 Softswitch node
- Cisco PGW 2200 Softswitch host or host pair as a child of the Cisco PGW 2200 Softswitch node
- Top-level BAMS
- HSI server
- Cisco ITP-L as a child of a Cisco PGW 2200 Softswitch node
- Cisco LAN switch
- Cisco PGW 2200 Softswitch farm
- Cisco PGW 2200 Softswitch node or multiple nodes as children of the Cisco PGW 2200 Softswitch farm

The Deployment Wizard reads the templates and presents screens prompting you for information about the devices.

Overview of Steps to Deploy a Cisco PGW 2200 Softswitch Node Manually

Task 1. If one does not already exist, deploy a physical site as the container for the node.

Task 2. Deploy a Cisco PGW 2200 Softswitch node object.

Task 3. Deploy each of the devices that the node contains (Cisco PGW 2200 Softswitch host, ITP-L, LAN Switch).

Task 4. If applicable, deploy the BAMS.

Task 5. If applicable, deploy the HSI server.

> **Note**   Only one deployment wizard per user can be open at any time. If you attempt to open a second wizard, a message advises you that the deployment wizard is already active. Complete the first deployment task before proceeding.

Overview of Steps to Deploy a Cisco PGW 2200 Softswitch Farm Manually

Task 1. If one does not already exist, deploy a physical site as the container for the node.

Task 2. Deploy a Cisco PGW 2200 Softswitch farm object.

Task 3. Deploy each of the Cisco PGW 2200 Softswitch nodes that the farm contains.

Task 4. For each node, deploy each of the devices that the node contains (Cisco PGW 2200 Softswitch host, ITP-L, LAN Switch).

Task 5. If applicable, deploy the BAMS.

Task 6. If applicable, deploy the HSI server.

> **Note** Only one deployment wizard per user can be open at any time. If you attempt to open a second wizard, a message advises you that the deployment wizard is already active. Complete the first deployment task before proceeding.

Deploying a Physical Site

Use the following procedure to deploy a physical site as the container for a Cisco PGW 2200 Softswitch node:

Step 1 Open the Map Viewer.

Step 2 In the left pane, right-click the **Physical** view icon.

Step 3 Choose **Deployment** > **Deploy Generic Objects**.

The Deployment Wizard Templates window opens showing a list of templates.

Step 4 Select **Site**, and click **Forward**.

The Object Parameters window opens.

Step 5 Specify the number of sites you are creating, or accept 1 as the default, and click **Forward**.

Step 6 Enter the name you want to use for the physical site (no spaces). Click **Forward**.

The Deployment Wizard Views window opens.

Step 7 Click **Select**.

Step 8 In the Object Selector window, select the Physical object, and click **Forward**.

A screen displays summarizing the deployment you have created.

> **Note** Although you can create a physical site as a child of an existing physical site, Cisco MNM does not support more than one site level in the seed files it exports or imports.

Step 9 Click **Finish**.

You are informed if the deployment was successful, and a physical site icon displays in the right pane of the Map Viewer window.

Step 10   Deploy the Cisco PGW 2200 Softswitch node object as described in the "Deploying a Cisco PGW 2200 Softswitch Node Object" section on page 5-12.

Deploying a Cisco PGW 2200 Softswitch Node Object

Use the following procedure to deploy a Cisco PGW 2200 Softswitch node object:

Step 1   Open the Map Viewer.

Step 2   In the left pane, right-click the **MGC-Node-View** icon.

Step 3   Choose **Deployment > Deploy MGC Node**.

The Deployment Template opens.

Step 4   Enter the name for the Cisco PGW 2200 Softswitch node (no spaces). Click **Forward**.

A screen displays summarizing the deployment you have created and allows you to commit or reject the deployment.

Step 5   Click **Finish**.

You are informed if the deployment was successful, and a Cisco PGW 2200 Softswitch node icon displays in the right pane of the Map Viewer window.

Step 6   Deploy the devices in the node as described in the "Deploying Network Devices" section on page 5-12.

Deploying Network Devices

Use the following procedure to deploy a Cisco PGW 2200 Softswitch host, ITP-L, LAN Switch, HSI server, or BAMS:

Step 1   Open the Map Viewer.

Step 2   In the left pane, expand the MGC-Node-View icon and click to select the desired Cisco PGW 2200 Softswitch node.

Note   Although you can alternatively begin deployment from the device-specific view, starting from the appropriate node avoids having to specify the node relationship in the deployment template.

Step 3   Right-click the **Cisco PGW 2200 Softswitch node** icon and choose **Deployment > Deploy MGC Node Component**.

The Deployment Wizard Templates window opens listing these template types:

- BAMS
- 2900XL Switch
- Catalyst 5500 Switch
- Catalyst 6509 Switch

Note   Although the Cisco Catalyst switches listed above can be deployed using the Deploy MGC Node
Component Wizard, when deployed they do not appear as children of the node.

- Cisco HSI Host
- Cisco PGW 2200 Softswitch Host
- Cisco PGW 2200 Softswitch Node
- Cisco ITP-L
- Integrated ITP-L
- Integrated ITP-L for Coresident EMs

Note   You cannot deploy an ITP-L or integrated ITP-L in a node that is under a farm object.

Step 4   Select the desired device type, and click **Forward**.

The Deployment Wizard Object Parameters window opens.

Step 5   Enter device data. See Table 5-1 on page 5-3 for descriptions of the fields.

Step 6   Click **Forward**.

The Deployment Wizard Views window opens.

Step 7   Click **Select**.

The Object Selector displays.

Step 8   Click the + (shown in Figure 5-2) to show the physical site(s) in the Physical View.

Figure 5-2   *Expanding the Physical Site View*
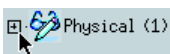
Step 9   Select the physical site for the current node, and click **Apply**.

Step 10   Click **Finish**.

An icon for the new device displays in the right pane of the Map Viewer. Cisco MNM begins discovering
the device, as shown by the crosshatching of the object icon, and the discovering status indicator attached
to it. Here is an example:

Figure 5-3   *Device in Discovering State*

For a Cisco PGW 2200 Softswitch host, ITP-L, or LAN Switch, the device icon also displays in the left
pane in the MGC-Node-View as a child of the current Cisco PGW 2200 Softswitch node. If the
Cisco BAMS is configured to send call detail records (CDRs) to the Cisco PGW 2200 Softswitch host,
and is actively polling CDRs, the BAMS icon also displays as a child of the node.

When discovery is complete, Cisco MNM sends a "Discovery is now complete" alarm that can be viewed
in the Event Manager.

See the "About the Discovery Process" section on page 5-14 for details on what occurs during discovery.

Note
- The icon for the new object also displays in the Physical View and the device-specific view for its device type.

- For information on troubleshooting deployment errors, see Appendix C, "Troubleshooting Cisco MNM," "Solving Deployment and Discovery Errors" section on page C-5.

About the Discovery Process

After you deploy a device, Cisco MNM contacts the device and discovers information about its configuration. For example, when you deploy a Cisco ITP-L, Cisco MNM discovers any Ethernet and TDM (DS1) interfaces and their IP addresses. When you deploy a Cisco LAN Switch, Cisco MNM discovers interfaces, ports, and modules. When you deploy the Cisco PGW 2200 Softswitch host, Cisco MNM discovers the system components, as well as signaling, trunking, and dial plan components. Figure 5-4 shows how the Cisco PGW 2200 Softswitch host appears in the Map Viewer after discovery.

Figure 5-4   Map Viewer Display of the Cisco PGW 2200 Softswitch Host After Discovery
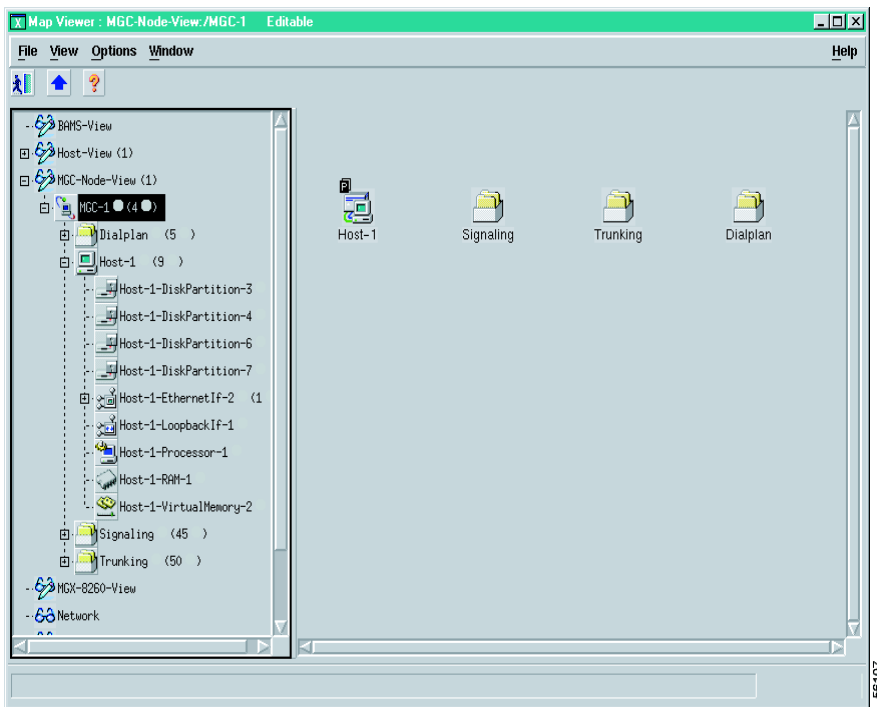
The various subcomponent discovery mechanisms are described in the following sections.

Note After initial deployment, Cisco MNM automatically rediscovers each device at a predefined interval and keeps track of the time that each device was last discovered. The default interval for automatic rediscovery is every 6 hours. When the specified interval has elapsed, Cisco MNM automatically rediscovers the device. See the "Synchronizing the Cisco MNM with Device Changes" section on page 5-20 for details.

Discovery of Cisco PGW 2200 Softswitch Host, Cisco HSI Server, and Cisco BAMS Components

The Cisco PGW 2200 Softswitch host, Cisco HSI server, and Cisco BAMS discovery mechanism processes the ifTable of the device and deploys an object to represent each supported interface. Cisco 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 5-5.

Figure 5-5   *Cisco PGW 2200 Softswitch Host, Cisco HSI Server, and Cisco BAMS Discovery*
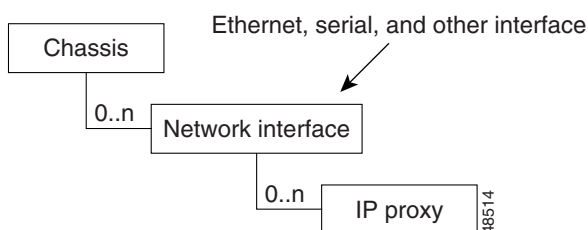
For a Cisco BAMS to be deployed into the correct node, you must perform the following actions:

- Configure the Cisco BAMS to collect CDRs for the relevant Cisco PGW 2200 Softswitch host residing in the same node.

  For the procedure of configuration, see the section, "Configuring the Cisco MGC for Using BAMS", of the *Cisco Billing and Measurements Server User's Guide* at
  http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/bams/3.30/guide/330_ug.html

- Configure the Cisco BAMS to actively poll CDRs from that Cisco PGW 2200 Softswitch host (set the "activate" flag to "1" in the Cisco BAMS to start the process).

  For more information on Cisco BAMS configuration, See the section, "Cisco BAMS Server Configuration", of the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* at
  http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/provisioning/guide/prvgde.html

  For more information on Cisco BAMS parameter definitions and values, see the *Cisco Billing and Measurements Server User's Guide* at
  http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/bams/3.30/guide/330_ug.html

- Add the following line to the /etc/inet/hosts file:

  <IP Address> <hostname>

  This action associates the IP address of the Cisco PGW 2200 Softswitch host with the Cisco PGW 2200 Softswitch host name.

  Then you can use the command **ping** *hostname* to see if the device is reachable.

When you deploy the configuration, the Cisco BAMS is then automatically placed in the node containing that host, which is dynamically updated. If the BAMS object does not appear in the node view immediately, rediscover the Cisco BAMS; Otherwise the Cisco MNM will do a rediscovery at a predefined interval. The default interval for an automatic rediscovery is six hours. If you deactivate polling, Cisco MNM removes the BAMS object from the node. When you reactivate polling, it restores the BAMS object to the node.

Note   For information on troubleshooting Cisco BAMS discovery problems, see Appendix C, "Troubleshooting Other Issues," "Troubleshooting Other Issues" section on page C-7.

Discovery of System Components

For the Cisco PGW 2200 Softswitch host, Cisco HSI server, and Cisco BAMS, system components are deployed that represent logical components of the UNIX system, as shown in Table 5-2.

.

Table 5-2   *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)

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 Cisco MNM 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 rather than 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 a child of its corresponding VLAN. In order to correlate interfaces from the ifTable to their corresponding VLANS in the vtpVLanTable, Cisco MNM uses the description of the ifTable entry, which is of the form:

VLANx

Where x is the index of the corresponding entry in the vtpVlanTable.

The Cisco 2900XL subrack component displays, as shown in Figure 5-6.

Figure 5-6   Cisco 2900XL Chassis Discovery
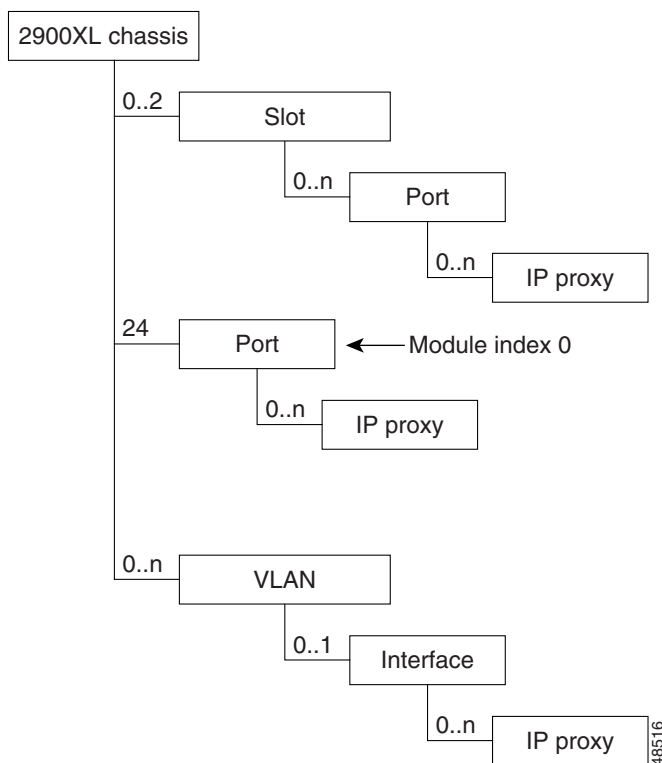
Discovery of Cisco Catalyst 2900XL Components

Cisco MNM models slots, VLANs, and ports on Cisco Catalyst 2900XL series devices. During auto discovery, Cisco MNM retrieves the tables shown in Table 5-3.

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

Table 5-3   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 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 Cisco MNM 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 rather than 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 a child of its corresponding VLAN. In order to correlate interfaces from the ifTable to their corresponding VLANS in the vtpVLanTable, Cisco MNM 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 displays, as shown in Figure 5-7.

Figure 5-7   *Cisco 2900XL Chassis Discovery*
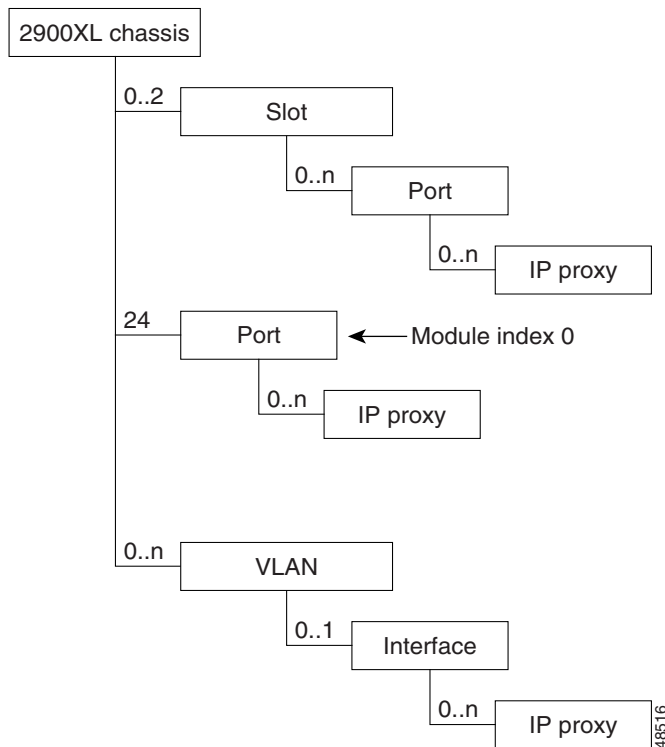
Discovery of Cisco Catalyst 5500 and 6509 Components

Cisco MNM models slots, VLANs, and ports on Cisco Catalyst 5500 and 6509 (similar to 5500) series devices. During auto discovery, Cisco MNM retrieves the tables shown in Table 5-4.

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.

Table 5-4   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 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 5-8.

Figure 5-8   Catalyst 5500 Chassis Discovery
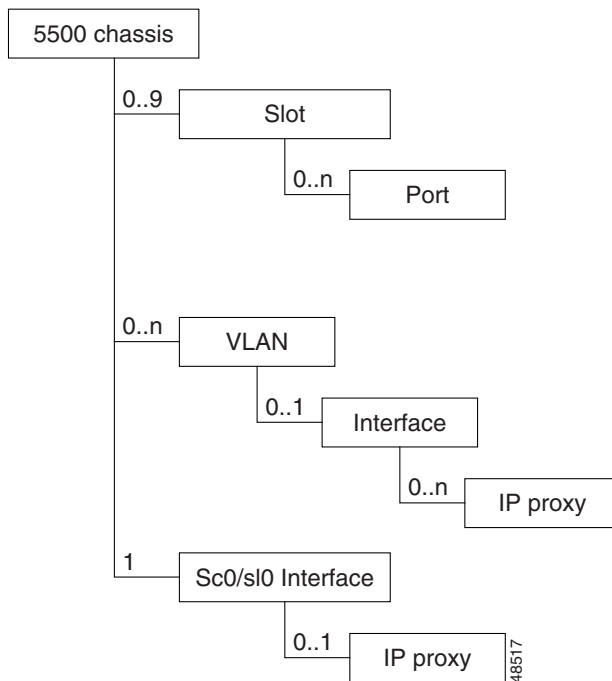
Keeping the Cisco MNM Network Model Up to Date

Through periodic rediscovery of the components of each deployed device, Cisco MNM ensures that its database and the Cisco MNM network model are synchronized with the underlying network elements. The default interval at which automatic rediscovery occurs is every 6 hours, but you can change the interval, and you can manually invoke rediscovery when needed. These tasks are described in the "Synchronizing the Cisco MNM with Device Changes" section on page 5-20.

If basic account information about a device (such as its password) changes, you can modify the information in the device Accounts dialog box. If the device is no longer in the network, you can delete it. This is described in the "Modifying or Deleting Deployed Objects" section on page 5-21

SNMP Traps for Configuration Changes

All relevant management data in the Cisco MNM database is automatically updated on receipt of a modification trap from the various network elements in the Cisco PGW 2200 Softswitch node.

The traps in Table 5-5 are used to signal changes in the network elements.

Table 5-5   Network Element Configuration Traps

Network Element	Configuration Changed Trap
Cisco PGW 2200 Softswitch host	POM: DynamicReconfiguration
LAN switch	coldStart, warmStart, configChange
Cisco ITP-L	reload, configChange

When Cisco MNM receives a **POM:DynamicReconfiguration** trap from the active Cisco PGW 2200 Softswitch host, it resynchronizes its view of the connectivity network with that of the device.

Synchronizing the Cisco MNM with Device Changes

You can change the interval at which Cisco MNM checks deployed devices for any changes to their components. You can also rediscover a device immediately when needed.

Auto-discovery frequency applies to all devices of the same type.

For SSH-enabled components (defined as the Security Policy at deployment or in the Accounts dialog box), Discovery uses SSH.

To Change the Automatic Rediscovery Interval

Use the following procedure to change the frequency of automatic rediscovery for a particular device type:

Step 1   In the Map Viewer, right-click the desired object, and choose **States**.

The States dialog box opens.

Step 2   On the Polling tab, change the frequency for **Auto-Discovery**. The default is every 6 hours.

> **Note** Setting very frequent discovery can place a heavy demand on system resources.

Step 3   Click the Save tool or choose **File > Save**.

Step 4   Close the dialog box.

When the device is rediscovered, if the Event Browser is open, it displays the message, "Discovery is now complete". With each new discovery, any earlier discovery messages are cleared; only the most recent discovery message displays.

To Manually Rediscover a Device

Use the following procedure to rediscover a device on demand:

Step 1   In the Map Viewer, select the object, and right-click.

Step 2   Choose **States**. The States dialog box opens.

Step 3   On the States tab, click **Rediscover**. You are asked if you want to rediscover the device.

Step 4   Click **Yes**. Cisco MNM rediscovers the device. During discovery, Current State is "discovering." When the discovery is complete, Current State changes to Active (for the Cisco HSI server, Cisco BAMS, and Cisco PGW 2200 Softswitch host) or Normal (for the Cisco ITP-L and LAN Switch).

> **Note** When discovery completes, the message "Discovery is now complete" displays. Earlier discovery messages are cleared; only the most recent discovery message displays.

Step 5   Close the dialog box.

Modifying or Deleting Deployed Objects

Modify a deployed object when either of the following is changed:

*   The device password
*   SNMP community strings

If an object's IP address changes, delete the object, and redeploy it. Also delete a deployed object when the device is removed from the network or when you want to redeploy the object.

Modifying a Deployed Object

You can change device login, password, and SNMP community strings in the Accounts dialog box. Use the following procedure to modify deployment information:

Step 1   In the Map Viewer, right-click the device you want to modify, and choose **Accounts**.

The Accounts dialog box opens.

Step 2 Modify the information, as needed:

- Use the Accounts tab to change Host Login ID, Login Password, and Host Root Password.
- Use the SNMP tab to change community strings.

Step 3 When you are done, choose **File > Save** or click the **Save** tool, and close the dialog box.

The new information is saved. When Cisco MNM rediscovers the object at the next scheduled interval, this information is used to discover the device components.

✎
Note To immediately rediscover the device components, right-click the device, and choose **States**. On the **States** tab, click **Rediscover**. All components of the device are rediscovered.

Deleting a Deployed Object

You can delete a single object or multiple objects if:

- The device has been removed from the network.
- There was something wrong in the seed file, but it did not cause deployment to fail.
- The device's IP address has changed.

In the last two cases, redeploy the device after deleting the object representing it.

⚠
Caution Do not delete the object that represents a component of a device, such as an interface. Instead, let Cisco MNM rediscover the device. In rediscovery, removed components are deleted automatically.

Use the following procedure to delete one or more deployed objects:

Step 1 In the Map Viewer, do one of the following:

- Right-click a single object to delete it.
- To delete multiple objects, **Ctrl-click** to select objects in different areas of a window, or **Shift-click** to select a block of objects, and then right-click.

Step 2 Choose **Deployment > Delete Objects**. The Deployment Wizard Summary window opens with the message "Ready to delete (n) object(s)," where *n* is the number of objects selected.

Step 3 Click **Finish**.

The selected object or group of objects is deleted. A message informs you that one or more objects have been deleted from the system.

Exporting Deployment Information to an Inventory or Seed File

You can export deployment information to an inventory or seed file. A seed file includes information similar to that shown in Example 5-1 on page 5-7. An inventory file covers only the Cisco PGW 2200 Softswitch node devices but includes detailed system information obtained during discovery. For each device, it captures the current

- IP address
- Hardware type
- Operating system, host version, and software versions

Note   Inventory information for the BAMS is included if the BAMS has been configured to collect call detail records for a Cisco PGW 2200 Softswitch host.

An inventory file might be used by software that tracks inventory data about the network. A seed file can be used to capture a snapshot of your network deployment at a particular time, to be used for later deployment or to replicate a deployed network.

An example of an inventory file is shown here:

Example 5-3   Example of Exported Inventory File

```
MGC (Name = MGC-1) {

    HOST (Name = Host-1, SysName = nssuvsc21, IpAddr = 10.10.10.71, HardwareModel =
    SUNW,UltraSPARC-IIi-Engine, HostId = 80d1bd49, HostVersion = 9.0(0.16), HostVendor =
    "Cisco Systems, Inc.", Switch_Type = Switched-VSC, OS_Version = Generic_105181-23,
    OS_Release = 5.6)
    2600 (Name = SLT, SysName = n2600a.cisco.com, IpAddr = 10.10.10.72, ChassisId =
    "JAB032101S4 (3076808945)", ChassisType = 89, ChassisVersion = 0x202, ROM_Sys_Version
    = "Cisco Internetwork Operating System Software  IOS (tm) C2600 Software
    (C2600-IPSS7-M), Version 12.1(3)T,  RELEASE SOFTWARE (fc1) Copyright (c) 1986-2000 by
    cisco Systems, Inc. Compiled Wed 19-Jul-00 19:49 by ccai", ROM_Monitor_Version = "
    System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1) Copyright (c) 1999 by
    cisco Systems, Inc. TAC:Home:SW:IOS:Specials for info ", Sys_Config_Name =
    flash:c2600-ipss7-mz.121-3.T.bin)
    5500 (Name = Switch-1, SysName = nssu-cat5500-1, IpAddr = 10.10.10.74,
    Chassis_Serial_No. = 9999999, ChassisModel = WS-C5509, ChassisType = 14,
    Sys_Booted_Image = bootflash:cat5000-sup3.5-5-4b.bin)
    }
```

Table 5-6 shows the attributes exported for the various device types.

Table 5-6   Deployment Information Exported to an Inventory File

Attribute	Types	Description
name	All	Name of the object in Cisco MNM
ip	All except Cisco PGW 2200 Softswitch node and farm	IP address of the device
os	All except Cisco PGW 2200 Softswitch node and farm	Operating system name and version
boot	Cisco ITP-L/LAN switch	Name of the OS boot image
hostID	Cisco PGW 2200 Softswitch host/BAMS/HSI server	Solaris host ID
hostName	Cisco PGW 2200 Softswitch host/BAMS/HSI server	Name of the host

Use the following procedure to export deployment information to an inventory or a seed file:

Step 1   From the Map Viewer screen, click the MGC-Node-View icon.

Step 2   Right-click, and choose **Deployment > Deploy Network Seed File**.

The Deploy Network dialog box opens.

Step 3   Click the **Advanced** tab.

Step 4   In the Export section for Filename, enter a name for the file to be created.

Step 5   Do one of the following:

- To export the information as an inventory file, click **Export Inventory**.

- To export the information as a seed file, click **Export Seed File**.

A message prompting you for confirmation displays.

Step 6   Click **Yes**.

A message confirming the file creation displays.

> **Note**   By default, the file is saved in the *<CEMF Root>*/bin/.mgcControllerx.sysmgr folder. Specify the path if you want to save it to a different location.

Step 7   Click **Close**.

Step 8   Close the Deploy Network dialog box.

C H A P T E R **6**

Managing Faults with Cisco MNM

Revised: December 15, 2009, OL-18339-03

This chapter contains the following sections:

See Appendix A, "Alarm Message Reference"for information about alarm events.

Overview of Fault Management Features

One of the most important aspects of network management is the ability to identify problems on the system and to take action to resolve them quickly and efficiently. For example, a power supply failure in a chassis may be critical to the running of the network, which would need prompt attention.

In network management, these problems are typically called *faults,* and the message (or lack of message) that comes from the network device is called an *alarm* or *alarm event*.

> **Note** Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, ITP-L will replace SLT in publications and the product.

Cisco Media Gateway Controller (MGC) Node Manager (MNM) provides fault management of the devices in the Cisco MNM node. When the Cisco PGW 2200 Softswitch host detects a problem with one of its logical connections, it generates a trap. Cisco MNM receives the trap and delegates it to the graphical object that represents its logical connection. For example, if Cisco MNM receives a trap that the link to a Cisco ITP-L is down, it delegates the trap to the object representing the link.

To facilitate the monitoring of the network and identifying potential problems, Cisco MNM propagates the alarm state of network elements upward through each object view. When an object receives an alarm, the object changes color to reflect its new state, and all parent objects also change color to reflect the most severe alarm on any of the child objects.

> ✎
>
> **Note** If there are multiple alarm events propagated in an object tree, only the most severe is displayed at the highest level.

Cisco MNM periodically polls managed devices to make sure that each device is still reachable using SMNP (status polling). If the device is not reachable, an annotation appears on the display in the Map Viewer, an alarm is generated, and the object is placed in an error state. Cisco MNM continues to poll the device until connectivity is re-established. At that point, the alarm is cleared, the annotation on the display is removed, and the object is returned to its normal state. Duplicate alarms are filtered out.

For example, when a C7 IP Link goes out of service, a major alarm is immediately raised and propagated up to the Cisco PGW 2200 Softswitch host object. If the IP connection to a Cisco PGW 2200 Softswitch node is lost, a critical alarm is raised. A failover causes a major alarm.

In addition to managing alarms sent by SNMP traps, Cisco MNM monitors system resources on the Cisco PGW 2200 Softswitch host, the Cisco HSI server, and the Cisco Billing and Measurements Server (BAMS) and raises alarms for events such as an application being down, or a file usage being above a specified percentage.

To investigate an alarm that is displayed in the Cisco MNM Map Viewer, you typically perform the following steps:

Step 1   Drill down through the tree view to the object that has raised the alarm,

Step 2   From the object, open the Event Browser.

Step 3   In the Event Browser, identify the alarm details and take appropriate action to resolve the problem.

In addition to using the Event Browser to check on alarms flagged in the Map Viewer, you can use the Query Editor included in the Event Browser to filter alarms on any desired criteria. Diagnostic services can be invoked on events so that faults can be managed from the window that shows the event.

With Cisco MNM, you can also forward alarms to any configured remote host and continuously export alarm events as they are raised to a text file.

The "Managing Faults with Cisco MNM" section on page 6-3, describes the main tasks and procedures for managing faults. If you are interested in some of the principles Cisco MNM applies in its fault management, see the "How Cisco MNM Handles Events" section on page 6-17.

What Is Managed

Cisco MNM performs fault management on the Cisco PGW 2200 Softswitch node devices including the Cisco PGW 2200 Softswitch host network connectivity. This includes the logical connections from the active Cisco PGW 2200 Softswitch host to the

- Interfaces (Ethernet, TDM)
- STPs
- Point codes (SS7 routes)
- Remote Cisco PGW 2200 Softswitches
- TCAP nodes
- Cisco Media Gateways

The logical connections from the active Cisco PGW 2200 Softswitch host are shown as subnodes under the common Cisco PGW 2200 Softswitch host object. If the standby Cisco PGW 2200 Softswitch host is not processing calls, only the network connectivity of the active Cisco PGW 2200 Softswitch host is shown.

For a reference describing the alarm events for specific devices, see Appendix A, "Alarm Message Reference."

In addition to accepting SNMP traps from managed devices, Cisco MNM also generates alarm events based on its own internal traps.

Managing Faults with Cisco MNM

The following summarizes the tasks required for managing faults with Cisco MNM. These tasks do not need to be performed in sequence.

- Task 1. Adjusting Status Polling Settings If Needed, page 6-3
- Task 2. Customizing Event Management, page 6-4
- Task 3. Monitoring the Network for Alarm Events, page 6-8, using the Map Viewer alarm display and the customized alerts you set up in task 2.
- Task 4. Using the Event Browser, page 6-8, to view, filter, and clear events, and to start diagnostic services on a problem device.
- Task 5. Using Troubleshooting Tools, page 6-17, which is opened directly from the Event Browser.

The procedures for completing each task is provided in the sections below.

Task 1. Adjusting Status Polling Settings If Needed

Status polling checks the device status, such as up, down, active, or standby, as shown on the Status tab of the Properties dialog box for the device. You can specify a different status polling frequency for each device type, such as Cisco ITP-Ls or Cisco LAN switches. All devices of that type and all components of such devices have the same polling frequency. For example, if you set a 5 minute polling frequency for one Cisco ITP-L in the network, the frequency is applied to all Cisco ITP-Ls in the network and to all monitored elements on the Cisco ITP-L, such as the TDM interfaces.

For the Cisco ITP-L and Cisco LAN switch, the polling frequency is set at the device level. All components of the device have the same polling frequency as the parent device. For example, setting a frequency of every 10 minutes for a Cisco ITP-L also polls its TDM interfaces every 10 minutes.

Note
- Default status polling frequency is every 2 minutes.
- To stop status polling when there is a known problem with a device or the device is taken out of service, decommission it. See the "Commissioning, Decommissioning, and Rediscovering Devices" section on page 6-23.

Use the following procedure to set or change a status polling frequency:

Step 1 In the Map Viewer, right-click the desired device, and choose **States**.

The States dialog box opens.

Note • If the **States** option is not available, select the parent device.

  • For the Cisco PGW 2200 Softswitch host, including its Cisco PGW 2200 Softswitch node signaling or trunking components, select the Cisco PGW 2200 Softswitch Host object.

Step 2 Set the desired Status polling frequency. To change from minutes to hours, select from the drop-down menu. For all devices and types of polling, the minimum frequency is 1 minute and the maximum is 24 hours.

Step 3 Click the **Save** tool to save the changes.

Step 4 Close the dialog box.

Note For information on Performance and Configuration polling, see Chapter 7, "Managing the Performance of Cisco MNM Devices." For information on Auto-Discovery polling, see Chapter 5, "Deploying Your Network in Cisco MNM," "Synchronizing the Cisco MNM with Device Changes" section on page 5-20.

Task 2. Customizing Event Management

The Cisco EMF Event Manager provides three tools that can be used together to customize how you manage events:

  • Thresholding regimes can be used to set up criteria for raising alarms on groups of devices based on selected performance measurements that cross a specified threshold. The thresholding regime also specifies what notification profile is used when the threshold is crossed and the alarm is raised.

  • Notification profiles define how you want to be notified of the threshold-crossing alert, such as with a pop-up message window or a sound. You can also have a script run when the threshold is crossed.

  • Event groups let you group events according to your own criteria, such as event severity or device type.

After an overview of each of these Event Manager tools, this section gives an example of how to create and use a scoreboard and how to set threshold-crossing alerts.

About 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 deviates from preset criteria.

Typically, you apply a standard set of criteria to an entire set of objects as part of a management policy. An example policy is illustrated below:

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

A thresholding regime has a set of trigger conditions, and each trigger condition is 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 the expression is satisfied

Setting up a thresholding regime allows you to apply or change the management policy of all 5000 routers at once rather than having to apply it to each one individually. You can change the central regime to apply the new policy to all objects within a group.

Once a threshold has been crossed, you can have the system notify you or carry out a sequence of actions. The specification of the actions to carry out is called a *notification profile*. Notification profiles are described in the "About Notification Profiles" section on page 6-5.

About Notification Profiles

Notification profiles consist of a specified series of notifications that should be carried out as a result of the profile being triggered by a thresholding regime. Thresholding regimes are described in the "About Thresholding Regimes" section on page 6-4.

Notification types available are:

- **Beep Once**—Produces a single beep
- **Raise Window**—Brings all windows that contain the controller object icon to the front of the window stack
- **Flash Icon**—Causes the controlling object icon to flash in active windows
- **Beep Continuously**—Produces a continuous beep
- **Popup Dialog**—Opens a window that contains a user 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 notifications can be given a time delay, allowing a simple form of escalation process to be implemented. For example:

When a notification profile is triggered, raise a minor event; if the notification profile has not been reset within 30 minutes, 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 used to keep track of the current status of active notifications. Notification profiles can be viewed as templates that are used at trigger time to create an active running version. You can view the state of any notification profiles currently running on an object.

About Event Groups

A typical telecommunications network can generate a large volume of events. Only a small proportion of these events may affect service or require immediate attention. Others may still be of interest but are not urgent. For effective network management, you must be able to quickly identify the critical issues from the less than critical events.

You may also want to categorize the handling of certain events based on geographical location or the technical knowledge of certain users.

Event groups allow you to easily divide events into manageable groups based on user defined filtering criteria, such as:

- Event severity

- Event state

- Type of network element affected by the event

For display purposes, you can arrange these event groups on *scoreboards*. Each scoreboard shows a summary box for each group, allowing you 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.

Event groups have three possible trigger conditions:

1. When the first event enters the group, invoke notification profiles

2. When the first event on an object enters the group, invoke notification profiles

3. When *any* event enters the group, invoke notification profiles

For a description of tools used with event groups, see the "About Thresholding Regimes" section on page 6-4 and the "About Notification Profiles" section on page 6-5.

Creating and Using Scoreboards

You can create a scoreboard to display the alarms you are interested in. For example, you might create a single scoreboard to display the critical, major, and minor alarms received for your entire network, as well as alarms site-by-site.

The major tasks are:

- Create a scoreboard using the Notification Profiles application

- Using the event group application, create an event group for the alarm criteria you are interested in

- Add the event group to the scoreboard

Two examples are provided in the next section.

Scoreboard Example 1

Use a scoreboard to monitor all alarms on a network using the following procedure:

Step 1   In Notification Profiles, create a notification to display a pop-up window.

Step 2   Create a new event group by doing the following:

a. On the Launchpad, click **Event Groups**.

b. Choose **Edit > Create > Event Group**.

c. Fill in a name and description for the group.

d. Click **Edit Query** to modify the default query.

e. For Severity, choose **Critical/Major/Minor**.

f. Choose **File > Exit**. You are prompted to save the query. Click **Yes**.

g. Click **Forward**.

h. From the list of trigger conditions, choose **Trigger every time an event enters the Event Group**.

i. Click **Edit**.

j. From the list of notification profiles, select the pop-up window.

    k. Click **Finish**.

    l. Click **Forward**.

    m. Click **Finish**.

Example 2

Use a scoreboard to monitor alarms at a particular site using the following procedure:

Step 1   Create a new event group as described in Example 1.

Step 2   For Severity, choose **Critical/Major/Minor**.

Step 3   For Event Status, keep the default, **Active Only**.

Step 4   For Object Scope, select all objects for the desired site.

Step 5   Click **Finish**.

Step 6   In Notification Profiles, select the scoreboard used in Example 1 and add the Event Group.

Setting Threshold Crossing Alerts

You can trigger a threshold crossing alert (TCA) when a particular performance indicator crosses a specific threshold. In the example here, a TCA is created to alert you when the CPU utilization of a Cisco PGW 2200 Softswitch host crosses a specified threshold.

Task 1

Use the following procedure to create an object group for a Cisco PGW 2200 Softswitch host processor:

Step 1   On the Launchpad, right-click **Object Group** and choose **Create New Group**.

Step 2   Fill in a name and description for the group.

Step 3   Click **Query Setup**, and click **Add Object(s)**.

Step 4   In the Host View, select the Cisco PGW 2200 Softswitch host, and choose the Processor-1 object.

Step 5   Click **Apply**, to add this object to the group. You can add similar objects from the other deployed Cisco PGW 2200 Softswitch hosts if you have multiple hosts deployed.

Step 6   Click **File > Close**, and save the query when prompted.

Step 7   Click **File > Close** again, and save object group changes when prompted.

Task 2

Use the following procedure to create a trigger condition:

Step 1   On the Launchpad, click **Thresholds**.

Step 2   Click **Edit > Create New Thresholding Regime**.

Step 3   Give the regime a name and a description.

Step 4   From the object group, choose the object group created in Task 1.

Step 5   Click **Forward**.

Step 6   Click **Add** to create a new threshold.

Step 7   From the list of attributes, choose **mgcProcessor**.

Step 8   Under that object, choose **HOST-RESOURCES-MIB.hrProcessorTablemgcProcessor**.

Step 9   Under that object, choose **hrProcessorTable**, and then choose **Utilization**.

Step 10   Choose (**>**) from the list of operators.

Step 11   Specify a value, such as 70, and click **Add**. A trigger condition is created.

Step 12   Click **Forward**, and choose whether to use the default reset condition.

Step 13   Click **Forward**, and specify how often the trigger or reset condition should be checked.

Step 14   Click **Forward**, and choose the notification profile to associate the new thresholding profile.

Step 15   Click **Finish**.

Step 16   Click **Forward** to activate the thresholding regime.

Step 17   Click **Forward** and **Finish** to save the thresholding regime.

Task 3. Monitoring the Network for Alarm Events

You can monitor the network for alarm events in two ways:

- Using the Map Viewer Node View, you can see color-coded alarm indicators displayed on problem objects. In the Node View, alarms are propagated up from child elements to parent devices, so by watching just the main network devices, you can see when alarm events have occurred in any of their subcomponents. By drilling down, you can find the affected network element and then open the Event Browser to inspect the problem.

  For details on using the Map Viewer and understanding its display, see Chapter 3, "Getting Started with Cisco MNM," "Using the Map Viewer" section on page 3-10.

- Using customized event management tools such as scoreboards and threshold-crossing alerts, you can have Cisco MNM notify you of selected problems. For information on these tools, see the "Task 2. Customizing Event Management" section on page 6-4.

Task 4. Using the Event Browser

In Cisco MNM, an 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 at any one time.

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. The Event Browser can be started from:

- Map Viewer—to check on events for one or more selected devices
- LaunchPad—to run a query for particular events

You can have more than one Event Browser session open at a time, and each session can have different queries specified. All users can see any event. When an event is received, it is shown as active and unacknowledged (the Clear and Acknowledge column indicators on the event browser window are shown as grey). At this stage, no action has been taken. In the Event Browser window, you can acknowledge that a particular event is one that you are going to act upon, 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 that other users know that the event requires no further attention.

Some events are cleared automatically according to predefined clear correlation rules. These rules are described in the "Automatic Alarm Clearing" section on page 6-19.

Note   The BAMS File Rename Failure alarm (POL115) must be manually cleared, not only in Cisco MNM but also on the BAMS, before new alarms of that type can be generated.

Opening the Event Browser for One or More Selected Devices

Use this procedure when you have identified an alarm event for a particular device or devices in the Map Viewer.

Step 1   In the Map Viewer, select the device or devices.

Step 2   Right-click the device, and choose **Tools > Event Browser**.

The Event Browser window opens displaying events for the selected devices. Go to the "Using the Event Browser to Manage Events" section on page 6-9 for more information.

Opening the Event Browser to Run a Query

Use this procedure when you want to check the network for alarm events of a particular type.

On the Launchpad, click the **Events** icon.

The Event Browser opens to the Query Editor for you to define a query to display events that match the query criteria. For more information, see the "Filtering Events Using Queries" section on page 6-14. Once you have created a query, go to the "Using the Event Browser to Manage Events" section on page 6-9.

Using the Event Browser to Manage Events

You can open the Event Browser from the Map Viewer or the Launchpad to check events for specific devices or to run queries.

Use the Event Browser to:

- Get details on events.
- View event history.
- 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.
- When the fault has been corrected and the event requires no further attention, clear the event. It is then removed from the Event Browser.

- Start diagnostic or other services to troubleshoot the event.

Use the following procedure to manage events in the Event Browser:

Step 1 Open the Event Browser window as described in the "Opening the Event Browser for One or More Selected Devices" section on page 6-9 or the "Opening the Event Browser to Run a Query" section on page 6-9.

Step 2 (Optional) Change the view options:

- To change sort order, choose **Edit > Sorting Options**, and select the desired fields to sort.
- To change how the severity column is color-coded, choose **View > Set Color Coding**.

Step 3 (Optional) Turn automatic updating off or on:

- Choose **View > Enable Auto Update** to toggle between automatic and manual updating.

  Auto Update is the default state and allows you to view incoming events that are automatically updated in the window. If you are using manual updating, click **Refresh** periodically to see new events.

Step 4 (Optional) View event history to see any events from the last seven days that match the current query but have had their status changed by being acknowledged, cleared, or unacknowledged:

- Choose **View > Event History**.

Step 5 Select one or more events by clicking event severity, name, time, or description.

Step 6 (Optional) View a full description of an event, including acknowledge and clearing details:

- Double-click the event. The Full Event Description window displays. For more information, refer to the "About the Full Event Description Window" section on page 6-12.

Step 7 Do one of the following to change the event state, as appropriate:

- To acknowledge that you are handling the event, click **ACK**. The indicator changes to the color of the severity of the event. Or, right click the event and choose **Event State > Acknowledge** from the drop-down menu.
- To unacknowledge an event, right click the event and choose **Event State > Unacknowledge** from the popup menu.
- To clear the event when it has been resolved, select the event, and click **Clear Events**. This displays the Events Clearing window. Enter the reason for clearing the event, and click **Apply**. The indicator changes to the new color of the severity of the event.
- (If you acknowledged the event or are the administrator) To unacknowledge an event that is not resolved but you are not handling, click **ACK**.

Step 8 (Optional) Click **Print**, to save the contents of all or part of the Browser to a file or to print a paper copy.

Step 9 (If automatic updating is off) Click **Refresh** to view the new events that meet the current criteria.

Step 10 Close the Event Browser window.

> **Note** Query criteria are discarded when you close the window.

About the Event Browser Window

Use the Event Browser window to view and manage events, either on devices selected in the Map Viewer or selected through a query. The window is shown in Figure 6-1.

Figure 6-1   Event Browser Window
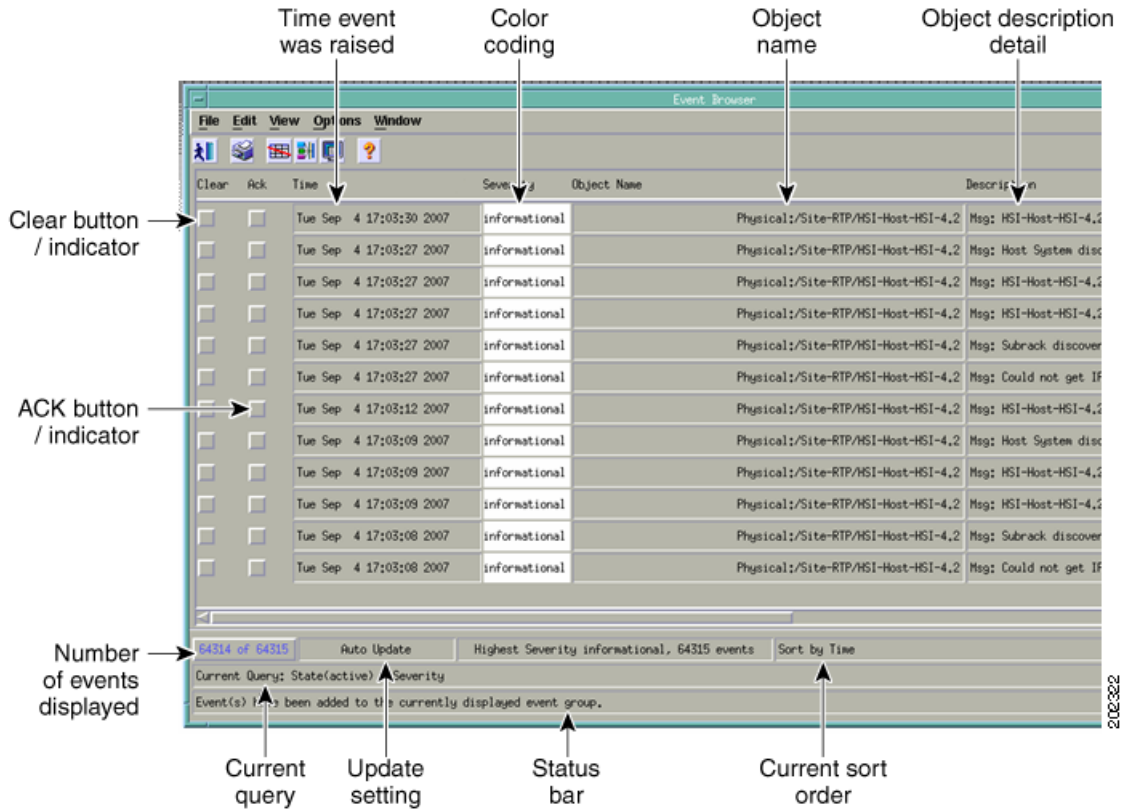
Main Panel

The main panel in the Event Browser window, shown in Figure 6-1, displays information about events including:

- Object 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, displays 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

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

Event Severity Color-Coding

Each event has a severity that indicates the importance of the event and is identified with a corresponding color as shown in Table 6-1.

Table 6-1   Colors Used to Indicate Severity

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

Status Bar Information

The Event Browser window also displays the following 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. The status bar indicates whether there are more events on the system.

About the Full Event Description Window

Double-clicking an event in the Event Browser displays the Full Event Description window (see Figure 6-2). This window provides details of the event, including acknowledge and clearing details.

Figure 6-2   Full Event Description Window

Note   If the event has not been cleared, the Event State is Active and the Clearing Method, User Responsible for Clearing, and Clearing Time and Date sections are disabled. You cannot alter the information displayed.

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 Cisco EMF 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 that reported the event.
- Management Domain—The Management domain that reported the event.
- 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

Filtering Events Using Queries

The Event Browser monitors all events on all devices. To work efficiently, you might 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 look only at events that are warnings or are critical. You can define a query so that the Event Browser displays only the events that meet the criteria you defined.

> **Note** A query applies to the current Event Browser session only; stored queries are not supported. You can modify a current query, but once you close the Event Browser the query is discarded.

Use the following steps to define a query:

Step 1 Do one of the following to open the Query Editor:

- On the Launchpad, click the Events icon.
- If the Event Browser is already open, choose **Edit > Query Setup** or click the **Query Filter** tool:

The Query Editor window, similar to Figure 6-3, opens.

Step 2 Set filtering (query) criteria:

- To add a value to the query, select it in the Available Values list and click **>>** to place the value in the Selected Value list. To remove a value, select the value in the Selected Values list and click **<<**. See the "About the Query Editor Window" section on page 6-15 for details.
- To activate selected values on a given tab, click the **Activate** box. 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.

See the "About the Query Editor Window" section on page 6-15 for details.

Step 3 Click **Apply**, and close the Query Editor.

The following message displays:

Save Query Changes?

Step 4 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 current session only. When you close the Event Browser, the query criteria resets to the default.

Modifying a Query

Use the following steps to modify a query:

Step 1   Choose **Edit > Query Setup** or click the Query Filter tool:

The Query Editor window (Figure 6-3) is displayed with the current settings.

Step 2   Modify filtering (query) criteria:

- To add a value to the query, select the value in the Available Values list and click **>>** to place it in the Selected Value list. To remove a value, select it in the Selected Values list and click **<<**. See the "About the Query Editor Window" section on page 6-15 for details.
- To activate selected values on a given tab, click the **Activate** box. 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.

Step 3   Click **Apply**, and close the Query Editor.

The following message displays:

Save Query Changes?

Step 4   Click **Yes**.

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

Query changes are saved for the current session only. When you close the Event Browser, the query criteria resets to the default.

About the Query Editor Window

The Query Editor is shown in Figure 6-3.

Figure 6-3   Query Editor Window
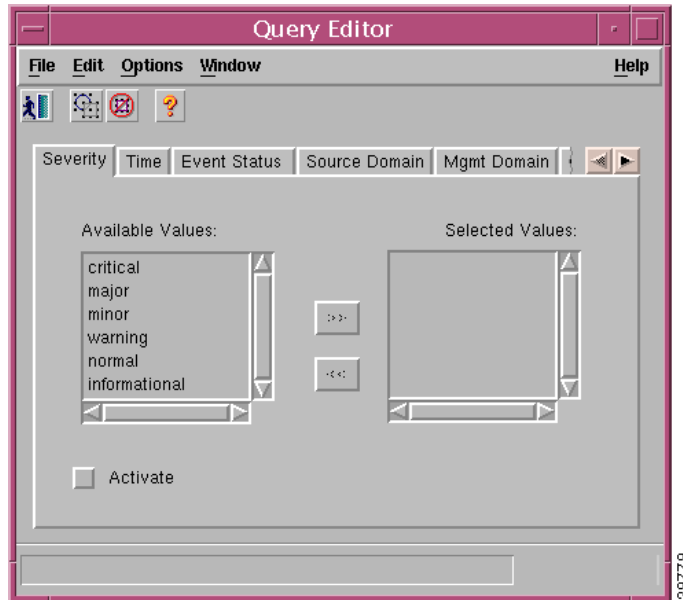
The criteria that can be used to specify a query is grouped on tabs. After selecting criteria from the Available Values list on a tab, click the **Activate** box to activate the criteria. A dark gray tab is active (On): its query is used in the Event Browser. A light gray tab is inactive (Off): its query is not used.

The Query Editor includes these tabs:

- Severity—Critical, major, minor, warning, normal, or informational.

- Time—Time range for which you want to view events, specified with time of day, day of the week, and date.

- Event Status—Acknowledged or unacknowledged, active or cleared.

- Source Domain—Where the event was generated: SNMP, the managed network, internal, or generated by Cisco MNM.

- Mgmt Domain—The management domain of the SNMP trap information. The SNMP Management Information Base (MIB) information typically defines the equipment type generating a trap.

- User—Name of the user associated with an acknowledged or cleared event.

- Event Class—Type of event.

- Object Scope—Use to select all the events of a node and its children. Select from an object tree, specifying the number of levels to view for a selected node. To specify scope:

    - On the Object Scope tab, click **Add Scope**. The View Scope selector displays.

    - Select the desired node.

    - In the Number of Levels field, type the number of levels to view.

    - Select **Descendants**.

    - Click **Apply**.

- Object Class—Type of object, such as managed, container, network, site.

- Object Attribute Presence—For various object types, attributes to query.

- Object Attribute Value—For specified object types and attributes, values to query for.

Task 5. Using Troubleshooting Tools

Once an alarm has been identified, you can use Cisco MNM to launch a variety of diagnostic and troubleshooting tools. For details, see Chapter 8, "Other Network Management Tasks," "Using Diagnostic Tools" section on page 8-65.

In the Event Browser, you can right-click a device and open troubleshooting tools such as:

- A Diagnostics dialog box. The Diagnostics dialog box provides shortcuts for common diagnostics that normally require using UNIX or MML commands. You can ping the device for connectivity, use Traceroute, check the alarm log, check the status of running processes, display the BAMS system log, and audit the BAMS trunk groups, cross-checking them with the Cisco PGW 2200 Softswitch host configuration, and retrieve state information on various network elements.

Note   The alarm log for the Cisco PGW 2200 Softswitch, BAMS, HSI, ITP-L, and Catalyst is the file traplog.log. CIsco EMF messages go to a separate file, mgcTrapProcessor.log.

- The MGC toolbar (also known as the MGC toolkit), which contains a suite of diagnostic and troubleshooting tools. For details, see Chapter 8, "Other Network Management Tasks," "Using the MGC Toolbar" section on page 8-67.
- CiscoView, to troubleshoot problems on the Cisco ITP-L or Cisco LAN Switch. You can also use Cisco MNM to Telnet to a device or to launch an X terminal window. For details, see Chapter 8, "Other Network Management Tasks," "Using Cisco MNM To Launch Device Configuration" section on page 8-4.

How Cisco MNM Handles Events

Refer to this section if you are interested in the principles applied by Cisco MNM in processing and displaying events. It includes:

- Understanding Event Propagation, page 6-17
- Understanding Alarm Acknowledgement and Clearing, page 6-18
- Understanding Status Polling, page 6-20

Understanding Event Propagation

To make the identification of potential problems easier, Cisco MNM propagates the alarm state of objects upwards through the Physical and Node object views.

Note   To minimize redundant updating, alarms are propagated only in the Physical and Node views, not in device views. In a device view, a gray dot indicates an alarm somewhere in the tree. Check the relevant device in the Node view to find the alarm.

If an object receives an event, the object changes color to reflect its new state, and 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, and the bay within a site.

If a minor alarm is received on Port B, then Port B and all of the objects up to the region turn yellow to indicate a potential minor problem, as illustrated in Figure 6-4.

Figure 6-4   ***Example Minor Event Propagation***
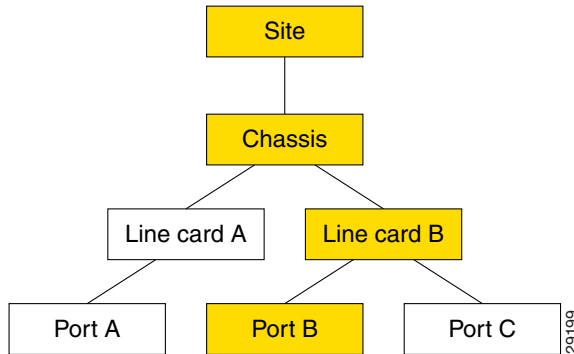
If a critical alarm was then received on Port A, that port, and all of the objects up to the region, turn red to indicate a potential critical problem, as illustrated in Figure 6-5.

Figure 6-5   ***Example Critical Event Propagation***
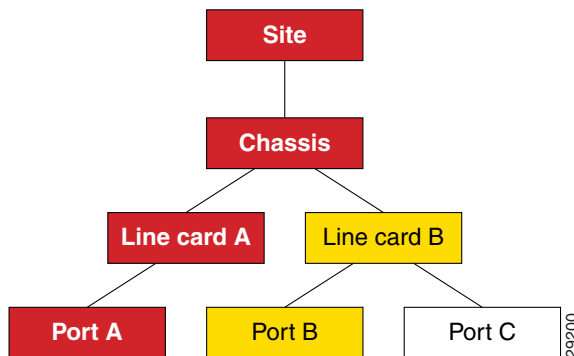
If the critical alarm is cleared, the icons return to yellow.

Cisco MNM filters out duplicate traps from a network element. It also filters out traps from network elements that report a problem and reports within a few seconds (up to 6) when the problem is resolved. Cisco PGW 2200 Softswitch 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.

Understanding Alarm Acknowledgement and Clearing

This section describes how event acknowledgement and clearing work in the Event Browser.

When a new event is received, its event state is active and unacknowledged. Acknowledging the event indicates to other users that it is being handled. When it is resolved, you can clear the event.

When you cannot clear an event due to an existing problem, the event can be returned to the unacknowledged state and later acknowledged or cleared by another user.

Whether an event is unacknowledged or acknowledged, the event is considered active until it is cleared. The relationship between event states is shown in Figure 6-6.

Some events are cleared automatically when the originating condition is resolved, according to rules described in the "Automatic Alarm Clearing" section on page 6-19.

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.

Figure 6-6   State Diagram for Events
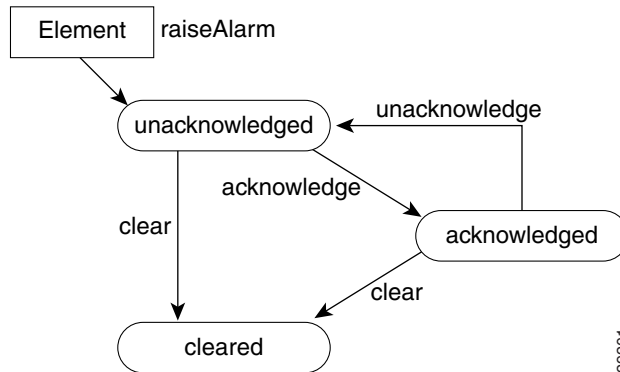
Automatic Alarm Clearing

Cisco MNM automatically clears alarms based on certain built-in, logical rules. 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.

These rules are maintained in Clear Correlation files. A sample Clear Correlation file is:

CLEAR_CORRELATION_RULE

    INCOMING_ALARM_CLASSlinkUpAlarmClass

    ALARM_CLASS_TO_CLEARlinkDownAlarmClass

    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 tables show the clear conditions for the alarms for each Cisco PGW 2200 Softswitch node device.

Table 6-2   Cisco PGW 2200 Softswitch Host Clear Correlation

Alarm	Clear Condition
processingError	processingNormal
communicationFailure	communicationSuccess
qualityOfServiceError	qualityOfServiceNormal

Table 6-2   Cisco PGW 2200 Softswitch Host Clear Correlation (continued)

equipmentError	equipmentNormal
environmentError	environmentNormal

Table 6-3   Cisco ITP-L Clear Correlation

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

Table 6-4   Cisco LAN Switch Clear Correlation

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

Table 6-5   Resource Alarms (Cisco PGW 2200 Softswitch host, HSI server, and BAMS) 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 criaAppName 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.

Understanding Status Polling

Cisco MNM periodically polls each managed object (the Cisco PGW 2200 Softswitch host, Cisco ITP-L, LAN switch, HSI server, and BAMS) to ensure that the device is still reachable using SNMP. If the device is not reachable, its state is indicated by annotation on the Map Viewer, and an alarm is generated. In addition, the object is placed into the error state.

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

Cisco MNM also displays the status of the Cisco PGW 2200 Softswitch host connectivity network. This includes the logical connections from the active Cisco PGW 2200 Softswitch host to the following:

- Interfaces (Ethernet, TDM)

- STPs
- Point codes (SS7 routes)
- Remote Cisco PGW 2200 Softswitches
- TCAP nodes
- Cisco Media Gateways

The logical connections from the active Cisco PGW 2200 Softswitch host are shown as subnodes under the common Cisco PGW 2200 Softswitch host object. If the standby Cisco PGW 2200 Softswitch host is not processing calls, only the network connectivity of the active Cisco PGW 2200 Softswitch host is shown.

Status details are provided below.

Network Interface Status

Cisco MNM 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 transitions to another state, as shown in Table 6-6.

Table 6-6   Transition 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 Cisco MNM 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, Cisco MNM 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 Cisco MNM. When Cisco MNM detects this trap, it transitions the object representing that interface to the down state. To handle the case where Cisco MNM 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 Cisco MNM detects this trap, it transitions the interface back into the normal state. If Cisco MNM missed this trap, the next status poll detects that the interface is back up. Internally, Cisco MNM transitions the interface back to the normal state and clears the appropriate alarms on the object.

Cisco PGW 2200 Softswitch Host Status

Cisco MNM periodically checks the status of each Cisco PGW 2200 Softswitch 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 shown in Table 6-7.

.

Table 6-7   Cisco PGW 2200 Softswitch Host States

Component Status	Network Interface State
ACTIVE	active
STANDBY	standby
OOS	oos
No answer	not-running
Not reachable	unreachable

BAMS Status

Cisco MNM 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 shown in Table 6-8.

.

Table 6-8   BAMS States

Component Status	Network Interface State
Active	active
Standby	standby
Outage	oos
Other	other
No answer	not-running
Not reachable	unreachable

HSI Status

Cisco MNM periodically checks the status of each HSI device. The SNMP:HOST-RESOURCES-MIB.hr.sysStatus attribute is retrieved, and its value is used to determine the required state of the object, as shown in Table 6-9.

Table 6-9   HSI Status

Component Status	Network Interface Status
Active	active
Other	other
No answer	not-running
Not reachable	unreachable

Trap Receipt Not Guaranteed

Cisco MNM does not provide any guarantee that it received a trap from the southbound systems or network elements. Cisco MNM does not perform any negotiation with the network elements to detect or recover lost traps.

How Cisco MNM Manages Multiple IP Addresses for Status Polling

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

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

Any interface on the device might 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. Cisco MNM is designed to avoid these situations by using trap proxies and IP address failover.

Commissioning, Decommissioning, and Rediscovering Devices

When a device is administratively off the network, or it has a known problem and you do not want to manage it, you can decommission the device in Cisco MNM to stop it from being polled and generating unnecessary alarms.

When a device is decommissioned, no actual changes are made to the device, which still sends traps to Cisco MNM. However, the resulting alarm events are not reported and do not initiate any actions or status changes. Status and performance polling are also suspended.

Note When a device is decommissioned, all its subcomponents are also decommissioned.

When the device is back in service, commission it to resume polling. At that point, Cisco MNM starts discovery to resolve any component changes that may have occurred while the device was decommissioned.

When a device's subcomponents have changed or you have corrected a problem that interfered with discovery, you can rediscover the device to immediately update the Cisco MNM network model with the changes.

Note Rediscovery is necessary only when you want the update to occur before the next auto-discovery polling interval when any changes are routinely detected.

Use the following procedure to decommission, commission, or rediscover a device:

Step 1   In the Map Viewer window, select the object and right-click.

Step 2   Choose **States**. The States dialog box opens.

Step 3   On the States tab, do one of the following:

- Click **Decommission** to stop processing traps from the device.

- Click **Commission** to resume processing traps after a device had been decommissioned.

- Click **Rediscover** to rediscover a device, updating the network model with any device changes since the last auto-discovery.

    You are prompted to confirm the action.

Step 4   Click **Yes**. Cisco MNM executes the action. The device state changes to reflect the change.

> ✏️
>
> **Note**   When a device is rediscovered, if the Event Browser is open, it displays the message, "Discovery is now complete." With each new discovery, any earlier discovery messages are cleared; only the most recent discovery message appears.

Step 5   Close the dialog box.

Forwarding Traps to Other Systems

You can forward the traps (alarms) collected from managed elements by Cisco MNM to other systems. In addition to receiving SNMP traps from node devices, Cisco MNM monitors resource usage on the Cisco PGW 2200 Softswitch host, HSI server, and the BAMS. Traps are generated, for example, when disk usage exceeds a given threshold or when applications are down.There are two types of trap forwarding:

- Using cmnmtrapforward
- Using Northbound Event Interface

Using cmnmtrapforward

Use the **cmnmtrapforward** command to automate the procedure to stop or start forwarding traps to other systems by updating the trapForwardFile file.

To Start Trap Forwarding

Follow these steps to start trap forwarding:

Step 1   From the Cisco EMF base directory, enter the following command:

cmnmtrapforward

Information similar to the following is displayed:

```
Configure trap forwarding to other hosts? [y/n]: [n]
```

Step 2   Enter **Y**. Information similar to the following is displayed:

```
Trap Forwarding is configured for the following IPs
   172.16.128.46
Please enter a Trap Forwarding IP address [?,q]
```

Step 3   Enter the IP address to which traps will be forwarded, and press **Enter**. Information similar to the following is displayed:

```
Enter another IP address? [y/n]: [n]
```

Step 4 Continue to add IP addresses, or press **N** when you are finished. The following prompt appears:

```
Restarting TrapManager....
```

To Stop Trap Forwarding

Enter the following command from the Cisco EMF base directory to stop trap forwarding:

./cmnmtrapforward -d <IP address of destination host>

The destination IP address is removed from the trapForwardFile file.

Use the **cmnmtrapforward -h** command to view more information about this command.

Using Northbound Event Interface

The Northbound Event Interface (NEI) allows for integration with network management systems (NMSs), such as Hewlett Packard-OpenView Element Management Framework (HP-OEMF) and CIC (Cisco Information Center). Using NEI, you can export topological information about managed objects and forwardCisco EMF events to NMSs.

The main purpose of NEI is to convert Cisco EMF events (appearing in the Event Browser) to a particular output for NMSs. Output can be in the form of an SNMP trap, log files, or TCP connections.

NEI has two main functions: exporting and forwarding. To define export and forward filters, you can create a filter file that will contain both types of information.

For further information on NEI, go to

http://www.cisco.com/en/US/docs/net_mgmt/element_manager_system/3.2_service_pack_7/installation/guide/nei.html

✎
Note   Northbound CORBA flowthrough provisioning is no longer supported.

Sample Filter File in MNM

The following is a sample filter file for a physical view in Cisco MNM:

```
name="physical-traps.nbf"
exporting
{
    delta
    {
      temp="/tmp/filter.delta.tmp"
      result="/tmp/filter.delta.result"
    }
    dump
    {
      temp="/tmp/filter.dump.tmp"
      result="/tmp/filter.dump.result"
    }
      filter="NbNullExporter"
      origin="Physical:/"
}
forwarding
```

```
{
  filter="NbExtensibleSNMPForwarder"
  snmp-destination="10.20.1.19"
  snmp-port="162"
  enterprise="1.3.6.1.4.1.1469.6"
  added_aqs
  {
    severity="critical"
    severity="major"
    severity="minor"
    status="cleared"
    status="acknowledged"
    status="unacknowledged"
  }
  changed_aqs
  {
    status="acknowledged"
    status="unacknowledged"
  }
  containment-tree="MGC-Node-View"
}
```

Difference between NEI and cmnmtrapforward

This section briefly explains the differences between using NEI and Trap Forwarding. It contains

- Northbound Event Interface
- cmnmtrapforward
- Recommendation

Northbound Event Interface

NEI allows integration with higher fault management systems, such as HP-OEMF. NEI includes two main areas of Functionality,

- Configurable topological export - to build managed objects as defined within a Cisco MNM server using CLASS mapping files

- Configurable MNM fault forwarding - forward SNMPv1 and SNMPv2c traps generated from MNM faults to higher fault management systems, such as HP-OEMF. Customers create filter files with two sections, namely "exporting" and "forwarding."

cmnmtrapforward

Raw traps received by Cisco MNM from the devices being managed are forwarded to multiple third party NMSs by adding hostname ip address, generic trap id, specific trap id, enterprise oid, and details in the trapForwardingFile. This feature does not include the functionality of exporting and forwarding filters as supported by NEI, nor does it forward alarms that are generated by Cisco MNM itself, such as communication failures detected during polling of managed devices.

Recommendation

Since trap forwarding has minimal value when compared to NEI, we recommended using NEI for forwarding traps to third party NMS.

Specifying the Length of Time Alarms Are Stored

All alarms are automatically stored in the Cisco MNM database and purged at regular intervals to make room for new alarms. The Alarm Deleter, built into Cisco EMF, is set up to run at midnight every night. The Alarm Deleter queries the alarm database and deletes alarms that meet the specified criteria. The default is to delete cleared alarms that are seven days old.

If you want to change the frequency with which old alarms are deleted, you can change the values in the alarmDelete.ini file. An example of the file is shown here:

```
[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"
```

Table 6-10 describes the variables used in defining the deletion rules.

Table 6-10   Alarm Deleter Attributes

Variable	Description
ageOfAlarmsInDays	The age of the alarm, in days, before it is to be deleted.
ageOAlarmsInHours	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.

Managing the Performance of Cisco MNM Devices

Revised: December 15, 2009, OL-18339-03

This chapter contains the following sections that describe basic procedures for managing the performance of the Cisco Media Gateway Controller (MGC) Node Manager (MNM) node:

- Overview of Performance Management Features, page 7-2
- Monitoring Network Performance, page 7-4
  - Task 1. Setting Performance Polling Frequencies, page 7-5
  - Task 2. Starting Polling On a Network Element, page 7-6
  - Task 3. Viewing Performance Data, page 7-7
  - Exporting the Currently Displayed Performance Data, page 7-16
  - Printing a Performance File, page 7-16
- Selecting What To Monitor, page 7-16, provides some general guidelines and examples

For reference information on the performance measurements collected by Cisco MNM, see Appendix B, "Performance Measurements Reference."

This chapter also describes the procedures that may be used by system administrators:

- Filtering Measurements Collected by Cisco MNM, page 7-18
- Changing Performance Thresholds, page 7-18
- Exporting Bulk Performance Data, page 7-19
- Changing How Performance Data Is Archived, page 7-20

Note You can set performance thresholds for various measurements. When performance falls below the threshold level, Cisco MNM notifies you with a *threshold crossing alert* (TCA). See Chapter 6, "Managing Faults with Cisco MNM" for details on setting and managing performance thresholds.

Overview of Performance Management Features

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. This information can be used to evaluate the performance of specific equipment, assess the requirements for upgrades or software downloads, and identify problem areas in the network.

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.

Cisco MNM provides performance management features to collect, display, and store performance data. You can:

- Collect selected performance attributes on any Cisco PGW 2200 Softswitch node device or group of devices at specific intervals

- Drill down in the Map Viewer from the network level to the device level to view individual device statistics

- In the Performance Manager, you can:

    – View performance data for selected time periods

    – Depending on the device, view performance data in line graph, bar chart, or table format

    – Export the displayed performance data to a flat file

    – Print performance data

The system administrator can:

- Filter measurements collected by Cisco MNM

- Change performance thresholds

- Export bulk performance data

- Change how performance data is archived

✎ **Note**   Performance data related to trunk groups and SS7 can only be viewed if the BAMS is deployed.

What Is Monitored

Most devices in the Cisco PGW 2200 Softswitch node have a set of attributes whose performance statistics can be monitored. Depending on the type of device, performance data is collected in one of two ways:

- Cisco MNM collects performance data from the network devices by polling SNMP data. This is called *performance polling.*

- Cisco MNM retrieves performance data for the active Cisco PGW 2200 Softswitch host signaling and trunking components (also known as the Cisco PGW 2200 Softswitch host configuration) by retrieving flat files generated by the host and the BAMS. This is called *configuration polling.*

✎ **Note**   SNMP data can be viewed only in raw, not summarized, form.

Table 7-1 lists the Cisco MNM-managed elements, devices and subcomponents for which performance data is collected. Of these, most can have data displayed in either raw or summary form (column 2). For those with SNMP data, only raw data can be viewed (column 3). Some elements are supported only by Cisco PGW 2200 Softswitch Release 9, as indicated.

Tip Specific performance measurements are in Appendix B, "Performance Measurements Reference." If you are viewing the document online, you can click the page number in the first column to go to the performance measurements list for that element type.

Note See Chapter 1, "Overview of Cisco Media Gateway Controller Node Manager," "How Cisco MNM Models the Network" section on page 1-9 for information about supported elements.

Table 7-1   Elements with Performance Data

Element Types with Performance Data	Raw or Summary Data	Raw Data Only
Cisco BAMS (Appendix B, page 7)	X	—
Cisco PGW 2200 Softswitch host (Appendix B, page 4)	X	—
Cisco ITP-L (Appendix B, page 8)	X	—
Cisco LAN switch (Appendix B, page 8)	X	—
Cisco 2900 LAN switch port (Appendix B, page 8)	—	X
Cisco 5500 and 6509 LAN switch ports	—	X
HSI Adjunct, BAMS and Cisco PGW 2200 Softswitch system components (Appendix B, page 11)	—	—
Fixed disk (Appendix B, page 11)	—	X
RAM (Appendix B, page 12)	—	X
Processor (Appendix B, page 11)	—	X
Virtual memory (Appendix B, page 12)	—	X
Interfaces (Appendix B, page 10)	—	—
Serial (Appendix B, page 10)	—	X
TDM (ITP-L only)	—	X
Ethernet (Appendix B, page 10)	—	X
Generic (Appendix B, page 10)	—	X
Signaling & Trunk Group Components (Appendix B, page 12)	—	—
Adjacent point code	X	—
C7 IP link	X	—
Network card or adapter	X	—
CAS path (Release 9)	X	—
Point code	X	—
EISUP path	X	—
Ethernet interface	X	—

Table 7-1   Elements with Performance Data (continued)

Element Types with Performance Data	Raw or Summary Data	Raw Data Only
FAS path	X	—
IP FAS path	X	—
IP link	X	—
Linkset	X	—
MGCP path	X	—
NAS path	X	—
SGCP path	X	—
SIP link (Release 9)	X	—
SIP path (Release 9)	X	—
TDM link	X	—
Trunk group	X	—

Note   Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, ITP-L will replace SLT in publications and the product.

Cisco MNM does not collect performance data for the following device types:

- Loopback interface for Cisco PGW 2200 Softswitch, HSI server, or BAMS
- Cisco ITP-L SS7 MTP2 Channels
- Signaling components:
  - D-channel backup
  - TCAP IP path
  - SS route
  - SS7 subsystem
  - Signaling Gateway and Signaling Gateway Pair
  - SS7 signal path to Signaling Gateway Pair
  - SS7 Signaling Gateway Subsystem

Monitoring Network Performance

Monitoring network performance involves three basic tasks:

Task 1. Select the devices to poll and the polling frequency for each one.

Task 2. Start polling.

Task 3. View performance data using the Performance Manager.

See the following sections for more information.

Task 1. Setting Performance Polling Frequencies

You can specify a different polling frequency for each device type. All devices of that type and all components of such devices will have the same polling frequency. For example, if you set a 10 minute polling frequency for one Cisco ITP-L in the network, the frequency is applied to all Cisco ITP-Ls in the network and to all monitored elements on the Cisco ITP-L, such as the TDM interfaces.

For the Cisco ITP-L and Cisco LAN switch, the polling frequency is set at the device level. All components of the device have the same polling frequency as the parent device. For example, setting a frequency of every 10 minutes for a Cisco ITP-L also polls its TDM interfaces every 10 minutes.

Note The polling frequency you set in the Cisco PGW 2200 Softswitch host determines how often the host generates flat files that contain performance data on signaling and trunk group components. Do not set the polling frequency in Cisco MNM to be less (more frequent) than the Cisco PGW 2200 Softswitch host polling frequency, but you can set a greater interval (less frequent) in Cisco MNM if you do not want to process all the performance files generated. For example, you can set Cisco PGW 2200 Softswitch host performance data collection to every 20 minutes.

Default polling frequencies are

- Every 5 minutes for performance polling
- Every 15 minutes for configuration polling (signaling and trunking components)

For SSH-enabled components (defined as the Security Policy at deployment or in the Accounts dialog box), polling uses SSH.

Note Both the active and standby Cisco PGW 2200 Softswitch hosts should be polled to prevent loss of performance data if a Cisco PGW 2200 Softswitch host failover occurs.

Use the following procedure to set or change a polling frequency:

Step 1 In the Map Viewer window, right-click the desired device, and choose **States**.

Note For the Cisco PGW 2200 Softswitch host, including Cisco PGW 2200 Softswitch node signaling or trunking components, select the Cisco PGW 2200 Softswitch Host object.

Note If the **States** option is not available, select the parent device.

The States dialog box opens.

Step 2 Set the desired polling frequency:

- For any of the Cisco PGW 2200 Softswitch node devices, including the Cisco PGW 2200 Softswitch host, HSI server, and the BAMS system components, set the Performance Polling frequency.

- For the Cisco PGW 2200 Softswitch node signaling and trunking components, set the Configuration Polling frequency.

- Select the minutes or hours option from the pull-down menu. For all devices and types of polling, the minimum frequency is 1 minute and the maximum is 24 hours.

Note
- Setting the auto-start polling option ensures that if a new device of this type is deployed, it begins polling immediately without you having to turn polling on. See Chapter 5, "Deploying Your Network in Cisco MNM" for more information.

- For information on Auto-Discovery polling, see Chapter 5, "Deploying Your Network in Cisco MNM," "Synchronizing the Cisco MNM with Device Changes" section on page 5-20. Status polling checks the device status, such as up, down, active, or standby, as shown on the Status tab of the Properties dialog box for the device. For more information, see Chapter 6, "Managing Faults with Cisco MNM," "Task 1. Adjusting Status Polling Settings If Needed" section on page 6-3.

Step 3 Go to "Task 2. Starting Polling On a Network Element" to start polling at the selected frequency.

Task 2. Starting Polling On a Network Element

You can enable performance polling on an individual network element (a device or a component of a device) or on all the elements in a Cisco PGW 2200 Softswitch node. For polling to be enabled, the parent device must be in the normal (commissioned) state. Enabling polling places the device into the polling state.

Note For information on commissioning and decommissioning devices, see Chapter 6, "Managing Faults with Cisco MNM," "Commissioning, Decommissioning, and Rediscovering Devices" section on page 6-23.

For the Cisco ITP-L and Cisco LAN switch, polling is turned on or off at the device level. Polling is enabled or disabled for all components of the device along with the parent device. For example, starting polling on a Cisco ITP-L starts polling on its TDM interfaces.

Use the following procedure to start polling on one or more network elements:

Step 1 In the Map Viewer, do one of the following:

- For an individual element, right-click the desired object, and choose **States**.

- For all the devices in a Cisco PGW 2200 Softswitch node, under MGC-Node-View, right- click the desired node, and select **MGC Node States**.

The States dialog box opens.

Note
- If the **States** option is not available, select the parent device.

- For the Cisco PGW 2200 Softswitch host, including Cisco PGW 2200 Softswitch node signaling or trunking components, select the Cisco PGW 2200 Softswitch host object.

Step 2 Click **Start Polling**. You are prompted to confirm the operation.

Step 3 Click **Yes**.

If you want to stop performance polling later, access this dialog again, and click **Stop Polling**.

During polling, a polling symbol appears just above the object icon in the Map Viewer, as shown in Figure 7-1.

Figure 7-1   Map Viewer Icon of ITP-L TDM Interface in Polling State

Note See Chapter 3, "Getting Started with Cisco MNM," "Viewing Cisco MNM Status Information" section on page 3-9 for more on status symbols.

Step 4 Go to the "Task 3. Viewing Performance Data" section on page 7-7.

Task 3. Viewing Performance Data

Once you set the polling interval and start performance polling for an element, you can view the data collected in the Performance Manager.

From the Performance Manager window, you can:

- Identify and view data for all monitored attributes on a selected managed element.
- Identify and modify the summary intervals and rules, if any, configured for selected monitored attributes.
- View historical performance data over a requested period of time (in tabular or graphical format).
- Print performance data to a printer or file.
- Export the displayed performance data to a file.

Note Because of constraints imposed by the BAMS, the trunk group performance data is not reported in real time and might be delayed for up to 45 minutes. For details, refer to the BAMS documentation.

Use the following procedure to view performance data:

Step 1 In the Map Viewer window, right-click the desired object, and choose **Tools > Performance Manager**.

Note • You can also open the Performance Manager by right-clicking an object in the Event Browser or the Object Manager.

- If the **Performance Manager** option is not available, performance data is not collected for the selected element. Try navigating down a level to a component that may be monitored.

The Performance Manager window opens. The window title bar shows the name of the selected object. For details on the window, see the "About the Performance Manager Window" section on page 7-10.

Step 2   From the Monitored Attributes list, select the attribute whose data you want to view.

> **Note**   Select a range of multiple attributes in a list by holding down the **Shift** key and selecting attributes in the list. 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, with a column for each attribute. Only the first selected attribute is shown in the line chart or bar chart.

Step 3   (Optional) Modify the Time Period settings to display data collected between a specified start and end date.

Step 4   (Optional) By default, data is presented in raw (unsummarized) form. To view summary data instead:

- From the Interval pull-down menu, select a summary interval. The summary interval is the period of time over which the summary rule is applied. Options vary according to the attribute selected.

> **Note**   If polling has begun during the last day, selecting an interval of a day results in no data being displayed.

- (If a summary interval is selected) From the Rule drop-down menu, select the summary rule to be used. The default summary rule is one day (24 hours).

Step 5   Click **Refresh** to display data for the selected attribute.

> **Note**   The Refresh button is dimmed when there is nothing to refresh. Refresh is available 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 clicking the mouse.

Step 6   Click the **Line Chart**, **Bar Chart** (if available), or **Table Display** tab to view your data in the desired format.

Step 7   For details on reading and manipulating the Performance Manager display, go to the "About the Performance Manager Window" section on page 7-10

.

Updating the Performance Manager Display

To update the data display after changing the time period, summary interval, View menu options, or attribute, click **Refresh**.

> **Note**   If you have stopped polling on a device, to update the data you must start polling again, and then click **Refresh**.

Performance Manager Usage Examples

Here are two examples using performace manager to view host performance data like UDP/TCP related information and view Cisco PGW 2200 Softswitch node performance data like CALL: SuccCall TOT/CALL: FailCall TOT.

To view host performance data like UDP/TCP information, right-click the host whose data you want to view in Host-View of Map Viewer. Select Tool>Performance Manager and select the attribute you want to view in the Monitored Attributes. Adjust the Time Period and Summary if needed and click Refresh.

UDP In Datagrams information displays in the window like the one shown in Figure 7-2.

Figure 7-2   UDP In Datagrams Display in Performance Manager Window
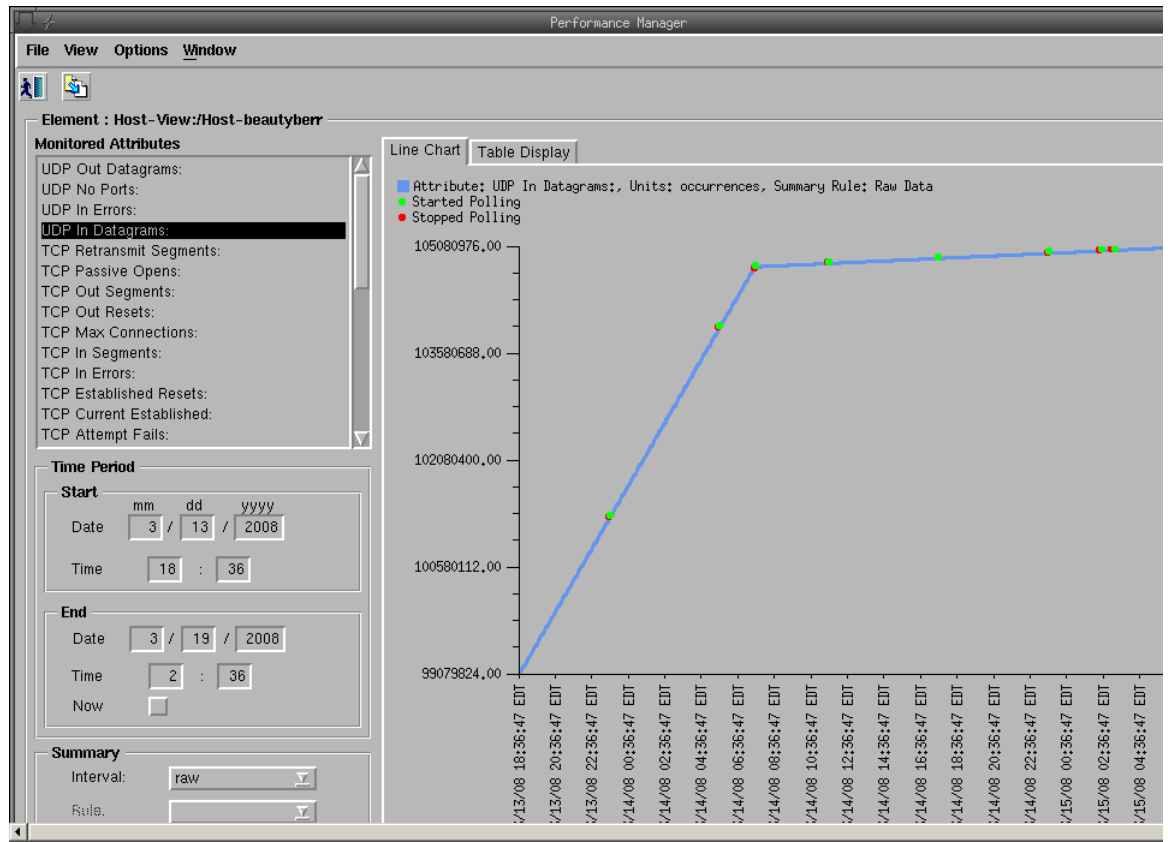
To view Cisco PGW 2200 Softswitch node performance data like call-related information, right-click the Cisco PGW 2200 Softswitch node whose data you want to view in MGC-Node-View of Map Viewer. Select Tool>Performance Manager and select the attribute you want to view in the Monitored Attributes. Adjust the Time Period and Summary if needed and click Refresh.

CALL: SuccCall TOT information displays in the window like the one shown in Figure 7-3.

Figure 7-3   CALL: SuccCall TOT Display in Performance Manager Window
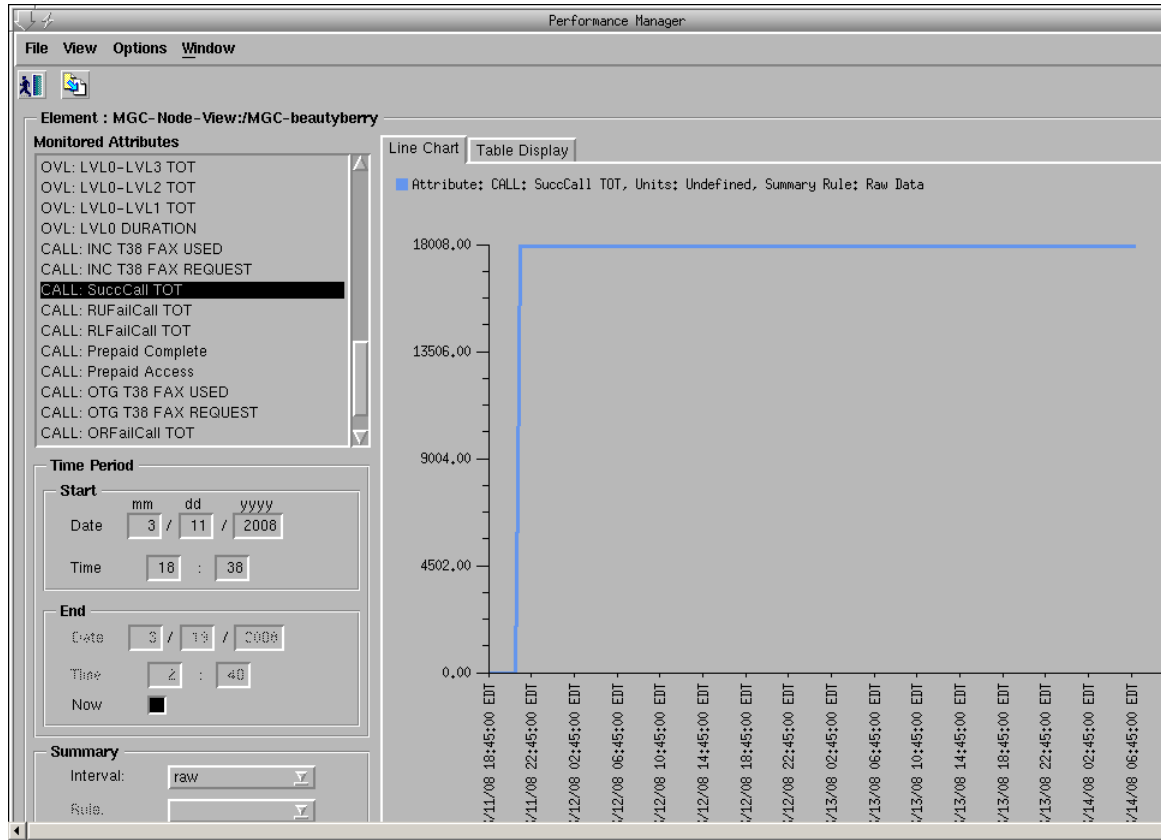
About the Performance Manager Window

When you open the Performance Manager, a window displays like the one shown in Figure 7-4.

Figure 7-4   Performance Manager Window
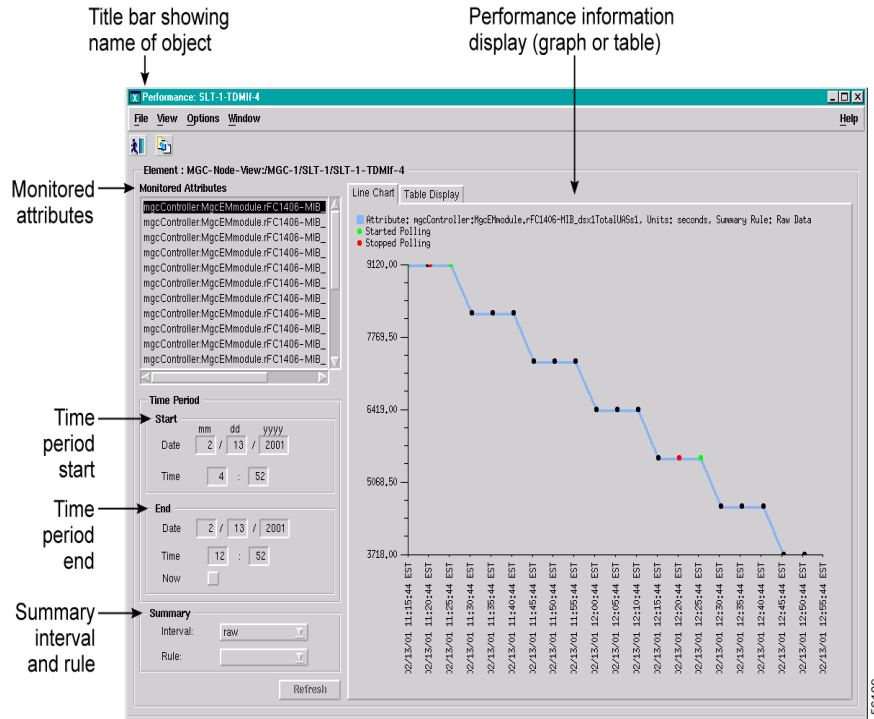
Monitored Attributes

The Monitored Attributes list displays the performance counters for the selected device. Initially, the first attribute in the list is selected. The performance information for the selected attribute is displayed in the right panel. To view the performance of another attribute, select the attribute, and click **Refresh**. You can select multiple attributes by pressing **Ctrl** and clicking individual attributes.

See Appendix B, "Performance Measurements Reference," for details on attributes monitored for the various Cisco PGW 2200 Softswitch node devices.

Performance Information Display

Line charts, bar charts, and tables: You can view the data for most attributes in a line chart or table. Summarized data can also be viewed in a bar chart.

Line charts plot one single attribute at a time (the attribute currently selected in the Monitored Attributes list). Time is plotted on the horizontal axis, and the count is plotted on the vertical axis (see Figure 7-5).

Bar charts show comparisons of summarized data over time, such as totals for week 1 and totals for week 2.

Tables can display data for multiple attributes. The data for each attribute is shown in its own column. Each cell in the column displays the value of one data interval (see Figure 7-6).

Figure 7-5   Sample Line Chart
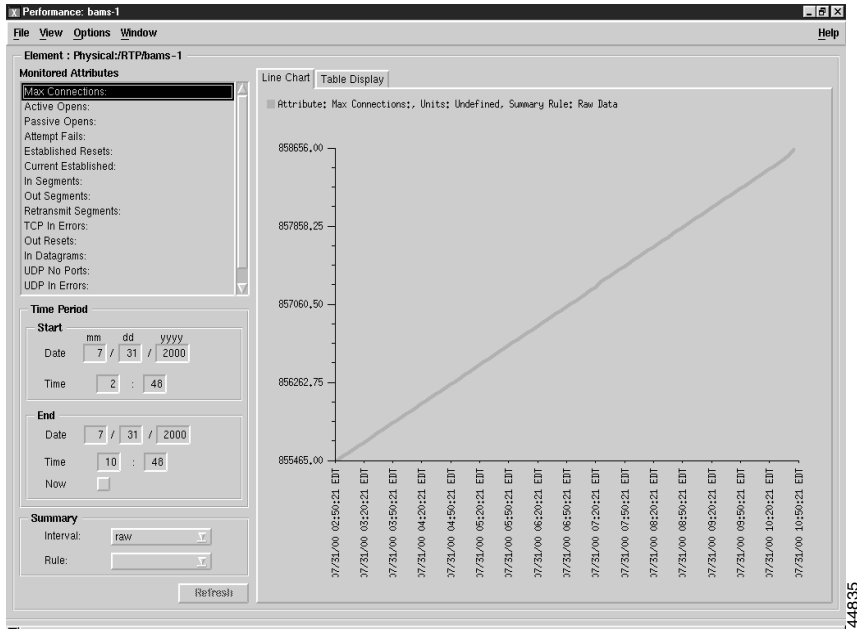
Figure 7-6   Sample Table
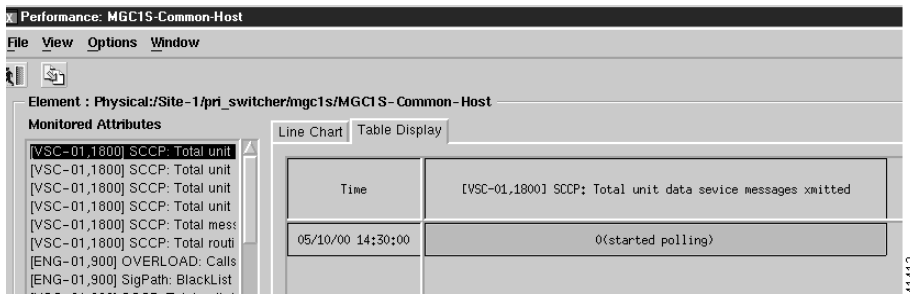
Color-code key: As the key at the top of the display shows, the colored dots (in line charts) or cells (in tables) indicate these events in data collection:

- Green indicates when performance polling started.
- Yellow indicates that a poll for an attribute was missed.
- Red indicates when performance polling stopped.

View options: In a line or bar chart, the View menu allows you to display additional information on the chart by selecting:

- Values—Plots the values of the samples collected
- Points—Plots the time that the samples were collected, marking each data point with a black dot

Tip If values are displayed on a chart, zooming in one or two levels helps make the values readable.

Time period start and end

- Start Date—The date to start displaying data (in the format *mm/dd/yyyy)*.

- End Date—The date to stop displaying data. Alternatively, for End Date, you can select the **Now** check box to view the data from the selected start date to the present date and time.

> **Note** The Now option is dynamic. Selecting **Now** at 10:30 p.m. displays all available data between the start date and time and 10:30 p.m. Selecting Now at 11:00 p.m. displays all data through 11:00 p.m. Use **Now** to view the latest data.

- Start Time—The time from which you want to display data. Use 24 hour format.

- End Time—The time to which you want to display data. If you selected **Now** for End Date, you do not need to specify an End Time.

> **Note** The default start date and time is the current date and time minus 8 hours. The default end date and time is the time when you open the Performance Manager.

Summary

By default, data is displayed in raw (unsummarized) form. For most network elements, you can also view summarized data. Where you want to inspect performance over time, a summary view is typically more meaningful. 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 value summaries of the data. Managing the network is facilitated by being able to summarize data in hourly, daily, or weekly intervals

> **Note** Data for some network elements can be viewed only in raw, not summarized, form. See Table 7-1 on page 7-3 for a list. When raw is selected, the Bar Chart view is not available, and the Summary Rule option is dimmed.

Summary interval: Select raw or, for a summary, the desired interval:

- Hourly summaries are generated on the hour.

- Daily summaries are generated at midnight.

- 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 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 attribute summaries have the same timestamps.

> **Note** In the above example, data generated between 9:30 and 10:00 is ignored An hourly summary for 9:00 to 10:00 would be misleading, because it would have been generated using only half the usual number of values.

Summary rule: If you selected a summary interval, choose the way you want the data summarized:

- Total—Adds 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.

Refresh button

Click **Refresh** to update the display with the most current data or to update the display after changing the time period, summary interval, View menu option, or the attribute selected.

The Refresh button is dimmed when there is nothing to refresh. Refresh is available 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 clicking the mouse.

Navigating in the Performance Manager

You can zoom in, zoom out, and move around the displayed charts by using the keys and mouse buttons described in Table 7-2.

Table 7-2   Chart Viewing Actions

Press	Action
Shift-click	Selects multiple blocks of attributes in a list.
Ctrl-click	Selects multiple attributes in different areas of 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.

Use the following procedure to zoom in or out in a chart:

Step 1   Click and drag the left mouse button to select the area you want to zoom, as shown in Figure 7-7.

Figure 7-7   Selecting an Area to Zoom
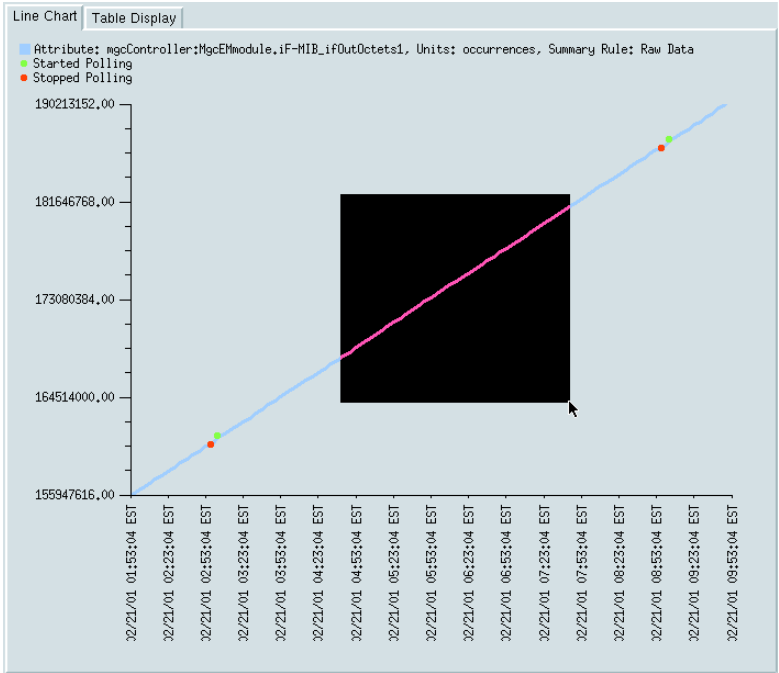
Figure 7-8 shows the results of zooming in two levels and turning on the view of data values.

Figure 7-8   A Zoomed Line Chart with Values On
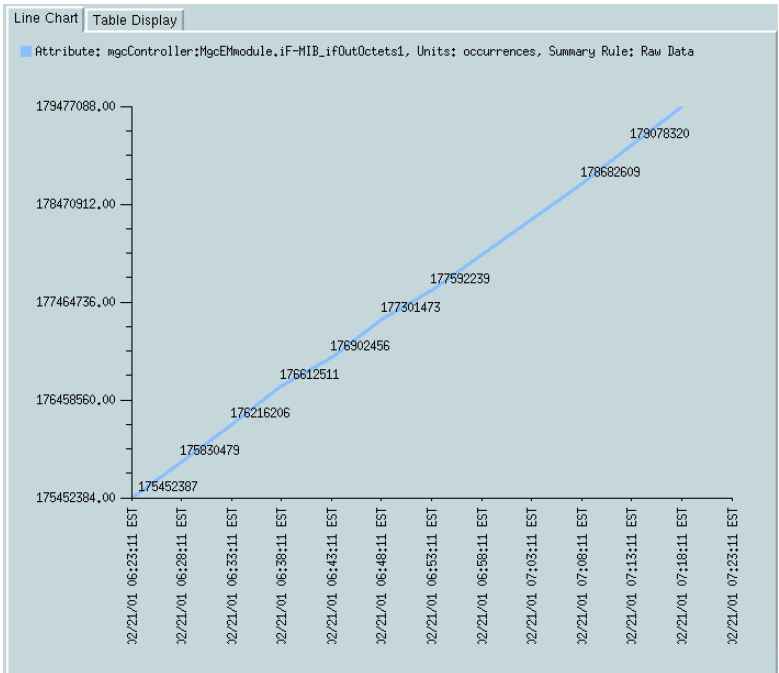
Step 2   To return to the previous zoom level, click the middle mouse button.

Exporting the Currently Displayed Performance Data

You can export performance data in two ways:

- Using the File command in the Performance Manager, you can create an ASCII file containing the performance data currently displayed (data for the selected object and specified time period). This procedure is covered in this section.

- Using the **historyAdmin expor**t command, you or a northbound system can generate files that contain bulk performance data for all objects in the network over a given number of days. See the "Exporting Bulk Performance Data" section on page 7-19.

The data file can be brought into another application for analysis.

Use the following procedure to create a file containing the currently displayed data:

Step 1   Open Performance Manager on the object for which you want to export performance data.

Step 2   Select **File > Export To File** or click [icon]. The File Chooser dialog box opens.

Step 3   Enter the name and path for the file, and click **Apply**. A file is created containing the currently displayed performance data.

> **Note**   By default, the file is saved in the *<CEMF_ROOT>*/bin/performanceMgr.sysmgr folder. Select a different path to save the file to a different location.

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 performance statistics in plain text format.

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

Use the following steps to print a performance file:

Step 1   Open the Performance Manager and select the desired attribute or attributes.

Step 2   From the **File** menu, select **Print**. Choose either **As Chart** or **As Table**. If you selected multiple attributes, choose **As Table**.

Selecting What To Monitor

Intelligent performance management requires that you understand which attributes are the critical indicators of performance for various network elements and which areas of your particular network are likely to have the greatest impact on performance for your users.

Before using the Performance Manager, identify what you want to know so that you can focus on a manageable set of indicators. As you gain experience with the Cisco PGW 2200 Softswitch node and with Cisco MNM, you can add to or refine your lists of monitored attributes for key performance factors.

To help you get started, this section presents examples of attributes you might monitor for several network elements. These lists are offered as examples only and are not intended as recommendations.

Note   The measurements list presented here is not a complete list of counters for monitoring performance. For comprehensive performance, other attributes should be monitored.

SS7 Monitoring Example

See the example attributes in Table 7-3 for information on monitoring SS7 performance.

Table 7-3   SS7 Monitored Attributes (An Example)

Network Element	Measurement Group	Counter	Description
C7 IP Link	C7Link (SS7 Link statistics)	C7LNK: DUR UNAVAIL	Duration unavailable (in seconds)
		C7LNK: MSU DROP-CONG	Total messages dropped due to congestion
Point Code	C7SP (SS7 Signal Path statistics)	C7SP: SP DUR UNAVAIL	Duration unavailable
		C7SP: XMIT MSU DROP/RTE	Total number of messages dropped due to routing failure
Point Code	ISUP	ISUP:XMIT CGB TOT	Circuit group blocked msgs transmitted
		ISUP:RCV CGB TOT	Circuit group blocked msgs received
		ISUP:XMIT CGU TOT	Circuit group unblocked msgs transmitted
		ISUP:RCV CGU TOT	Circuit group unblocked msgs received
If you are using Blacklist features, also monitor the following:			
Signaling Service	SP (Signaling Service statistics)	SP:Blacklist Call Ctr	Number of blacklist calls

System Administration for Performance Management

This section is designed for system administrators. It describes the following procedures related to administration of Cisco MNM performance management:

✎
Note   For more information on system administration related to performance management, see "Performance
Data Storage" in the *Cisco Element Management Framework Installation and Administration Guide* at
http://www.cisco.com/en/US/docs/net_mgmt/element_manager_system/3.2/installation/guide
/install_1.html.

Filtering Measurements Collected by Cisco MNM

Cisco MNM predefines the performance measurements collected on SNMP-managed devices and
processes whatever data is available. For measurements on signaling and trunking components
(Cisco PGW 2200 Softswitch host configuration), the Cisco PGW 2200 Softswitch host writes out flat
files containing the data. You can use measurement filters to collect a subset of configuration
measurements.

Use the following procedure to filter measurements for SNMP-managed elements:

Step 1   Edit the **measFilters** file in ***<CEMF_ROOT>*/config/hostController**. This file, read at startup,
determines what measurements are retrieved from the Cisco PGW 2200 Softswitch-generated flat files.
The following illustrates the format of the measurement filter files:

Measurement Name, *|*Component Name*

Where the variables are those defined in Table 7-4.

Step 2   Insert a pound sign (#) at the beginning of the line you want to comment out.

Step 3   For the change to take effect, stop and restart Cisco EMF.

Table 7-4   Cisco MNM Measurement Filters

Parameter	Description
Measurement name	Any measurement specified in the Cisco PGW 2200 Softswitch host measCats.dat file.
Component name	Any MML component specified in the Cisco PGW 2200 Softswitch host components.dat file. An asterisk (*) matches all components.

Changing Performance Thresholds

If you want to check or change performance thresholds on the Cisco PGW 2200 Softswitch host, HSI
server, and the BAMS, you must use MML to set the thresholds on the device itself.

Use the following procedure to access the device from Cisco MNM:

Step 1 In the Map Viewer window, right-click the device and choose **Tools > Connection Service**.

A Telnet or ssh window opens, depending on your security policy.

Step 2 Change the desired performance thresholds.

Step 3 For information on using MML commands with the Cisco PGW 2200 Softswitch host, refer to the *Cisco PGW 2200 Softswitch Release 9 MML Command Reference.*

For information on the BAMS, see "Setting up Disk Monitoring Thresholds at

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/bams/3.30/guide/330ch2.html

Exporting Bulk Performance Data

Cisco MNM allows exporting performance data in two ways:

- Using the **historyAdmin export** command, you or a northbound system can generate files that contain bulk performance data for all objects in the network over a given number of days. Instructions are provided in this section.

- Using the File command in the Performance Manager, you can create an ASCII file that contains the performance data currently displayed (data for the selected object and specified time period). See the "Exporting the Currently Displayed Performance Data" section on page 7-16.

The data file can be brought into another application for analysis.

$\begin{aligned}&\mathrel{\rlap{\hspace{0.2em}\raise0.1em\hbox{$\nwarrow$}}}\end{aligned}$

Tip Because performance data is not archived indefinitely, you may want to export data before it is deleted from the archive database. See the "Changing How Performance Data Is Archived" section on page 7-20 for details on archiving.

Use the following procedure to export data about the entire monitored network:

Step 1 (Optional) Change the export settings:

- Modify the file **<CEMF_ROOT>/bin/historyAdmin** to set the desired starting and ending date and time, summary interval, and rule if appropriate.

Step 2 Create the file:

- Enter the cemf shell:

    /<CEMF_ROOT>/bin/cemf shell

    The message "Running bin/sh" appears and the Cisco MNM command prompt appears:

    CEMF Manager >

- At the command prompt, enter the command **/opt/cemf/bin/historyAdmin export**.

- export <filename> <separator> <max file size (KB)> [all | <number_of_days>] <criteria name> ... (where *filename* is the name of the file to be created).

Note - For a list of all available criteria names, enter the following command:
    <CEMF_ROOT>/bin/historyAdmin list.

- A northbound system can use Telnet or another facility to access the Cisco MNM server.

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>
```

A sample file looks like:

```
> historyAdmin export dumpFile TAB 10 all criteria1
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
```

Changing How Performance Data Is Archived

Cisco MNM stores performance data in a database that is periodically purged so that it does not grow indefinitely. You can change how long data is stored before purging and specify roll-up rules and other actions that should be taken on performance data after a set length of time.

The attributeHistoryServer.ini file, described in Table 7-5, controls the behavior of the performance purging mechanism. These are the default settings:

minValueCount   = 50
maxValueCount   = 1000
minRawDataAge   = 60

These values can be modified using the historyAdmin utility. Because the settings have a significant effect on database size, performance, and overall disk requirements, take care when changing these parameters.

Table 7-5   attributeHistoryServer.ini file Attributes

Parameter	Description
minValueCount	Specifies the minimum number of values for each sample. Data is never removed from a sample if doing so would result in that sample having fewer than the minimum number of values. This value is set to 50 on a standard Cisco EMF 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 Cisco EMF installation. For example, if the system has just received 100 changes to an attribute in the 40 seconds preceding a purge, the last 100 values are kept, and not just the last 50.
maxValueCount	Specifies the maximum number of values to be kept for each sample. Whenever this number 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 Cisco EMF installation.

Note   In some cases, these 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 specifies 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.

For information on configuring how alarms are stored and deleted, see the Chapter 6, "Managing Faults with Cisco MNM," "Specifying the Length of Time Alarms Are Stored" section on page 6-27.

Other Network Management Tasks

Revised: December 15, 2009, OL-18339-03

This chapter provides information on the following:

Performing Routine Network Management

This section presents checklists of routine procedures for network management using Cisco Media Gateway Controller (MGC) Node Manager (MNM). Because Cisco MNM is used in many different types of situations, no single checklist can describe optimal procedures for all cases. This information is designed to guide you with your own management routines, tailored to your particular network and users.

Note Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, ITP-L will replace SLT in publications and the product.

Procedures for Getting Started

Task	Steps
Install Cisco EMF and Cisco MNM (system administrator).	See the Cisco MNM Installation Guide.
Configure network devices for management (system administrator).	See Chapter 2, "Configuring Network Devices for Management".
Set up security (system administrator).	See Chapter 4, "Setting Up Cisco MNM Security".
Deploy the network, creating a model of your network in Cisco MNM.	See Chapter 5, "Deploying Your Network in Cisco MNM".
Identify key performance measurements to monitor.	See Chapter 7, "Managing the Performance of Cisco MNM Devices," "Selecting What To Monitor" section on page 7-16.
Set up threshold crossing alerts and scoreboards.	See Chapter 6, "Managing Faults with Cisco MNM," "Task 2. Customizing Event Management" section on page 6-4.

Routine Daily Procedures

Task	Steps
(Ongoing) Monitor the network for changes in status.	1. At the top level of the Map Viewer, monitor changes. 2. When you see an alarm, drill down to find where the problem occurred. 3. Right-click the device object and choose **Tools > Event Browser** to view details on the alarm. 4. Click **Acknowledge** for this event to indicate that the problem is being investigated. See Chapter 6, "Managing Faults with Cisco MNM," "Using the Event Browser to Manage Events" section on page 6-9 for details. After identifying the alarm, use diagnostics to diagnose the problem. See the "Using Diagnostic Tools" section on page 8-65.

Task	Steps
If the network is not monitored continuously, look at alarms that came in overnight, specifically: • Active alarms • Alarms that were received and cleared, including alarms cleared automatically • Destination in service alarms, such as PRIs or SS7s • Switchovers from standby to active status Work from the most severe alarm to the least severe.	Investigate active alarms as described in the previous task. Alternatively, in the Map Viewer, right-click the Cisco PGW 2200 Softswitch host object and choose **Properties**, and then click the **Software** tab. See the "Viewing Properties for Devices" section on page 8-9 for details.
Check the health of the devices assigned to you: • Are they in service? • Are they reachable using ping? • Is the device communicating with Cisco MNM?	If you cannot access a device, in the Map Viewer, right-click the device object, and choose **Tools > [Device name] Diagnostics**. On the General tab, click **IP Ping** or **SNMP Ping**. See the "Using Diagnostic Tools" section on page 8-65 for details.
Check the amount of disk space available on the Cisco PGW 2200 Softswitch host. Pay special attention to root (**/**) and **opt** directories.	Monitor the file system. In the Map Viewer, right-click the Cisco PGW 2200 Softswitch host object and choose **File Systems**. See the "Monitoring Cisco PGW 2200 Softswitch Host, the Cisco HSI Server, and the Cisco BAMS File Systems" section on page 8-19 for details.
Check the amount of virtual memory available on the Cisco PGW 2200 Softswitch host.	In the Map Viewer, right-click the Cisco PGW 2200 Softswitch host object and choose **Devices > Virtual Memory Properties**. See the "Viewing System Component Properties" section on page 8-22 for details.
Check the status of trunks.	Check status: In the Map Viewer, right-click the Trunking folder and choose **Properties**, and then click the Status tab. Verify trunk group: In the Map Viewer, right-click the BAMS and choose **Properties**, then click the Status tab.
Check CPU usage on the Cisco PGW 2200 Softswitch host.	In the Map Viewer, right-click the Cisco PGW 2200 Softswitch host object and choose **Devices > Processor Properties**. See the "Viewing System Component Properties" section on page 8-22 for details.

Task	Steps
Check the number of processes running on the Cisco PGW 2200 Softswitch host. Generally, there should not be more than 60 to 70 processes running.	To see the number of processes: In the Map Viewer, right-click the Cisco PGW 2200 Softswitch host object and choose **Properties**, and then click the Software tab. The number of processes is displayed at the bottom of the dialog box. See the "Viewing Properties for Devices" section on page 8-9 for details. To view the status of processes: In the Map Viewer, right-click the device object and choose **Tools > MGC Host Diagnostics**. On the General tab, click **Process Status**. See the "Using Diagnostic Tools" section on page 8-65 for details.
Check the number of users on the Cisco PGW 2200 Softswitch host.	In the Map Viewer, right-click the Cisco PGW 2200 Softswitch host object and choose **Properties**, and then click the **Software** tab. See the "Viewing Properties for Devices" section on page 8-9 for details.
Cisco ITP-Ls: Check memory used and RAM.	In the Map Viewer, right-click the Cisco ITP-L object, choose **Properties**, and then click the **Memory** tab. See the "Viewing Properties for Devices" section on page 8-9 for details.
For traffic engineering.	Look at trunk group measurements to identify when the network is reaching circuit capacity.
(As needed) Deploy new devices and delete obsolete devices.	See Chapter 5, "Deploying Your Network in Cisco MNM."

Routine Weekly Procedures

Task	For More Information, see
Analyze measurement data for trends: 1. Export desired performance data. 2. Import the data into an external measurement report and analysis tool such as Trinogy Trend.	Chapter 7, "Managing the Performance of Cisco MNM Devices," "Exporting Bulk Performance Data" section on page 7-19

Using Cisco MNM To Launch Device Configuration

From Cisco MNM, you can launch configuration tools for the Cisco PGW 2200 Softswitch node devices. Specifically, you can launch

- The Cisco Voice Services Provisioning Tool (VSPT) to configure the Cisco PGW 2200 Softswitch host.

Note   The Voice Services Provisioning Tool (VSPT) was formerly known as MNM-PT.

- CiscoView to configure the Cisco ITP-L and Cisco LAN switch
- Telnet or an X terminal window to use MML, UNIX, and OSI commands. If SSH is enabled on Cisco MNM and the target device, SSH is used instead.

Launching Configuration Tools

You can launch configuration tools for various devices from the Cisco MNM Map Viewer, as shown in Table 8-1.

Table 8-1   *Configuration Tools for Cisco PGW 2200 Softswitch Node Devices*

Cisco PGW 2200 Softswitch Node Device	Available Tools
Cisco PGW 2200 Softswitch host	Cisco VSPT or Cisco MNM Telnet or ssh; MML
Cisco BAMS	Telnet or ssh; MML
Cisco HSI server	Telnet or ssh; MML
Cisco ITP-L	CiscoView Telnet or ssh
Cisco LAN Switch	CiscoView Telnet or ssh

Use the following procedure to launch a configuration tool:

Step 1   In the Map Viewer window, right-click the device you want to configure, and choose **Tools**.

Step 2   From the **Tools** menu, choose one of the following:

- **Voice Services Provisioning Tool** to configure the Cisco PGW 2200 Softswitch host

> **Note**   The Voice Services Provisioning Tool option is only available when the Cisco VSPT is installed. To get more information on Cisco VSPT installation, see Chapter 2, "Installing Cisco VSPT" in the *Cisco Voice Services Provisioning Tool User Guide.*

- **CiscoView** to configure the Cisco ITP-L and Cisco LAN switch

The application opens.

> **Note**   The Cisco PGW 2200 Softswitch deployment user ID and password are passed to Cisco VSPT and you are logged in with the privileges assigned to that user: read-write or read-only. If there is no deployment user ID and password, the Cisco VSPT opens to the log in window, and you must log in manually.

Step 3   Perform the desired configuration.

Step 4   Close the application when you are done.

Use the following procedure to launch a Telnet session (or ssh, if SSH is enabled) or an X terminal window to use UNIX, OSI, and MML commands:

Step 1   In the Map Viewer window, right-click the desired device, and choose **Tools**.

Step 2   From the **Tools** menu, choose **Connection Service**.

A Telnet, ssh, or X terminal window opens, and you are connected to the selected device.

Step 3   Enter MML commands, or perform other desired operations.

Step 4   Close the window when you are done.

Viewing or Modifying Account and SNMP Information

You can view the account and SNMP information that resides in the Cisco MNM database for any of the following Cisco PGW 2200 Softswitch node devices:

- Cisco PGW 2200 Softswitch host
- Cisco BAMS
- Cisco ITP-L
- Cisco LAN Switch
- Cisco HSI server

Account information and SNMP read and write community strings are defined when a device is deployed. If the actual device information changes—for example, if a password is changed—you can modify it to update the Cisco MNM database. The changed information is used in device rediscovery.

Use the following procedure to view or change account or SNMP information in the Cisco MNM database:

Step 1   In the Map Viewer window, select the desired device or devices.

Note   Alternatively, if you have a Properties, States, Diagnostics, or File Systems dialog box open for the device, you can use the dialog box Navigation menu to open the Accounts dialog box.

Step 2   Right-click and choose **Accounts**.

The Accounts dialog box opens.

Step 3   If you have selected more than one device, choose the desired device in the list box on the left side of the dialog box.

Step 4   Check or change device information. See the "About the Accounts Dialog Box" section on page 8-7.

Step 5   If you make changes, click the toolbar **Save** button, or choose **File > Save**. The updated information is saved in the Cisco MNM database.

Step 6   In the Accounts dialog box, you can use the toolbar buttons or menu options to:

- Print the information on the current tab.
- Close the dialog box.
- Toggle dynamic update mode off and on.

- Refresh the window to update the information when dynamic update mode is off.
- Acknowledge that you have seen dynamically-updated changes.

You can use the Navigation menu to open the Properties, File Systems (where applicable), States, or Diagnostics dialog box for the selected component.

Note
- The status bar shows the current status of the device.
- If the account is locked (lock icon is closed), you do not have permission to view this information.

About the Accounts Dialog Box

The Accounts dialog box displays login and SNMP information for the selected network device. This information is used when the device is rediscovered. The Accounts dialog box contains the Accounts tab and the SNMP tab.

By default, the Accounts dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off, acknowledge that you have seen updated information, and check for changes when dynamic updating is off.

The Accounts dialog box includes a Navigation menu that allows navigating directly to Properties, File Systems, States, or Diagnostics dialog boxes for the selected component, without having to reselect the component in the Map Viewer. See Chapter 3, "Getting Started with Cisco MNM," "Navigating between Dialog Boxes for a Given Component" section on page 3-31 for details.

Accounts Dialog Box Toolbar

The toolbar contains buttons for these functions:

- Close the current window.
- Print the contents of the window.
- Toggle dynamic update mode, to allow viewing or not viewing real-time changes.
- Refresh the window, to update the information when dynamic update mode is off.
- Acknowledge that you have seen dynamically updated dialog box changes.
- Save your changes to the Cisco MNM database.

Dynamic updates are displayed in blue. When an update occurs, the dialog box moves in front of other open Cisco MNM windows. Click **Acknowledge** to acknowledge that you have seen the changes to and remove the blue highlighting.

Accounts Tab

The Accounts tab contains the following fields:

Login ID—The login ID defined in the Cisco MNM database

Password—The password defined in the Cisco MNM database

Root or Enable Password—The root or enable super-user password defined in the Cisco MNM database

Security Policy—The security protocol used for communication with the device

- Choose SSH if you have installed the Cisco EMF SSH add-in and the device is SSH-enabled. With SSH support installed, all operations that previously used Telnet or FTP to communicate with network elements instead use ssh (the secure shell program, the SSH counterpart of Telnet) and sftp (secure FTP).

- Choose None for non-secure devices.

SNMP Tab

The SNMP tab contains the following fields:

Read Community—SNMP read-community string.

Write Community—SNMP write-community string.

Timeout (seconds)—The number of milliseconds the system attempts to connect remotely when performing an SNMP operation before timing out. The default value is 5000.

Retries—The number of times the system attempts to connect when performing an SNMP operation. The default value is 2.

Varbinds/Packet—The number of varbinds sent in a single packet to an SNMP agent. The default value is 5.

SNMP Version—The version of SNMP running on the device. Versions 1 and 2c are supported.

Viewing Properties for Devices and Their Components

You can view properties for any of the Cisco PGW 2200 Softswitch node devices and their components.

You can view properties for the following devices. See the "Viewing Properties for Devices" section on page 8-9.

- Cisco PGW 2200 Softswitch host
- Cisco BAMS
- Cisco HSI server
- Cisco ITP-L
- Cisco LAN switch

You can view properties for Serial, Ethernet, and TDM interfaces. See the "Viewing Properties for Interfaces" section on page 8-14.

You can view properties and monitor the usage of the Cisco PGW 2200 Softswitch host, Cisco HSI server, and the Cisco BAMS file systems. See the "Monitoring Cisco PGW 2200 Softswitch Host, the Cisco HSI Server, and the Cisco BAMS File Systems" section on page 8-19.

You can view properties for system components (disk partitions, processor, RAM, and virtual memory) of the Cisco PGW 2200 Softswitch host, the Cisco HSI server, and the Cisco BAMS. See the "Viewing System Component Properties" section on page 8-22.

You can view properties for the following Cisco PGW 2200 Softswitch node components:

- Signaling components. See the "Viewing Signaling Component Properties" section on page 8-24.
- Trunking components. See the "Viewing Trunk Group Component Properties" section on page 8-54.

All Properties dialog boxes share the basic functionality described in the following "Common Functionality in Properties Dialog Boxes" section on page 8-9.

Common Functionality in Properties Dialog Boxes

All Properties dialog boxes display dynamically updated information and provide similar functionality with the main functions accessible from a toolbar. If a Properties dialog box is opened for more than one component, a list box on the left side of the dialog box lists the available components. The Properties information applies to the selected component.

Properties dialog boxes include a menu where you can navigate directly to other dialog boxes for the selected component without having to reselect the component in Map Viewer. See Chapter 3, "Getting Started with Cisco MNM," "Navigating between Dialog Boxes for a Given Component" on page 31.

> **Note**   The specific properties you see depends not only on the network element you are inspecting but also on the release of the Cisco PGW 2200 Softswitch host software that you are using.

Properties Dialog Box Toolbar

In every Properties dialog box (see Figure 8-1), a toolbar contains buttons for these functions:

- Close the current window.
- Print the contents of the window.
- Toggle dynamic update mode, to allow viewing or not viewing real-time changes.
- Refresh the window, to update the information when dynamic update mode is off.
- Acknowledge that you have seen dynamically updated dialog box changes.

In addition, because the File System dialog box includes settings that you can modify to change how the file system is monitored, the File System Properties dialog box contains a Save button.

Dynamic updates are displayed in blue. When an update occurs, the dialog box moves in front of other open Cisco MNM windows. Click **Acknowledge** to acknowledge that you have seen the changes and to remove the blue highlighting.

Figure 8-1   Device Properties Dialog Box Toolbar

Viewing Properties for Devices

You can view properties for any of the following Cisco PGW 2200 Softswitch node devices. Property fields may vary.

- Cisco PGW 2200 Softswitch host
- Cisco HSI server
- Cisco BAMS
- Cisco ITP-L
- Cisco LAN switch

Use the following procedure to view properties for a device:

Step 1   In the Map Viewer window, select the desired device or devices.

Step 2   Right-click and choose **Properties**.

The Properties dialog box opens.

If you have selected more than one device, choose the desired device in the list box on the left side of the dialog box.

Step 3   Check device properties. See the "About the Device Properties Dialog Box" section on page 8-10 for details on properties.

Step 4   (Optional) In the Properties dialog box, use the toolbar buttons or menu options to manipulate the display.

Note   The status bar shows the current status of the device.

About the Device Properties Dialog Box

The Properties dialog box contains a toolbar and tabs displaying various categories of device properties. The contents of the tabs varies with the device type.

By default, the Properties dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off, acknowledge that you have seen updated information, and to check for changes when dynamic updating is off. All fields are display-only.

See the "Common Functionality in Properties Dialog Boxes" section on page 8-9 for more information.

General Tab

The General tab contains the following display-only fields:

- Management Address—Network management IP address.
- System Name—Administratively assigned name for the device.
- Location—Physical location of the device.
- Contact—Contact person or organization and brief contact information, such as phone number.
- (Cisco BAMS, Cisco HSI server, and Cisco PGW 2200 Softswitch only) System Status—Current operational status of the device. Values are Active, Standby, Outage, Error, and Other.
- Up-time—Time since the device was initialized.
- Description—Description of the device.

Details Tab

The Details tab contains the following fields:

For the Cisco PGW 2200 Softswitch, Cisco HSI server, and Cisco BAMS
- Hardware Model—Hardware model for the device.
- OS Version—Version of the operating system.
- OS Release—Release level of the operating system.

- Host ID—Host ID.

- Memory Size—Amount of physical main memory.

- System Date—Local time and day on the host.

- Last Boot Time—Time the machine was last booted.

For the Cisco ITP-L and Cisco LAN Switch

- Model—Chassis type.

- Chassis ID—Unique identifier for the chassis (Cisco ITP-L) or serial number (Cisco LAN switch).

For the Cisco ITP-L only

- Hardware Version—Chassis hardware revision level.

- ROM System Version—ROM system software version.

- ROM Monitor Version—ROM monitor version.

For the HSI server only

- Host Port-1—The first port number to be used by the Cisco HSI. The default value is 0.

- Host Port-2—The second port number to be used by the Cisco HSI. The default value is 0. This value should not be changed; it should always be set to 0.

> **Note**   This value must match the peer port setting on the Cisco PGW 2200 Softswitch EISUP IPLNK object.

For the Cisco LAN switch only

- Fan Status—Status of the fan. Values are OK, Other, Minor Fault, and Major Fault.

Details area

- System Type—Chassis system type.

- Backplane Type—Chassis backplane type.

Power Supply area

- Status (Primary and Secondary)—Power supply status. Values are OK, Other, Major Fault, and Minor Fault.

- Type (Primary and Secondary)—Type of power supply.

Host, HSI, or BAMS Tab (Cisco PGW 2200 Softswitch host, HSI server, or BAMS)

The Cisco PGW 2200 Softswitch Host or BAMS tab contains the following fields:

- In the **Call Agent**, **BAMS Software**, or **HSI Software** area, information about the software:

    - Host, BAMS Version, or HSI Version—Software version.

    - Patch Level—Patch level of the software.

    - (Cisco PGW 2200 Softswitch only) Host Vendor—Vendor of the host software.

    - Home Directory—Software home directory.

    - (Cisco PGW 2200 Softswitch only) Active Config Name—Name of the active MML configuration, if any.

- (Cisco PGW 2200 Softswitch only) Desired State—Desired state of the platform, such as standalone.

- (Cisco PGW 2200 Softswitch only) Switch Type—Switching configuration of the host.

- (Cisco PGW 2200 Softswitch only) Failover Peer Addresses A and B—IP address of each failover machine.

- (Cisco HSI server only)Primary MGC—In the first row, under IP Address, the primary IP address of the primary Cisco PGW 2200 Softswitch; under Port, the first port number of the primaryCisco PGW 2200 Softswitch.

  In the second row, the secondary IP address and the second port number of the primary Cisco PGW 2200 Softswitch. These must match the primary information in the first row.

- (Cisco HSI server only)Secondary MGC—In the first row, under IP Address, the primary IP address of the secondary Cisco PGW 2200 Softswitch; under Port, the first port number of the secondary Cisco PGW 2200 Softswitch.

  In the second row, the secondary IP address and the second port number of the secondary Cisco PGW 2200 Softswitch. These must match the information in the first row.

> **Note** The Secondary MGC parameter is not used in a standalone Cisco PGW 2200 Softswitch configuration.

Network Tab (all)

The Network tab contains the following fields:

- IP addresses configured on the device—IP addresses from the IP address table. A device can have more than one IP address.

- IP Address—IP address of the selected entity.

- Net Mask—Subnet mask associated with the IP address.

- Interface Index—Interface on which the IP address is configured.

The Cisco LAN switch also contains these fields:

- Broadcast Address—The broadcast address of the switch.

- Net Mask—The net mask of the chassis.

- Booted Image—The name of the image from which the system was booted.

- Last Configuration Change—Time (in hundredths of a second) since the configuration of the system was last changed.

The Cisco PGW 2200 Softswitch host also contains a **Configuration** area:

- IP addresses configured on the Call Agent—Cisco PGW 2200 Softswitch host network addresses.

Software Tab (Cisco PGW 2200 Softswitch host, Cisco HSI server, and Cisco BAMS)

The Software tab contains the following fields describing software installed on the device:

- The software running on the selected device—A list of installed software. Select the software whose details you want to view.

- Name—Name of the selected software.

- Parameters—Parameters supplied to the software when it was run.

- Path—Location from where the software was run.

- Type—Type of software, such as operating system or device driver.
- Status—Status of the running software. Values are Running, Runnable, Not Runnable, and Invalid.

These fields apply to the Cisco PGW 2200 Softswitch host overall:

- Number of Processes—Actual: Number of process contexts currently running. Maximum: Number of process contexts this system can support.
- Number of Users—Actual: Number of user sessions for which this host is storing information. Maximum: Number of user sessions this host can support.

Virtual IP Tab (Cisco PGW 2200 Softswitch host)

The Virtual IP tab contains the following fields:

- Virtual IP address 1-Virtual IP address from Cisco PGW 2200 Softswitch host.
- Virtual IP Address 2- Second Virtual IP address from Cisco PGW 2200 Softswitch host.

Memory Tab (Cisco ITP-L and Cisco LAN Switch)

The Memory Tab contains the following fields:

- Memory Pool—A list of memory pools supported by the device. Select the memory pool whose details you want to view.
- Pool Name—Name assigned to the selected memory pool, such as DRAM.
- Memory Used—Number of memory pool bytes that are currently in use by applications.
- Memory Free—Number of memory pool bytes that are unused.
- Largest Free—Largest number of contiguous bytes that are currently unused.

Cisco ITP-L only:

- Configuration Memory—Bytes of nonvolatile configuration memory In Use/Total bytes of nonvolatile configuration memory.
- Processor RAM—Bytes of RAM available to the CPU.

Configuration Tab (Cisco ITP-L)

The Configuration Tab contains the following fields:

History area

- Configuration events on the device—List of configuration events in the device history. Select a device to view its details.

Event time:

- Source—Source of the selected configuration event.
- Destination—Configuration data destination for the event.
- Image Name—Name of the system boot image.
- Reason for Last Reload—Reason the system was last restarted.
- Running Last Changed—Value of system uptime (sysUpTime) when the running configuration last changed.
- Startup Last Changed—Value of system uptime when the startup configuration was last saved.

- Running Last Saved—Value of system uptime when the running configuration was last saved.

Poll Tab (BAMS)

The Poll Tab contains the following fields:

- Poll information—Poll table
- Host Name (primary and secondary)—Cisco PGW 2200 Softswitch host for this BAMS
- Prefix (primary and secondary)—Prefix for data files on the host
- Suffix (primary and secondary)—Suffix for data files on the host
- Remote Directory (primary and secondary)—Remote directory on the host
- Action—Action to perform after polling
- Interval—Polling unit (in minutes). Default value is 10
- Timeout—Timeout for file transfer. Default value is 10
- Maxtries—Maximum number of retries on each file. Default value is 3

RAS Parameters Tab (HSI Server)

The RAS Parameters Tab contains the following fields:

- Gatekeeper ID—Identifying name of the gatekeeper with which the endpoint is trying to register.
- Gateway Prefix—The telephone prefix for which the gateway is registering to be able to terminate.
- RAS Port—Number of the port receiving all RAS transactions for the current endpoint. Set to 0 to allow the OS to look for the available port.
- Gatekeeper IP Address—The IP address of a known gatekeeper with which an endpoint attempts to register.
- Gatekeeper Port—The port associated with the Gatekeeper IP Address, which can be either a well-known port or another port by agreement.

Viewing Properties for Interfaces

You can view properties for serial, Ethernet, loopback, and TDM interfaces of the various Cisco PGW 2200 Softswitch node devices. You can view properties for ports, VLAN, and SCO/SLO interfaces of the Cisco LAN switch.

Use the following procedure to view properties information for interfaces:

Step 1   In the Map Viewer window, select the desired interface.

> **Note**   Find TDM interfaces under the Cisco ITP-L.

Step 2   Right-click and choose **Properties**.

The Properties dialog box opens.

Step 3   If you have selected more than one device, choose the desired device in the list box on the left side of the dialog box.

Check device properties. See the "About the Serial, Ethernet, Loopback, and SCO/SLO Interface Properties Dialog Box" section on page 8-15 and the "About the TDM Interface Properties Dialog Box" section on page 8-16 for details on interface properties.

Step 4 (Optional) In the Properties dialog box, you can use the toolbar buttons or menu options to:

- Print the information on the current tab.
- Close the dialog box.
- Toggle dynamic update mode off and on.
- Refresh the window to update the information when dynamic update mode is off.
- Acknowledge that you have seen dynamically updated changes.

Note The status bar shows the current status of the interface.

About the Serial, Ethernet, Loopback, and SCO/SLO Interface Properties Dialog Box

The Serial, Ethernet, Loopback, and SCO/SLO Interface Properties dialog boxes contain a toolbar and a General and Details tab. All fields are display-only.

By default, the Properties dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off, acknowledge that you have seen updated information, and check for changes as desired when dynamic updating is off.

See the "Common Functionality in Properties Dialog Boxes" section on page 8-9 for more on dialog box functionality.

General Tab

The General tab contains the following display-only fields:

- (Ethernet, Loopback, and SCO/SLO) Physical Address—The interface address at the protocol sublayer.
- Description—A description of the interface.
- System Name—The administratively-assigned name for the interface.
- Interface Type—The type of interface, such as FDDI.
- Admin Status—The desired state of the interface. Values are Up, Down, or Testing.
- Operational Status—The current operational state of the interface. Values are Up, Down, Testing, Unknown, Dormant, Not Present, and Lower Layer Down.

Details Tab

The Details tab contains the following fields:

- Interface Index—Index of this interface in the interface table (ifTable)
- MTU—Size of the largest packet that can be sent or received on the interface
- (Ethernet, Serial, SCO/SLO only) Speed—Estimated speed of the interface, in bits per second
- Last Change—Time at which an interface was last created or deleted

About the TDM Interface Properties Dialog Box

The TDM Interface Properties dialog box contains a toolbar and a General and Details tab. All fields are display-only.

By default, the Properties dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off, acknowledge that you have seen updated information, and check for changes as desired when dynamic updating is off.

See the "Common Functionality in Properties Dialog Boxes" section on page 8-9 for more on dialog box functionality.

General Tab

The General tab contains the following display only fields:

- Description—A description of the interface
- System Name—The administratively assigned name for the interface
- Circuit ID—Transmission vendor's circuit identifier
- Speed—Estimated speed of the interface, in bits per second
- Interface Index—Index of this interface in the interface table (ifTable)
- Interface Type—The type of interface, such as FDDI
- Line Type—DS1 line type
- Line Coding—Variety of Zero Coding Suppression used on the link
- Last Change—Time at the last creation or deletion of an interface

Details Tab

The Details tab contains the following fields:

Status area

- Admin Status—The desired state of the interface. Values are Up, Down, and Testing.
- Operational Status—The current operational state of the interface. Values are Up, Down, Testing, Unknown, Dormant, Not Present, and Lower Layer Down.
- Line Status—Alarm status of the line.

Configuration area

- Signal Mode—Signaling mode. Values are None, Robbed bit, Bit oriented, and Message oriented.
- Send Code—Type of code sent across the interface. Values are No code, Line code, Payload code, and Reset code.
- Facilities Data Link—Use of the facilities data link.
- Loopback Config—Loopback configuration of the interface. Values are No loop, Payload loop, line loop, and other loop.
- Transmit Clock Source—Source of the transmit clock. Values are Loop timing, local timing, and through timing.

About the Cisco LAN Switch Port Properties Dialog Box

The Port Properties dialog box contains a toolbar and a General, Details, and VLAN tab. All fields are display-only.

By default, the Properties dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off, acknowledge that you have seen updated information, and check for changes as desired when dynamic updating is off.

See the "Common Functionality in Properties Dialog Boxes" section on page 8-9 for more on dialog box functionality.

General Tab

The General tab contains the following display-only fields:

- Physical Address—The interface address at the protocol sublayer.
- Description—A description of the interface.
- System Name—The administratively assigned name for the interface.
- Interface Type—The type of interface, such as FDDI.
- Admin Status—The desired state of the interface. Values are Up, Down, and Testing.
- Operational Status—The current operational state of the interface. Values are Up, Down, Testing, Unknown, Dormant, Not Present, and Lower Layer Down.
- MTU—Size of the largest packet that can be sent or received on the interface.
- Last Change—Time at the last creation or deletion of an interface.

Details Tab

The Details tab contains the following fields:

- Port Name—Name of the port.
- Port Type—Type of physical layer medium dependent interface on the port.
- Port Status—Current operational status of the port. Values are Up, Down, Testing, Unknown, Dormant, Not Present, and Lower Layer Down.
- Duplex—Indicates if port is operating in half-duplex, full-duplex, disagree, or auto-negotiation mode.
- Span Tree Fast Start—Whether the port is operating in span tree fast mode. Values are Enabled and Disabled.
- Desired Speed—Desired speed of the port, in bits per second.
- Speed—Estimated speed of the interface, in bits per second.

VLAN Tab

The VLAN tab contains the following fields:

- VLAN Number—Number assigned to the port.
- Switching Priority—Priority level the port uses to access the switching media. Values are Normal, High, and Not Applicable.
- Admin Status—Indicates whether the port will be assigned to a VLAN statically or dynamically. Values are Static and Dynamic.

- Operational Status—Current VLAN status of the port. Values are Inactive, Active, Shutdown, and VLAN Active Fault.

About the Cisco LAN Switch VLAN Properties Dialog Box

The VLAN Properties dialog box contains a toolbar and the fields described below. All fields are display-only.

By default, the Properties dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off, acknowledge that you have seen updated information, and check for changes as desired when dynamic updating is off.

See the "Common Functionality in Properties Dialog Boxes" section on page 8-9 for more on dialog box functionality.

Fields

- System Name—The administratively assigned name for the interface
- Spanning Tree Enabled—Whether spanning tree protocol is enabled for this VLAN

Viewing Properties for the Cisco ITP-L SS7 MTP2 Channel

Use the following procedure to view properties information for the MTP2 channel:

Step 1 In the Map Viewer widow, select the Cisco ITP-L.

Step 2 Right-click and choose **Channels > MTP2 Channel Properties**.

The SS7 MTP2 Properties dialog box opens.

Step 3 If you have selected more than one device, choose the desired device in the list box on the left side of the dialog box.

Step 4 Check device properties. See the "About the Serial, Ethernet, Loopback, and SCO/SLO Interface Properties Dialog Box" section on page 8-15 or the "About the TDM Interface Properties Dialog Box" section on page 8-16 for details on interface properties.

Step 5 (Optional) In the Properties dialog box, you can use the toolbar buttons or menu options to:

- Print the information on the current tab.
- Close the dialog box.
- Toggle dynamic update mode off and on.
- Refresh the window to update the information when dynamic update mode is off.
- Acknowledge that you have seen dynamically-updated changes.

Note The status bar shows the current status of the channel.

About the SS7 MTP2 Channel Properties Dialog Box

The Cisco ITP-L SS7 MTP2 Channel Properties dialog box contains a toolbar and the fields described below. All fields are display-only.

By default, the Properties dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off, acknowledge that you have seen updated information, and check for changes as desired when dynamic updating is off.

See the "Common Functionality in Properties Dialog Boxes" section on page 8-9 for more information on dialog box functionality.

The SS7 MTP2 Channel Properties dialog box contains the following fields:

- Channel Number—MTP2 channel number
- Link Status—Overall status of the link
- Alignment Error Rate Monitor—Status of the alignment error rate monitor state machine
- Signal Unit Error Monitor—Status of the signal unit error monitor (SUERM)
- Transmission Control—Status of the initial alignment control state machine
- Receive Control—Status of the receive control state machine
- Remote Processor Outage—Processor outage status of the remote
- Congestion Backhaul—Status of the congestion control state between the Cisco PGW 2200 Softswitch host and the Cisco ITP-L
- Congestion—Status of the congestion control state machine

Monitoring Cisco PGW 2200 Softswitch Host, the Cisco HSI Server, and the Cisco BAMS File Systems

You can monitor file systems on the Cisco PGW 2200 Softswitch host, Cisco HSI server, and the Cisco BAMS by

- Viewing file system information.
- Setting a threshold to have the device send a trap if file system usage passes the threshold.
- Viewing which file systems have exceeded their threshold.
- Polling file systems at a desired frequency, specifying a global polling frequency or individual frequencies for each file system.
- Polling all file systems now.
- Turning traps on or off for individual file systems based on trap severity.

Use the following procedure to monitor Cisco PGW 2200 Softswitch host, Cisco HSI server, or Cisco BAMS file systems:

Step 1   In the Map Viewer window, select the desired Cisco PGW 2200 Softswitch host, Cisco HSI server, or Cisco BAMS.

✎
Note   Alternatively, if you have an Accounts, Properties, States, or Diagnostics dialog box open for the device, you can use the dialog box Navigation menu to open the File Systems dialog box.

Step 2   Right-click and choose **File Systems**.

The File System Properties dialog box opens, displaying file system properties and settings for monitoring the file system.

If there is more than one selected device, the details shown apply to the currently highlighted device. In the list, click the device whose details you want to view or change. See the "About the File System Properties Dialog Box" section on page 8-20 for details.

Step 3   Check or change settings as needed:

- Use the General tab to view file system information.

- Use the Monitor tab to change settings for monitoring file system usage.

- Use the Exception tab to check file systems that have crossed their threshold.

> ✎
>
> **Note**   You can use the Navigation menu to open the Properties, Accounts, States, or Diagnostics dialog box for the selected component.

Step 4   If you make changes, click the toolbar **Save** button.

About the File System Properties Dialog Box

The File System Properties dialog box contains a toolbar and a single tab (General, Monitoring, and Exceptions).

By default, the Properties dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off, acknowledge that you have seen updated information, and check for changes when dynamic updating is off.

See the "Common Functionality in Properties Dialog Boxes" section on page 8-9 for more on dialog box functionality. Unlike other Properties dialog boxes, the File System Properties dialog box includes a toolbar Save button for saving changes to monitoring specifications.

General Tab

- File System—List of file systems for this device. Select a system to view details.

- Capacity—Percentage of normally available space that is currently allocated to files on the system.

- Used Space—Amount of space allocated to existing files.

- Free Space—Total amount of space available for the creation of new files by unprivileged users.

- Mount Point—Mount point (directory) of the file system.

Monitor Tab

- File System—List of file systems. Select a system to check or change monitoring settings.

- Current Utilization—Percent of disk space currently In Use/Percent full at which an event (alarm) will be triggered for the selected file system. Set alarm severity with Trap Severity.

- Poll Interval—Period in seconds when this file system should be checked to see if it exceeds its threshold.

Note The Poll Now function is not currently supported for an individual file system. Global Poll Now (all file systems) is supported.

- Threshold Command—Command to execute when the threshold is exceeded.
- Trap Severity—Severity of the trap that is sent when the threshold is exceeded. Values are Warning and Critical.
- When Above Threshold—Send a trap if the threshold is exceeded. Values are Send Trap and Don't Send Trap. Use Don't Send Trap to turn off notification for the selected file system.
- When Below Threshold—Send a trap if the file system usage falls below the threshold. Values are Send Trap and Don't Send Trap. Use Don't Send Trap to turn off notification for the selected file system.
- Global Poll Interval—Period in seconds when all file systems should be checked to see if any exceed the threshold.
- Poll Now button—Check all file systems for this device immediately.

Exceptions Tab

- File system list box—List of file systems that have exceeded their threshold. Select a file system to view details.
- File System—Name of the selected file system.
- Threshold—Threshold that has been exceeded.
- Current Utilization—Current percent utilization of the file system.

Viewing BAMS Node Properties

Use the following procedure to view BAMS Node properties:

Step 1 In the Map Viewer window, select the desired BAMS node.

Step 2 Right-click and choose **Properties**.

The BAMS Node Properties dialog box opens.

Step 3 (Optional) In the Properties dialog box, you can use the toolbar buttons or menu options to:

- Print the information on the current tab.
- Close the dialog box.
- Toggle dynamic update mode off and on.
- Refresh the window to update the information when dynamic update mode is off.
- Acknowledge that you have seen dynamically updated changes.

Note The status bar shows the current status of the interface.

About the BAMS Node Properties Dialog Box

The BAMS Node Properties dialog box contains a toolbar and tabs displaying various categories of component properties. All fields are display-only.

By default, the Properties dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off, acknowledge that you have seen updated information, and check for changes as desired when dynamic updating is off.

Properties Tab

The Properties tab contains the following display-only fields:

- Node Name—The name of the node.
- Node Status—Current Operational state of the node. Values are Active, Standby, Outage, Error, and Other.
- Measurement Interval—Interval in minute to generate measurement data.
- SC Collection—Indication flag of nail configuration collection.
- Dynamic Accumulator—Indication flag of dynamic accumulator usage.
- Zero-Count Suppression—Indication flag of the zero-count suppression feature.
- BAF ASCII Output—Indication flag of BAF records output in ASCII format.
- BAF Output—Indication flag of BAF records output.
- BAF Error Output—Indication flag of printing BAF error to syslog.
- ASCII Output—Indication flag of ASCII output.
- Measurement Output—Indication flag of measurement output function.
- Lookup Error Output—Indication which lookup errors are printed to syslog.

Poll Tab

- Poll information—Poll table.
- MGC Host (primary and secondary)—Cisco Cisco PGW 2200 Softswitch hosts that this BAMS node polls for CDR records.
- Prefix (primary and secondary)—Prefix for CDR data files on the Cisco PGW 2200 Softswitch host.
- Suffix (primary and secondary)—Suffix for CDR data files on the Cisco PGW 2200 Softswitch host.
- CDR Directory (primary and secondary)—Directory of the CDR data files on the Cisco PGW 2200 Softswitch host.
- Interval—Polling unit (in minutes). Default value is 10.
- Timeout—Timeout for file transfer. Default value is 10.
- Max Attempt—Maximum number of retries on each file. Default value is 3.

Viewing System Component Properties

You can check properties on the following system components of a Cisco PGW 2200 Softswitch host, a Cisco HSI server, or a Cisco BAMS:

- Disk partitions

- Processor
- RAM
- Virtual memory

> **Note** For information about viewing performance data for system components, see the Appendix B, "Performance Measurements Reference," "Performance Data Collected for System Components" section on page B-11.

Use the following procedure to view system component properties:

Step 1 In the Map Viewer window, do one of the following:

- To view information for all components of a particular type, select a Cisco PGW 2200 Softswitch host, a Cisco HSI server, or a Cisco BAMS, and right-click. Choose **Devices**, and then choose one of the following:
  - Disk Partition Properties
  - Processor Properties
  - RAM Properties
  - Virtual Memory Properties
- To view information for a particular component, under the Cisco PGW 2200 Softswitch host, the Cisco HSI server, or the Cisco BAMS, select the component and right-click. Choose **Properties**.

  The dialog box displays information on the selected component's properties. See the "About the System Components Properties Dialog Boxes" section on page 8-23 for details.

Step 2 (Optional) In the Properties dialog box, you can use the toolbar buttons or menu options to:

- Print the information on the current tab.
- Close the dialog box.
- Toggle dynamic update mode off and on.
- Refresh the window to update the information when dynamic update mode is off.
- Acknowledge that you have seen dynamically updated changes.

About the System Components Properties Dialog Boxes

There are two types of Cisco PGW 2200 Softswitch host, Cisco HSI server, and Cisco BAMS system component Properties dialog boxes:

- A Properties dialog box for fixed disk, RAM, and virtual memory
- A Properties dialog box for the processor

By default, the Properties dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off and check for changes when dynamic updating is off.

See the "Common Functionality in Properties Dialog Boxes" section on page 8-9 for more on dialog box functionality.

Fixed Disk, RAM, and Virtual Memory Properties Dialog Box

The Disk, RAM, and Virtual Memory Properties dialog boxes contain the following fields:

- Description—Description of the type and instance of the selected storage device.
- Allocation Units—Size in bytes of the data object allocated from this pool.
- Space Used—Amount of the storage that is allocated.
- Total Size—Size of the total device storage.
- Allocation Failures—Number of requests for storage that could not be honored.

Processor Properties Dialog Box

The Processor Properties dialog box contains the following fields:

- Description—Description of the processor.
- Status—Current operating status. Values are Running, Unknown, Testing, Warning, and Down.
- Utilization—Average over the last minute of the percent of time that the processor was active.
- Errors—Number of errors detected on this device.

Viewing Signaling Component Properties

You can view properties of the following signaling components of a Cisco PGW 2200 Softswitch node:

- Paths
- Links
- Point codes
- External nodes
- Interfaces
- SS7 components
- M3UA/SUA Components
- IPs In Mapping (used for EISUP and SIP signaling services only)
- In Sip Header
- Out Sip Header
- Domain Profile
- Profile
- SipI Version
- GW Pool
- IPGW

Use the following procedure to view signaling component properties:

Step 1 In the Map Viewer window, do one of the following:

- To view information for all components of a particular type, select the Signaling folder and right-click. Choose one of the following:

- **Paths**, and then choose the desired type of path component. See Table 8-2 for dialog box details.
- **Links**, and then choose the desired type of link component. See Table 8-3 for dialog box details.
- **Point Codes**, and then choose the desired type of point code component. See Table 8-4 for dialog box details.

> **Note** In Cisco PGW 2200 Softswitch Release 9.x, detailed DPC point code properties do not appear on the DPC Properties dialog box Details tab. Instead, drill down from the DPC to the SS7 path object (ss7svc1, for example), choose Properties, and in the Properties dialog box click the Details tab.

- **External Nodes**, and then choose the desired type of external node component. See Table 8-5 for dialog box details.
- **Interfaces**, and then choose the desired type of interface component. See Table 8-6 for dialog box details.
- **SS7 Components**, and then choose the desired type of SS7 component. See Table 8-7 for dialog box details.
- **M3UA/SUA Components**, and then choose either the M3UA Key or Route, or SUA Key or Route, component. See Table 8-8 for details.
- **IPs In Mapping**, and then choose IpInMapping Properties. See Table 8-9 for dialog box details.
- **In Sip Header,** and then choose IpSipHeader Properties. See Table 8-10 for dialog box details.
- **Out Sip Header,** and then choose OutSipHeader Properties. See Table 8-11 for dialog box details.
- **Domain Profile,** and then choose Domain Profile Properties. See Table 8-12 for dialog box details.
- **Profile,** and then choose Profile Properties. See Table 8-13 for dialog box details.
- **SipI Version,** and then choose SipIVersion Properties. See Table 8-14 for dialog box details.
- **GW Pool,** and then choose GWPool Properties. See Table 8-15 for dialog box details.
- **IPGW,** and then choose IPGW Properties. See Table 8-16 for dialog box details.

- To view information for a particular component, under the Signaling folder, select the desired component and right-click. Choose **Properties**.

  The dialog box displays information on the selected component's properties. See the "About the Signaling Components Properties Dialog Boxes" section on page 8-26 for details.

Step 2 (Optional) In the Properties dialog box, you can use the toolbar buttons or menu options to:

- Print the information on the current tab.
- Close the dialog box.
- Toggle dynamic update mode off and on.
- Refresh the window to update the information when dynamic update mode is off.
- Acknowledge that you have seen dynamically-updated changes.

About the Signaling Components Properties Dialog Boxes

The various Properties dialog boxes for signaling components contain a toolbar and fields described in tables below for each component type. By default, the Properties dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off, acknowledge that you have seen updated information, and check for changes as desired when dynamic updating is off.

- Signaling path components, in Table 8-2
- Signaling link components, in Table 8-3
- Signaling point code components, in Table 8-4
- Signaling external node components, in Table 8-5
- Signaling interface components, in Table 8-6
- Signaling SS7 components, in Table 8-7
- Signaling M3UA/SUA components, in Table 8-8
- IPs In Mapping components, in Table 8-9
- In Sip Header components, in Table 8-10
- Out Sip Header components, in Table 8-11
- Domain Profile components, in Table 8-12
- Profile components, in Table 8-13
- SipI Version components, in Table 8-14
- GW Pool components, in Table 8-15
- IPGW components, in Table 8-16

See the "Common Functionality in Properties Dialog Boxes" section on page 8-9 for more on dialog box functionality.

Table 8-2   *Properties of Signaling Path Components*

Field Name	Definition
Association Properties dialog box	
General tab	
MML Name	Name of the component.
Description	Description of the MML componen.t
Port	Local SCTP port number.
Peer Port	Destination SCTP port number.
External Node	Name of a previously configured external node.
First IP Address	First local address.
Second IP Address	Second local address.
First Peer Address	The highest priority destination address.
Second Peer Address	The lowest priority destination address.
Receive Window Bytes	Number of bytes to advertise for the local receive window.
IP Route 1	MML name of the first IP route.
IP Route 2	MML name of the second IP route.

Table 8-2   Properties of Signaling Path Components (continued)

Field Name	Definition
Time Between Heartbeats	Time between heartbeats. The heartbeat is this value plus the current retransmission timeout value.
Max Retransmissions	Maximum number of retransmissions to either the first or second peer address before it is declared failed.
Previously Configured SGP	MML name of a previously configured SGP.
Details tab	
Maximum Init Retransmission Timer	Maximum initial timer retransmission value.
Max Retransmission Timer	Maximum value allowed for the retransmission timer.
Min Retransmission Timer	Minimum value allowed for the retransmission timer.
Maximum Retransmissions to Dest	Maximum number of retransmissions over all destination addresses before the association is declared failed.
Max Bundling Wait Time	Maximum time SCTP will wait for other outgoing datagrams for bundling.
Max Init Retransmission Times	Maximum number of times to retransmit SCTP INIT message.
Max Time Before Sending SACK	Maximum time after a datagram is received before an SCTP SACK is sent.
Association State	State of SCTP association.
AXL Server Properties dialog Box	
MML Name	Name of the component.
Description	Description of the MML component.
First IP Address	First local address.
Second IP Address	Second local address.
Port	Local SCTP port number.
First Peer Address	The highest priority destination address.
Peer Port	Destination SCTP port number.
IP Route 1	MML name of the first IP route.
IP Route 2	MML name of the second IP route.
CTI Path	CTI Sig Path component.
Version	The version of CTI Path supported by Cisco PGW 2200 Softswitch.
BRI Path Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
External Node	MML Name of a previously configured external node.
Side	User for user side and network for network side; (network).

Cisco Media Gateway Controller Node Manager User Guide

Table 8-2   Properties of Signaling Path Components (continued)

Field Name	Definition
MDO	Message definition object file protocol name.
Customer Group ID	Four digit ID; (0000).
Call Ref Length	1 for 1 byte or 2 for 2 byte call reference length; (0).
Admin State	Administrative state of the component.
Destination Association	Point-code state.
Destination State	Destination Association.
Destination Package	Destination Package.
Locked	Number of bearer channels in LOCKED state.
Unlocked	Number of bearer channels in UNLOCKED state.
Shutdown	Number of bearer channels in SHUTDOWN state.
CAS Path Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
External Node	External node.
Customer Group ID	ID of the customer associated with the selected trunk group.
Side	Q.931 call model side.
Admin State	Administrative state of the component.
Locked	Number of bearer channels in LOCKED state.
Unlocked	Number of bearer channels in UNLOCKED state.
Shutdown	Number of bearer channels in SHUTDOWN state.
CTI Path Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
External Node	MML Name of a previously configured external node for this CTI Path.
CTI Manager Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
First IP Address	First local address.
Second IP Address	Second local address.
Port	Local SCTP port number.
First Peer Address	The highest priority destination address.
Peer Port	Destination SCTP port number.
IP Route 1	MML name of the first IP route.
IP Route 2	MML name of the second IP route.
CTI Path	CTI Sig Path component configured for this CTI Manager.

Table 8-2   Properties of Signaling Path Components (continued)

Field Name	Definition
Version	The version of CTI Manager supported by Cisco PGW 2200 Softswitch.
DPNSS Path Properties dialog box	
General tab	
MML Name	Name of the component.
Description	Description of the MML component.
Destination Association	Type of association.
Component Type	Type of component.
External Node	External node.
Customer VPN ID	VPN customer name assigned to the selected trunk group.
Customer Group ID	ID of the customer associated with the selected trunk group.
Signal Slot	Physical slot on 2600/3660 (optional).
Signal Port	Physical port on the slot of 2600/3660 (optional).
Destination Package	Name of the installed package.
A/B Flag	DPNSS side.
Details tab	
Admin State	Administrative state of the component.
Destination State	Destination state.
Locked	Number of bearer channels in LOCKED state.
Unlocked	Number of bearer channels in UNLOCKED state.
Shutdown	Number of bearer channels in SHUTDOWN state.
EISUP Path Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
External Node	External node
Customer Group ID	ID of the customer associated with the selected trunk group.
Customer Group Table	Customer group table.
Side	Q.931 call model side.
Destination State	Point-code state
Orig Label	Origination Location Label
Term Label	Termination Location Label
FAS Path Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
Customer Group Table	Customer group table.
Customer Group ID	ID of the customer associated with the selected trunk group.

Cisco Media Gateway Controller Node Manager User Guide

Table 8-2   Properties of Signaling Path Components (continued)

Field Name	Definition
Call Ref Length	Call reference length.
Side	Q.931 call model side.
MDO	Message definition object file protocol name.
A/B Flag	A/B flag.
ASP Part	Auxiliary signaling path.

IP FAS Path Properties dialog box

General tab

MML Name	Name of the component.
Description	Description of the MML component.
External Node	External node.
Customer Group Table	Customer group table.
Customer Group ID	ID of the customer associated with the selected trunk group.
Call Ref Length	Call reference length.
Side	Q.931 call model side.
MDO	Message definition object file protocol name.

Details tab

A/B Flag	A/B flag.
ASP Part	Auxiliary signaling path.
Admin State	Administrative state of the component.
Destination State	Point-code state.
Locked	Number of bearer channels in LOCKED state.
Unlocked	Number of bearer channels in UNLOCKED state.
Shutdown	Number of bearer channels in SHUTDOWN state.

MGCP Path Properties dialog box and **SGCP Path** Properties dialog box

MML Name	Name of the component.
Description	Description of the MML component.
External Node	External node.

NAS Path Properties dialog box

General tab

MML Name	Name of the component.
Description	Description of the MML component.
External Node	External node.
MDO	Message definition object file protocol name.
Customer Group ID	ID of the customer associated with the selected trunk group.
Signal Slot	Physical slot on the NAS defining the NFAS Group (optional).
Signal Port	Physical port on the slot of NAS defining the NFAS Group (optional).

Table 8-2   Properties of Signaling Path Components (continued)

Field Name	Definition
Details tab	
Admin State	Administrative state of the component.
Destination State	Point-code state.
Locked	Number of bearer channels in LOCKED state.
Unlocked	Number of bearer channels in UNLOCKED state.
Shutdown	Number of bearer channels in SHUTDOWN state.
Session Set Properties dialog box	
General tab	
MML Name	Name of the component.
Description	Description of the MML component.
External Node	External node.
First IP Address	First logical IP address.
Second IP Address	Second logical IP address.
First Peer Address	Remote IP address 1.
Second Peer Address	Remote IP address 2.
Ext Node Type	Session set external node type.
IP Route 1	Name of first IP route.
IP Route 2	Name of second IP route.
Details tab	
Port	Local port number of link interface on the Cisco PGW 2200 Softswitch host.
Peer Port	Port number of the link interface on the remote device.
Network Mask Address 1	Network mask (not supported after Cisco PGW 2200 Softswitch Release 9.3(2)).
Next Hop Address 1	Next hop (not supported after Cisco PGW 2200 Softswitch Release 9.3(2)).
Network Mask Address 2	Network mask (not supported after Cisco PGW 2200 Softswitch Release 9.3(2)).
Next Hop Address 2	Next hop (not supported after Cisco PGW 2200 Softswitch Release 9.3(2)).
SIP Path Properties dialog box	
MML Name	Name of the component
Description	Description of the MML component.
MDO	Message definition object file protocol name.
Admin State	Administrative state of the component.
Locked	Number of bearer channels in LOCKED state.
Unlocked	Number of bearer channels in UNLOCKED state.

Table 8-2   Properties of Signaling Path Components (continued)

Field Name	Definition
Shutdown	Number of bearer channels in SHUTDOWN state.
SS7 Path Properties dialog box	
General tab	
MML Name	Name of the component.
Description	Description of the MML component.
Customer Group ID	ID of the customer associated with the selected trunk group.
Customer Group Table	Customer group table.
ASP Part	Auxiliary signaling path.
MDO	Message definition object file protocol name.
Side	Q.931 call model side.
OPC	Originating point code.
DPC	Destination point code.
M3UAKey	MML name of M3UAKEY.
Details tab	
Admin State	Administrative state of the component.
Destination State	Point-code state.
Locked	Number of bearer channels in LOCKED state.
Unlocked	Number of bearer channels in UNLOCKED state.
Shutdown	Number of bearer channels in SHUTDOWN state.
TCAP Path Property dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
External Node	External node.
Label Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
Call Limit	Max number of calls allowed on this location label. 0-n. Integer value 0(default).
AXL Server Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
First IP Address	First local address.
Second IP Address	Second local address.
Port	Local SCTP port number.
First Peer Address	The highest priority destination address.
Peer Port	Destination SCTP port number.

Table 8-2   Properties of Signaling Path Components (continued)

Field Name	Definition
IP Route 1	MML name of the first IP route.
IP Route 2	MML name of the second IP route.
CTI Path	CTI Sig Path component.
Version	The version of CTI Path supported by Cisco PGW 2200 Softswitch.
CTI Path Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
External Node	MML Name of a previously configured external node for this CTI Path.
CTI Manager Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
First IP Address	First local address.
Second IP Address	Second local address.
Port	Local SCTP port number.
First Peer Address	The highest priority destination address.
Peer Port	MML name of the first IP route.
IP Route 1	MML name of the first IP route.
IP Route 2	MML name of the second IP route.
CTI Path	CTI Sig Path component configured for this CTI Manager.
Version	The version of CTI Manager supported by MGC.
H248Path Properties dialog box	
MML Name	Name of the component
External Node	External node.
Component Type	Type of the MML component
Description	Description of the MML component
Label	Call limiting label for gateway

Table 8-3   Properties of Signaling Link Components

Field Name	Definition
C7 IP Link Properties dialog box	
General tab	
MML Name	Name of the component.
Description	Description of the MML component.
IP Address	IP address.
Interface	Ethernet interface to which the link connects.

Table 8-3   Properties of Signaling Link Components (continued)

Field Name	Definition
Priority	Priority of the route.
Timeslot	Time slot used by the link.
Details tab	
Port	Local port number of the link interface on the MGC host.
Peer Address	Remote IP address of link address.
SLC	SS7 signaling link code.
Signal Channel State	State of the signaling channel.
Network Mask	Network mask.
Next Hop	Next hop.
D Channel Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
Service	Signaling service.
Status	Operational status of the D-channel.
Priority	Priority of the route.
Signal Slot	Physical slot on the gateway into which the T1/E1 is plugged.
Signal Port	Physical port on the gateway.
Session Set	Session set of backhaul link to the gateway.
TCP Link	Name of an existing TCP Link.
Sub Unit	Only for BRI D Channel. Integer 0 or 1.
IP Link Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
IP Address	IP address.
Interface	Ethernet interface to which the link connects (not supported after Cisco PGW 2200 Softswitch Release 9.3(2)).
Service	Signaling service.
Priority	Priority of the route.
Port	Local port number of link interface on the Cisco PGW 2200 Softswitch host.
Peer Port	Port number of the link interface on remote device.
Signal Slot	Physical slot on the gateway into which the T1/E1 is plugged.
Signal Port	Physical port on the gateway.
Signal Channel State	State of the signaling channel.
Network Mask	Network mask (not supported after Cisco PGW 2200 Softswitch Release 9.3(2)).

Table 8-3   Properties of Signaling Link Components (continued)

Field Name	Definition
Next Hop	Next hop (not supported after Cisco PGW 2200 Softswitch Release 9.3(2)).
IP Route	IP route's MML name.
State	State of the IP route.
IP Route Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
IP Address	Local IP address.
Destination	Destination hostname or IP address.
IP Route State	IP Route state.
Priority	Priority of the route.
Network Mask	Subnet mask of destination (optional).
Next Hop	Next hop router IP address.
Link Set Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
Protocol Family	Protocol used by the component.
APC	Adjacent point code for an STP.
Linkset Type	Type of transport for this link set.
Linkset State	Service state of the link.
SIP Link Properties dialog box	
General tab	
MML Name	Name of the component.
Description	Description of the MML component.
IP Address	IP address.
Interface	Ethernet interface to which the link connects (not supported after Cisco PGW 2200 Softswitch Release 9.3(2)).
Priority	Priority of the route.
Details tab	
Service	Type of signaling service.
Port	Local port number of the link interface on the Cisco PGW 2200 Softswitch host.
Signal Channel State	State of the signaling channel.
Network Mask	Network mask (not supported after Cisco PGW 2200 Softswitch Release 9.3(2)).
Next Hop	Next hop (not supported after Cisco PGW 2200 Softswitch Release 9.3(2)).

Cisco Media Gateway Controller Node Manager User Guide

Table 8-3   Properties of Signaling Link Components (continued)

Field Name	Definition
TDM Link Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
Interface	Ethernet interface to which the link connects.
Priority	Priority of the route.
Timeslot	Time slot used by the link.
Service	Type of signaling service.
SLC	SS7 signaling link code.
TCP Link Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
IP Address	IP address.
Type	Signaling Type. BRI.
Port	Local port number of link interface on the Cisco PGW 2200 Softswitch host.
IP Route	IP route's MML name.
External Node	External node.
Peer Port	Port number of the link interface on remote device.
Peer Address	Peer IP address.
Signal Channel State	State of the signaling channel.

Table 8-4   Properties of Signaling Point Code Components

Field Name	Definition
APC Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
Network Address	SS7 network address in dotted notation.
Network Indicator	Indicator assigned by the network administrator.
OPC	Originating point code.
DPC	Destination point code.
Route Set State	State of the point code.
DPC Properties dialog box	
General tab	
MML Name	Name of the component.
Description	Description of the MML component.
Network Address	SS7 network address in dotted notation.

Table 8-4   Properties of Signaling Point Code Components (continued)

Field Name	Definition
Network Indicator	Indicator assigned by the network administrator.
OPC	Originating point code.
DPC	Destination point code.
Details tab	
Admin State	Administrative state of the component.
Route Set State	State of the point code.
Destination State	Point-code state.
Locked	Number of bearer channels in LOCKED state.
Unlocked	Number of bearer channels in UNLOCKED state.
Shutdown	Number of bearer channels in SHUTDOWN state.
OPC Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
Network Address	SS7 network address in dotted notation.
Network Indicator	Indicator assigned by the network administrator.
OPC Type	Originating point code.

Table 8-5   Properties of Signaling External Node Components

Field Name	Definition
External Node Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
Extnode Type	Type of the external node.
Admin State	Administrative state of the component.
Locked	Number of bearer channels in LOCKED state.
Unlocked	Number of bearer channels in UNLOCKED state.
Shutdown	Number of bearer channels in SHUTDOWN state.
M3UA/SUA Group Number	M3UA/SUA group number.
ISDN Signaling Type	ISDN signaling type (optional).
SGP Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
External Node	External node's MML name.
SGP State	State of the Signaling Gateway Process.

Table 8-6   Properties of Signaling Interface Components

Field Name	Definition
Card Interface Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
Card Type	Type of card or adapter.
Slot	Location of card or adapter within host device.
Ethernet Interface Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
Card	Card that supports the interface.
TDM Interface Properties dialog box	
General tab	
MML Name	Name of the component.
Description	Description of the MML component.
Card	Card that supports the interface.
Signal Type	Signal type.
Coding	Line coding.
Format	Interface format.
Details tab	
Line Interface Number	Line interface number.
Resistance	Resistance.
Data Rate	Data rate.
Clock	Clock.
HDLC	High-level data link control.
DTE/DCE	Data terminal equipment/Data communications equipment.

Table 8-7   Properties of Signaling SS7 Components

Field Name	Definition
SS7 Route Properties dialog box	
MML Name	Name of the component.
Description	Description of the MML component.
Link Set	Link set that leads to destination device.
Priority	Priority of the route.
OPC	Originating point code.
DPC	Destination point code.
SS7 Subsystem Properties dialog box	

Table 8-7   Properties of Signaling SS7 Components (continued)

Field Name	Definition
MML Name	Name of the component.
Description	Description of the MML component.
Subsystem Number	Subsystem number.
Priority	Priority of the route.
Service	Type of signaling service.
Protocol Family	Protocol used by the component.
Transport Protocol	Transport protocol.
Mated APC	Adjacent point code for an STP mate.
STP/SCP Index	STP/Service control point index.
SuaKey	MML name of SUAKEY.
Local Subsystem Number	Local subsystem number (beginning in 9.5(2), used instead of Subsystem number).
Remote Subsystem Number	Remote subsystem number.
OPC	Origination point code.

Table 8-8   Properties of Signaling M3UA/SUA Components

Field Name	Definition
M3UA Key Properties dialog box	
MML Name	Routing key name, alphanumeric string up to 20 characters.
Description	Description of the MML component, up to 128 characters.
Service Indicator	(Optional) Service indicator: ISUP,TUP,N/A. Default: N/A
Routing Context	Routing context value, any integer except 0. Default: 0.
DPC	(Optional) Destination point code.
Network Appearance	(Optional) Network appearance. 0-32767. 0 indicates an invalid network appearance. Default: 0.
OPC	(Required) Originating point code.
M3UA Route Properties dialog box	
MML Name	M3UA route name, alphanumeric string up to 20 characters.
Description	Description of the MML component, up to 128 characters.
DPC	MML name of previously defined destination point code.
Pri	Priority.
External Node	MML name of a previously configured external node.
OPC	MML name of a previously configured origination point code.
SUA Key Properties dialog box	
MML Name	Routing key name, alphanumeric string up to 20 characters.

Table 8-8   Properties of Signaling M3UA/SUA Components (continued)

Field Name	Definition
Description	Description of the MML component, up to 128 characters.
OPC	(Required) Origination point code.
APC	(Optional) Adjacent point code.
Local SSN	Local subsystem number.
Routing Context	Routing context value, any integer except 0. Default: 0.
Network Appearance	(Optional) Network appearance. 0-32767. 0 indicates an invalid network appearance. Default: 0.
SUA Route Properties dialog box	
MML Name	SUA route name, alphanumeric string up to 20 characters.
Description	Description of the MML component, up to 128 characters.
APC	MML name of previously defined adjacent point code.
External Node	MML name of a previously configured external node.
Remote SSN	Remote subsystem number (destination).
OPC	MML name of a previously configured origination point code.

Table 8-9   Properties of IPs In Mapping Components

Field Name	Definition
IpInMapping Properties dialog box	
MML Name	MML name of this IpInMapping
Description	Description of the MML component
Sigsvc	Signaling services in which this IpInMapping is applied, SIP sigpath or EISUP sigpath
Allowed IP Address	Allowed IP address, host name or IP address with format x.x.x.x where x is 0-255
Allowed IP NetMask	Allowed net mask, the format is x.x.x.x where x is 0-255. The default is 255.255.255.255.
Port	Allowed SIP Port, only effective for SIP sigpath
Trunk Group Number	Trunk group number using the signaling services specified in Sigsvc (SIP or EISUP)

Table 8-10   Properties of In Sip Header Component

Field Name	Definition
InSipHeader Properties dialog box	
MML Name	The name of the SIP header table.
SIP Message Name	The SIP message that triggers a customized action. The value must be the name of a SIP request or response message.

Table 8-10   *Properties of In Sip Header Component (continued)*

Field Name	Definition
Treatment	The action that the Cisco PGW 2200 Softswitch takes when the SIP header is present.
Treatment Data Word 1 - 4	Data words that describe how the Cisco PGW 2200 Softswitch applies the treatment settings.
Index	Defines the preferred order for applying SIP header table entries. If a SIP header matches more than one entry in the SIP Header table, the Cisco PGW 2200 Softswitch applies the entry with the lowest Index value.
SIP header name	The name of a SIP header that the Cisco PGW 2200 Softswitch uses to modify traffic.
Condition	Defines how the Cisco PGW 2200 Softswitch uses the SIP header table entry to analyze traffic. This field requires one or more entries in the Condition DW fields.
Condition Data Word 1 - 4	The tags the Cisco PGW 2200 Softswitch uses to analyze SIP traffic. You can define up to four tags for each row in the SIP header table.

Table 8-11   *Properties of Out Sip Header Component*

Field Name	Definition
OutSipHeader Properties dialog box	
MML Name	The name of the SIP header table.
SIP Message Name	The SIP message that triggers a customized action. The value must be the name of a SIP request or response message.
Treatment	The action that the Cisco PGW 2200 Softswitch takes when the SIP header is present.
Treatment Data Word 1 - 4	The tag the Cisco PGW 2200 Softswitch uses based on the value in the Treatment field. You can apply up to four tags for each row in the SIP header table.
SIP header name	The name of a SIP header that the Cisco PGW 2200 Softswitch uses to modify traffic.
Index	Defines the order in which the Cisco PGW 2200 Softswitch applies SIP header table entries. If a SIP header matches more than one entry in the SIP Header table, the Cisco PGW 2200 Softswitch applies the entry with the lowest Index value.
policy	Defines the B2BUA mode applied to the call/trunk group
Condition	Defines how the Cisco PGW 2200 Softswitch uses the SIP header table entry to analyze traffic. This field requires one or more entries in the Condition DW fields.
Condition Data Word 1 - 4	The tags the Cisco PGW 2200 Softswitch uses to analyze SIP traffic. You can define up to four tags for each row in the SIP header table.

Table 8-12   Properties of Domain Profile Component

Field Name	Definition
Domain Properties dialog box	
Domain Name	The domain name used to analyze traffic
Domain Type	The direction of the profile
Profile Name	The name of a domain profile that is used for the domain name

Table 8-13   Properties of Profile Components

Field Name	Definition
Profile Properties dialog box	
default tab	
MML Name	The name of the profile.
Validation	Indicates whether the Cisco PGW 2200 Softswitch performs property validation.
Variant	The name of the variant.
Profile Type	The type of the profile.
Routing tab	
SIP Egress Routing Control	The preferred SIP header used for the initial routing decisions during sending of the Initial INVITE.
SIP Ingress Routing Control	The preferred SIP header used for the initial routing decisions(Initial INVITE).
Unavailable Procedure	Indicates the procedure to follow when there are no available ISUP circuits.
Enable IP Screening	Enables the incoming trunk group to select dial plan based on IP address, source ID and CLI prefix.
Map Redirecting Number Method	Decides the mapping from ISUP Redirecting Number and Original Called Number to outgoing SIP/EISUP message.
Inhibit Sip From Mapping	Decides the mapping from incoming SIP message to ISUP CLI
Customer Group ID	ID of customer associated with a particular trunk group.
Map CLI to Sip Header	Determines the mapping rule from calling line identity to SIP Headers.
Congestion Procedure	Indicates the procedure to follow when there is congestion on ISUP circuits.
Billing tab	
AOC Invoke Type	Allows configuration of whether or not the AOC Supplementary services are applicable on a per call basis or for all calls.
Charge Origin	Indicates whether or not to include Charge Number and Originating Line Info as a pair in the IAM.
AOC Enabled	Determines whether Advice of Charge (AOC) handling should be applied to this call.

Table 8-13   Properties of Profile Components (continued)

Field Name	Definition
Populate SDP Info in CDR	Enable or disable extraction of informationn from SDP and thereby not populating it in CDR.
AOC Default Tariff Id	Allows configuration of the default tariff ID to be applied when AOCInvokeType is configured for all calls (that is, AOCInvokeType = 2).
Media tab	
SDP Xmit To H323 Trigger	Indicates the point in a call when the Cisco PGW 2200 Softswitch sends the Session Destination Protocol (SDP) from the terminating call leg to the H.323 Signaling Interface (HSI).
GW Default Codec String	Gateway default codec string. Enables the IOCC-MGCP to send the ordered series of codec choices separated by semicolons. Refer to your gateway documentation for a list of supported codec names.
GW Default ATM Profile	Defines an initial list of profiles that the Cisco PGW 2200 Softswitch uses to control ATM profile negotiation between two MGWs.
Compression Type	Indicates the G.711 compression type used on the trunk.
Num1 tab	
Directory Number NOA	Default Directory Number NOA.
Charge Number	Default Charge Number.
A Number National Prefix	Determines the prefix of the outgoing calling number when NOA is set to National.
B-Number Normalization	Indication that B-number normalization is appropriate.
CLI Select	Calling line identification. Determines whether or not the additional calling party number is presented in the incoming IAM.
Directory Number NPI	Default directory number NPI.
Directory Number Screening	Default directory screening indicator (SI).
Directory Number	Default directory number. This property is needed on the trunk group for a switched call and on the SigPath for a nailed call.
Carrier Network Type	Default carrier identifier network type.
Country Code to be Prefixed	Provides against the origin trunk group of a call the country code digits, which if needed can be prefixed on a number before sending the call forward. Only required when the property domain is SigPath or LinkSet.
B-number tech Prefix	This property will provide a digit string to be used as a Tech Prefix to the B-number when sending the call forward.type="string" size min="1" max="16".
A-number Normalization	Indication that A-number normalization is appropriate
CGPN Include	Indicates whether or not to include the CGPN in an IAM.
Originating Line Information	Default originating line information. Maps to trunk group property DefaultOLI.

Table 8-13   Properties of Profile Components (continued)

Field Name	Definition
Number Plan Area	Numbering plan area. Indicates the NPA code associated with the incoming trunk group.
Directory Number Presentation	Default Directory Presentation Indicator.
Apply Country Code to A Number	Controls functionality that applies a country code prefix to the calling party number before sending the call forward.
A Number International Prefix	Determines the prefix of the outgoing calling number when NOA i set to International.
Default Presentation Number NOA	Default Presentation Number NOA value.
B Digit Country Code to be Removed	Country Code for comparison with Called Party Leading Digits and removing them from the number.
A Digit Country Code to be Removed	A string of digits (maximum of 5 digits) which will be compared to the A-number, and if matches will be removed from the front of the number.
Inhibit Outgoing Calling Name Display	Enables or disables the inhibiting of the outgoing calling name display in DPNSS and EISUP (HSI) protocols.
Default Presentation Number NPI	Default Presentation Number NPI value
Inhibit Incoming Calling Name Display	Enables or disables the inhibiting of the incoming calling name display in DPNSS and EISUP (HSI) protocols.
Inhibit Outgoing Connected Number Display	Enables or disables the inhibiting of the outgoing connected number display in DPNSS and EISUP (HSI) protocols.
Inhibit Incoming Connected Number Display	Enables or disables the inhibiting of the incoming connected number display in DPNSS and EISUP (HSI) protocols.
CLI Selection For Code of Practice 3	Provisions, on a per trunk group basis, the level of CLI selection that the Cisco PGW 2200 Softswitch uses when sending the calling line identities (such as Calling Party Number or Generic Number parameter) to the succeeding exchange.
B Number International Prefix	Determines the prefix of the outgoing called number when NOA is set to International.
Default PN Presentation Indicator	Default presentation number presentation indicator.
Inhibit Outgoing Connected Name Display	Enables or disables the inhibiting of the outgoing connected name display in DPNSS and EISUP (HSI) protocols.
Num2 tab	
Charge Number NOA	Default charge number NOA.
Carrier Network ID	Default carrier identifier network Identifier,
Default PN	Enables the incoming trunk group to have default PN if the incoming call does not have one.

Table 8-13   Properties of Profile Components (continued)

Field Name	Definition
Charge Number NPI	Default charge number NPI.
Inhibit Incoming Connected Name Display	Enables or disables the inhibiting of the incoming connected name display in DPNSS and EISUP (HSI) protocols.
Apply Country Code to B Number	Controls functionality that applies a country code prefix to the called party number before sending the call forward.
B Number National Prefix	Determines the prefix of the outgoing called number when NOA is set to National.
Carrier Network ID Plan	Default carrier national network identifier plan.
Profile tab	
Tone Option	Specifies whether playing tone to originating side is mandatory, only be effectively on ingress IP trunk group.
Sip IFacility Reject Handling	Indicates whether to swallow or treat as transparent message to handle ISUP facility reject message.
Anchor Media	Defines the media anchor policy on this IP trunk group.
Use Domain Profile	Indicates whether to use domain profile or not.
Sip Insert Reason Header	To indicate that whether a reason header containing cause code is needed.
SipI Egress Handling	Indicates that the value of handling disposition-param set in the the Content-Disposition header field associated with the ISUP MIME body. Configured on outgoing SIP-I trunk groups.
Common Profile	Pointer to another profile of type COMMONPROFILE.
Gateway Pool	Associate the gateway pool to an IP trunk group, so that media may anchor on this gateway pool.
Outbound Domain Profile Source	Indicates the source of getting outbound domain.
SipI Ingress Version Map	To indicate the profile name of the acceptable Version in Content-Type for SIP I trunk group.The ISUP variant will be decided by both the profile name and the incoming Version.
SIP COLPReq Enabled	To indicate whether to enable COLP request.
Trust Level	Indicates if the trunk group or domain is trusted or untrusted interface.
LRNDigitCCPrefix	An egress trunk group-based property which, if enabled, prefix the destination Country code in CC_DIG for the call to the location routing number and changes the NOA code to international.
SipI Confusion Handling	Indicates whether to swallow or treat as transparent message to handle ISUP confusion message.
SipI CANCEL Encapsulated REL	To indicate that whether the encapsulated REL message is needed in CANCEL.
Sip Egress GN2 From Screen	To indicate with which Screen Indictor's, the Generic Number can be mapped to SIP From header.

Cisco Media Gateway Controller Node Manager User Guide

Table 8-13   Properties of Profile Components (continued)

Field Name	Definition
NAT Traversal Enabled	Indicates whether PGW will do NAT traversal in add or modify request. The detailed NAT traversal method is depended in the sigPah property NATTraversalMethod.
Sip ICLICOL Preference	To indicate that whether CLI/Connected Number should take SIP header as preference.
Sip Egress Early Dialog RelType	To indicate whether to send CANCEL or BYE for the Early Dialog release.
LRNDigitCCrm	An egress trunk group-based property which, if enabled, prefix the destination Country code in CC_DIG for the call to the location routing number and changes the NOA code to international.
In Sip Header Table	Pointer to a inbound SIP header table. Value range: Existing inbound SIP header table name.
Dummy Codec String	Specifies the dummy codec list in H.248 add request when neither remote SDP nor local codec provision is available. This property is only effect for DBE.
Out Sip Header Table	Pointer to a outbound SIP header table.
Anchor Policy	Defines the media anchor policy in the policy function whether to enable gateway pool on IP trunk group.
SipI Egress MDO	To indicate the MDO variant for SIP-I egress on the outgoing SIP trunk group.
SipI Egress ISUP Version	To indicate the Version sub-parameter used in the Content-Type header field for SIP-I EGRESS on the outgoing SIP trunkgroup.
SipIToiw2	To indicator Toiw2 timer interval (milliseconds).
SipIngressLNPHandling	To indicator how to map the SIP routing number and telephone number.
Announcement Option	Specifies whether playing announcement to originating side is mandatory, only be effectively on ingress IP trunk group.
GR Profile	Pointer to another profile of type GRPROFILE.
Sip tab	
MGC Domain	MGC Domain Name in SIP Messages.
Respect Sip URI User Parm	Determines whether or not respect user=phone in p-asserted-id and remote-party-id header.
Topology Hiding Enabled	Indicates whether topology hiding is enabled or not.
MIN Event Subscribe Duration	The minimum duration for which an event can be subscribed. It is an integer value in millisecond.
Support 100 Response Code	Indicates whether Cisco PGW 2200 Softswitch will support reliable 100 response code.
TG TagLabel Trans Enable	Indicates how the Cisco PGW 2200 Softswitch handles the ingress trunk group tag label (if present) in the outgoing SIP INVITE message.
DelayedOfferToEarlyOfferInterworking	Indicates TCC send initial INVITE with sdp or not if receiveing INVITE w/o sdp from line.

Table 8-13   Properties of Profile Components (continued)

Field Name	Definition
MGC SIP Version	Supported MGC SIP Version.
MAX Subscription Duration	The maximum duration for which the subscription can exist. An integer value in milliseconds.
SIP IP Source	Tells MDL to use IP packet source address from SDP in INVITE message to do dial plan selection.
Unsolicited Notify Method	Enables or disables Unsolicited NOTIFY method for unsolicited notification of SIP DTMF digits by Cisco PGW 2200 Softswitch.
SIP Mime Body Support	Decides on SIP-T and SIP-GTD related special processing of data.
Support 183 Response Code	Flag indicating support of 183 response code.
Subscribe Notify Support	Enables or disables SUBSCRIBE/NOTIFY method for solicited notification of SIP DTMF digits
sipTransportMode	Transport mode supported by this trunkgroup.
Timer tab	
Wait for Originating SDP Timer	The timer is started when the originating SDP information has not been received.
EXPIRE Timer	Timer value (in milliseconds) in the EXPIRE header of SIP messages.
T1 Timer	T1 Timer (in milliseconds) for SIP messages other than INVITE messages.
Hold Timer	Maximum hold time for a SIP call.
Wait for Terminating SDP Timer	The timer is started when the terminating SDP information has not been received.
INVITE Timer	T1 timer for INVITE messages.
Retry Timer	The time (in milliseconds) Cisco PGW 2200 Softswitch waits before successfully retry of SIP calls
Retrans Method	Specifies the re-transmission mode for SIP messages.
Wait for Answer Timer	The timer is started when the Cisco PGW 2200 Softswitch instructs the MGW to apply ring back tone upon receiving Alerting. The timer is stopped when the Cisco PGW 2200 Softswitch receives the Answer message.
Response Attempts	Specifies the transmission times for SIP response.
Non Invite Req Attempts	Specifies the transmission times for SIP Non-INVITE request.
T2 Timer	T2 Timer (in milliseconds) for SIP messages other than INVITE messages.
Invite Attempts	Specifies the timer value (in milliseconds) for SIP waiting for final response of INVITE request.
Term Session Timer	The maximum session time in millisec allowed for a SIP call terminated by a Cisco PGW 2200 Softswitch.
Orig Session Timer	The maximum session time in millisecs allowed for a SIP call originated by the Cisco PGW 2200 Softswitch.

Table 8-13   *Properties of Profile Components (continued)*

Field Name	Definition
Mid-Call CP Interval	Mid-Call check pointing interval.
Invite Wait Timer	Specifies the timer value (in milliseconds) for SIP waiting for final response of INVITE request.
Misc tab	
Gateway Ring Back Tone Support	Indicates whether or not the ringback tone application is supported.
Feature Transparency Disabled	Allows the user to disable feature transparency for all calls on the Cisco PGW 2200 Softswitch.
Allow H323 Hairpin	Allow H.323 hairpinning. Allows the Cisco PGW 2200 Softswitch to interconnect H.323-originated and H.323-terminated calls by the HSI component.
Fax/Modem Tone	Specifies if notification of fax/modem tone from the Cisco PGW 2200 Softswitch is desired.
Play Announcement	Enables, on a per trunk group basis, the playing of an early announcement. This property can either contain an integer announcement identity, or, if it is set to 0 (default), the announcement function is considered disabled at the trunk group level.
H323 Destination	The IP Address and Port of H323 Destination in the format of IP1[:PORT1][;IP2:PORT2] or NULL.
Mid-Call Service Customer ID	Customer ID associated with mid-call service. Values are any alphanumeric with length of 4.
GTD Message Format	Decides the GTD format.
DTMF Capability	Defines the DTMF capability of the egress trunk group.
Network Type	Base on this property, Cisco PGW 2200 Softswitch will know if the underlying network is ATM or IP. Based on the network type retrieved, various network specific (eg,atm profiles) parameters would be sent down to gateway.
TG TagLabel	This property identifies name of the trunk group from which a call comes.
Satellite	Indicates if the trunk is going over a satellite.
Inside VRF Name	Inside Virtual routing and forwarding (VRF) name.
ITP Action Request	The indication of the required ITP action.
ExtCOT	Determines the type of COT handling for the specified destination.
Local Port	UDP port for SIP communication.
QSIG Tunnel Variant	Allows the QSIG Tunnel capability to be enabled across outbound EISUP (HSI) interfaces and specifies which variant will be used.
Transparency Disabled	Indicates if ISUP transparency is disabled.
Disable QSIG Release Method	Decides release method with single release complete message or QSIG release sequence.
Echo Cancel	Indicates if echo cancellation is required.

Table 8-13   *Properties of Profile Components (continued)*

Field Name	Definition
Propagate Delay Counter	Propagation Delay counter. Indicates the propagation delay value in milliseconds that will be increased if propagation delay is available.
ISUP Trans Early Backward Disabled	Indicates if the egress Cisco PGW 2200 Softswitch is to send an end-to-end message, called Early Backward Call Setup message, immediately after receiving the call setup message with GTD information about the outgoing protocol variant.
Max SIP Forward	The maximum number of SIP forward allowed.
Fax Support	FAX support. Indicates if T.38 FAX calls are supported on the trunk group. This property must be enabled on the incoming and outgoing trunk groups for T.38 fax calls to be successfully routed.
Enable CCBS Path Reservation	Allows configuration of the Path Reservation option for each QSIG destination. In the case of EISUP, this is valid for HSI destinations only.
Outside VRF Name	Outside Virtual routing and forwarding (VRF) name.
GWPool tab	
Gateway Selection Method	Specifies the border gateway selection method within a gateway pool.
Gateway Announcement Support	Specifies whether the gateway pool supports playing an announcement package to the IP side.
Gateway Tone Support	Specifies whether the gateway pool supports playing a tone to the IP side.
Gateway DTMF Support	Describes the DTMF capability support for a gateway pool.
Gateway Codec Support	Specifies whether the gateway pool supports transcoding for IP-to-IP traffic.
T1 tab	
T1	T1
T2	T2
T4	T4
T5	T5
T6	T6
T7	T7
T8	T8
T9	T9
T12	T12
T13	T13
T14	T14
T15	T15
T16	T16
T17	T17

Table 8-13   Properties of Profile Components (continued)

Field Name	Definition
T18	T18
T19	T19
T20	T20
T21	T21
T22	T22
T23	T23
T24	T24
T25	T25
T26	T26
T27	T27
T28	T28
T33	T33
T34	T34
T35	T35
T36	T36
T38	T38
T2 tab	
T_CGB	Wait timer for circuit group block message.
T_GRS	Wait timer for circuit group reset message.
T_CRA	Timer for circuit reservation acknowledgment.
T_CCRR	Timer for continuity check recheck request.
T_CVT	Timer for circuit validation test. Default: 0 (milliseconds).
T_CGBA	Wait timer for circuit group block ACK message.
T_CCR	Timer for continuity check request.
More1 tab	
Carrier Select Include	Indicates whether or not to include the carrier selection information paramter in an IAM.
RedirMax	Specifies the maximum allowable value of the redirection counter parameter available in some C7 signaling systems before the call is force-released. Used to prevent routing loops in certain applications.
ATM Connection Type	Populates the connection type parameter (ct:) in local connection option parameters. This property is read for both originating and terminating legs of all ATM-switched calls.
T Max Digits	Specifies maximum number of digits to receive for overlap digit processing for call termination to this traffic path(1~32).
Redirect Info Include	Indicates whether or not to include the Redirection Info in an IAM.
CGPN Presentation Restricted	Determines if incoming Presentation indication should be overridden.

Table 8-13   Properties of Profile Components (continued)

Field Name	Definition
Expiry Warning Tone Type	Duration of expiry warning tone (1-5 seconds).
GTD Cap Type	To read the GTD configuration parameter string. Used by Cisco PGW 2200 Softswitch as a pointer to the subset of GTD params.
Glare	Call collision handling.
Include CIP for Non-geographic	Indicates whether or not to include the Carrier Identification Parameter (CIP) in an IAM on all calls to non-geographic numbers.
Own Routing Number	To enable or disable the RO service handling at point of interconnect.
Customer VPN ID	Allows the user to assign a VPN customer name to the trunk group.
Overlap Digit Time	Overlap interdigit timer. The time to wait for the rest of the digits.
CLI Default Allowed	If set to TRUE then it adjusts the presentation restricted field in the CLI to Presentation Allowed; if FALSE then it takes the mapped value from the OCC or TCC protocol side or the default value from the Map for this field if there is no received value from the other protocol side.
Inband Info Available	Indicates whether the outgoing ACM should contain inband information in optional back call indicator.
More2 tab	
Send Address in CGPN	Determines if CLI digits should be sent in outgoing CGPN parameter
Hop Count	Number of contiguous SS7 interchange circuits remaining before a call must be completed.
Redirect Counter Include	Indicates whether or not to include the Redirect Counter in an IAM.
From	Display name of the calling party.
Orig Carrier ID	The originating carrier ID for the trunk group. Supports the carrier screening capability as handled in the protocol.
Maximum ACL	Maximum automatic congestion level. The Cisco PGW 2200 Softswitch indicates its congestion level (if it is greater than 0) in the ISUP release message.
Transaction Request Include	Indicates whether or not to include the Transaction request parameter in an IAM.
CGPN Presentation	Determines if the incoming calling number presentation indication is to be overridden.
GAP Include	Indicates whether or not to include the Generic Address Parameter in an IAM.
Loop Avoidance Support	Enables the support of the loop avoidance feature in DPNSS protocol.
T Min Digits	Specifies minimum number of digits to receive for overlap digit processing for call termination to this traffic path.
ACL Duration	Duration (in seconds) ACL remains in effect
Allow CRMCRA	Indicates whether or not to allow the use of the Circuit Reservation Message (CRM) and Circuit Reservation Acknowledgement message (CRA).

Table 8-13   Properties of Profile Components (continued)

Field Name	Definition
VPN On-Net Table Number	Allows the user to assign VPN ON-NET profile table indices for a particular trunk group.
MWI String ON	Enables support for a Message Waiting Indication (MWI) string in a DPNSS protocol message. The message instructs a particular extension to light its MWI LED (also known as the MWI lamp).
Service Code Include	Indicates whether or not to include the Service Code parameter in an IAM.
O Max Digits	Specifies maximum number of digits to receive for overlap digit processing for call origination from this traffic path.
Redirect Capability Include	Indicates whether or not to include the Redirect Capability in an IAM.
ACC Response Control	Specifies the ACC Response Controls listed in the ACC Response Category table.
Charge Non-geographic	Indicates whether or not to include the Charge Number in an IAM on all calls to non-geographic numbers.
Confusion	A flag indicating whether or not to send the Confusion message when an unrecognized message type is received.
OCN Include	Indicates whether or not to include the Original Called Number in an IAM.
Location Number	The default outgoing number used if a location number is not present in an incoming call.
Suppress CLI Digits	Suppresses the calling party number. Values are: 0 (do not suppress but leave the calling number intact) or 1 (remove calling party number so no number is forwarded).
Package Type	Package type. Determines MDL MGCP message handling according to the CAS trunk group package.
Notification Include	Indicates whether or not to include the Notification parameter in the Call Progress (CPG) message.
Cot Percentage	Determines the percentage of calls on the trunk upon which a continuity test is performed.
DPNSS RO Routing Number Length	For DPNSS - QSIG PR ROO inter-working, the DPNSS RO routing number and call reference are concatenated and in QSIG they are separate fields. An indication of where the divide point is between the fields is an optional parameter in the DPNSS spec. It is therefore necessary to provide a configurable definition of how to split these two fields.
MWI String OFF	Enables support for a Message Waiting Indication (MWI) string in a DPNSS protocol message. The message instructs a particular extension to extinguish its MWI LED (also known as the MWI lamp).
Enable Hop	A flag indicating whether or not to enable the hop counter.
More3 tab	
AOCNodeID	This property is included in the Advice of Charge message to identify the node in the network that is activating the AOC service to this call.

Table 8-13   Properties of Profile Components (continued)

Field Name	Definition
OwnClli	Specifies the common language location identifier (CLLI) that identifies the Cisco PGW 2200 Softswitch. This can be up to 11 alphanumerical digits.
H248 Gateway Reserve Value	Enable Megaco to send ADD commands with ReserveValue "on" or "off" to indicate MG to reverse resource or not.
GN Include	Indicates whether or not to include the Generic Number in an IAM.
CLLI	Common language location identifier.
Allow EXM	Indicates whether or not to allow the use of the Exit Message (EXM).
TlinkAlignTime	Configurable timer for all Q.761, Q.767 and ANSI protocols.
SipDtmfContentType	Dtmf content type for SIP info message.
Generate Redirection Number	Defines whether generate Redirection Number for SIP diversion.
Alarm Carrier	Indicates the method of alarm carrier so that circuit validation tests may be fully compliant with ANSI T1.113.
Screen Fail Action	Screen fail action. Indicates if an action is to be performed when a screening failure occurs.
JIP Default	Indicates the default JIP value to be sent when jipInclude = 1 and no JIP value is present. If the value is 0, jipDefault is treated as if no value is present. Value range: 0 through 9.
Default Bearer Capability	Default bearer capability. Indicates the coding used by the User Service Information parameter in the outgoing IAM message.
TBufferDigitLength	Limits the maximum number of digits allowed in the outgoing IAM and SAM.
OD 32 Digit Support	To allow 32 digits and overdecadic digits support for the ANSI, O721, O761 and O767 protocol variant.
SCP Credit Expired Timer	Duration of time (1-180 seconds) before credit expiry that SCP will be notified.
Ring-No-Answer	Indicates the time, in seconds, ringing is allowed to occur.
JIP Include	Indicates whether or not to include the Jurisdiction Information Parameter (JIP) in an IAM.
RestrictPresIfNoPAID	To indicate that for an incoming SIP call on this TG with no P-Asserted-Identify header.
Circuit Group Carrier	Indicates the method of circuit group carrier so that circuit validation tests may be fully compliant with ANSI T1.113.
ATP Include	Indicates whether or not to include the Access Transport Parameter in an IAM.
Expiry Warning Tone Duration	Duration of expiry warning tone (1-5 seconds).
VPN Off-Net Table Number	Allows the user to assign VPN OFF-NET profile table indices for a particular trunk group

Table 8-13   Properties of Profile Components (continued)

Field Name	Definition
RN Include	Indicates whether or not to include the Redirecting Number in an IAM.
O Overlap	Set to 1 to enable overlap signaling for call origination from this traffic path.

Table 8-14   Properties of SipIVersion Component

Field Name	Definition
SipIVersion Properties dialog box	
Profile	MML name of a SIP-I mapping profile.
SIP-I Version	SIP-I version defined by the operator and used in the SIP-I message Content-Type header field.
MDO	SIP-I variant name mapped to the SIP-I message ParamContent field.

Table 8-15   Properties of GW Pool Component

Field Name	Definition
GWPool Properties dialog box	
MML Name	Gateway pool ID
Profile Name	Profile name
Description	Gateway pool description

Table 8-16   Properties of IPGW Component

Field Name	Definition
IPGW Properties dialog box	
Gateway Pool Name	Name of the gateway pool
External Node	Name of the external node

Viewing Trunk Group Component Properties

You can view the properties of trunk group components of a Cisco PGW 2200 Softswitch node such as

- Configuration
- Status
- SIP attributes (Cisco PGW 2200 Softswitch Release 9 and later)

Use the following procedure to view trunk group component properties:

Step 1   In the Map Viewer window, do one of the following:

- To view information for all trunk group components, select the Trunking folder, and right-click. Choose **Trunk Group Properties**.

- To view information for a particular trunk group component, under the Trunking folder, select the desired component and right-click. Choose **Trunk Group Properties**.

  The dialog box displays information on the selected component's properties. See the "About the Trunk Group Properties Dialog Box" section on page 8-55 for details.

Step 2   (Optional) In the Properties dialog box, you can use the toolbar buttons or menu options to:

- Print the information on the current tab.

- Close the dialog box.

- Toggle dynamic update mode off and on.

- Refresh the window to update the information when dynamic update mode is off.

- Acknowledge that you have seen dynamically updated changes.

About the Trunk Group Properties Dialog Box

The Properties dialog box for trunk group components contains a toolbar and the fields described in Table 8-17. By default, the Properties dialog is dynamically updated as device information changes. You can use toolbar buttons to turn updating on or off, acknowledge that you have seen updated information, and check for changes as desired when dynamic updating is off.

See the "Common Functionality in Properties Dialog Boxes" section on page 8-9 for more on dialog box functionality.

Note   The trunk group properties you see, and the tabs they are located on, depend on the release of the Cisco PGW 2200 Softswitch software you are using.

Table 8-17   Properties of Trunk Group Components

Field Name	Definition
General tab	
Trunk Group Number	Trunk group number.
Trunk Type	Trunk transmission media.
Customer Group ID	ID of the customer associated with the selected trunk group.
Priority	Priority of the route.
Select Sequence	Selection sequence.
Service	Type of signaling service.
Queuable	Whether the trunk group is capable of queuing calls.
Package Type	CAS trunk group package.
Glare	Call collision handling.
Default Presentation Number NOA	Sets the default for Presentation Number NOA value.
Default Presentation Number NPI	Sets the default for Presentation Number NPI value.

Table 8-17   Properties of Trunk Group Components (continued)

Field Name	Definition
Default PN	Enables the incoming trunk group to have default presentation number if the incoming call does not have one; overdecadic digits are supported.
O Min Digits	This property specifies minimum number of digits to receive for overlap digit processing for call origination from this traffic path (integer, from 0 to 32). Default value: 0
O Max Digits	This property specifies maximum number of digits to receive for overlap digit processing for call origination from this traffic path (integer, from 1 to 32). Default value: 24
O Overlap	This property indicates whether overlap signaling for call origination from this traffic path is enabled (1=enabled, 0=not enabled). Default value: 0
Overlap Digit Time	This property specifies the waiting period for the rest of the digits (integer, from 0 to 60). Default value: 6
Trunkgroup Profile	Trunkgroup profile name.
Number Plan Area	The numbering plan area (NPA) code associated with the incoming trunk group.
Carrier ID	The carrier ID to which users on this trunk group are associated.
Orig. Carrier ID	Carrier ID digit string.
CLLI	Common language location identifier.
Carrier Screening	Whether to apply carrier selection and screening on the call.
Notify Setup Complete/Network Type	Whether to send notification when call setup completes.
Send Address to CGPN	Determines if CLI digits should be sent in outgoing CgPN parameter. Value is 0 (False) for don't include address digits in CgPN param or 1 (True) for including address digits in CgPN param; default is 1.
CGPN Presentation Restricted	Determines if incoming Presentation Indication should be overridden. Value is 0 (False) for leave as-is or 1 (True) for set to presentation restricted; default is 0.
Enable IP Screening	Enables the incoming trunk group to select dial plan based on IP address, source ID and CLI prefix tables.
Default PN Presentation Indicator	Sets default Presentation Number Presentation Indicator value.
SDP Xmit To H323 Trigger	Indicates the point in a call when theCisco PGW 2200 Softswitch sends the Session Destination Protocol (SDP) from the terminating call leg to the H.323 Signaling Interface (HSI).
T Overlap	This property indicates whether overlap signaling for call termination to this traffic path is enabled (1=enabled, 0 = not enabled). Default value: 0

Table 8-17   Properties of Trunk Group Components (continued)

Field Name	Definition
T Max Digits	This property specifies maximum number of digits to receive for overlap digit processing for call termination to this traffic path (integer, from 1 to 32). Default value: 24
T Min Digits	This property specifies minimum number of digits to receive for overlap digit processing for call termination to this traffic path (integer, from 0 to 32). Default value: 0
Maximum ACL	Maximum congestion level.
Configuration tab	
Fax/Modem Tone	Specifies if notification of the fax/modem tone from the Cisco PGW 2200 Softswitch is desired. Values are 0 (no) and 1 (yes).
Screen Fail Action	Indicates if an action is to be performed when a screening failure occurs. Values and 0 (no) and 1 (yes).
Ring-No-Answer	Time (in seconds) that ringing can occur.
AOC Enabled	Whether advice of charge handling should be applied to this call. Values and 0 (no) and 1 (yes).
Echo Cancel	Whether echo cancellation is required. Values and 0 (no) and 1 (yes).
ACC Control	Specifies the ACC Response Controls listed in the ACC Response Category table.
ACC Response Control	Turns on or off Automatic Congestion Control control procedures based on the Automatic Congestion Level value received by the Cisco PGW 2200 Softswitch from a linked switch.
External COT	External continuity test indicator.
Support 183 Response Code	Flag indicating support of 183 response code.
Customer VPN ID	Assigns a VPN customer name to the trunk group. Prefix="*" Default="00000000", Size min=1 max=8.
VPN On-Net Table Number	Assigns VPN ON NET profile table indices for a particular trunk group. Prefix="*" Default="0", Size min=1 max=8.
VPN Off-Net Table Number	Assigns VPN OFF NET profile table indices for a particular trunk group. Prefix="*" Default="0", Size min=1 max=8.
Populate SDP Info in CDR	Enables extraction of information from SDP. 1 enables, 0 disables. Default 0.
Support 100 Response Code	Flag indicating support of 100 response code.
ACL Duration	Duration (in seconds) that ACL remains in effect.
Satellite	Indicates if the trunk group is going over a satellite. Values and 0 (no) and 1 (yes).
Call Orig. Index	Starting number analysis digit index for call origination.
Call Term. Index	Starting number analysis digit index for call termination.

Table 8-17   Properties of Trunk Group Components (continued)

Field Name	Definition
Transparency Disabled	Indicates if ISDN User Part (ISUP) transparency is disabled. Values 0 (no) and 1 (yes).
COT Percentage	Statistical continuity test percentage.
Compression Type	The G.711 compression type used on the trunk.
From	The display name of the calling party.
Call Forward Reroute Disabled	Disables Call Forward rerouting for all calls. Prefix=”*. Range 0 - 1. Default 0.
Feature Transparency Disabled	Disables Feature Transparency for all calls. Prefix=”*. Range 0 - 1. Default 0.
OD 32 Digit Support	Indicates whether overdecadic and 32 digits are supported for ANSI, Q721, Q761, and Q767 protocol variants. Values 0 (no) and 1 (yes). Default 0.
Status tab	
Admin State	Administrative state of the component.
Locked	Number of bearer channels in LOCKED state.
Unlocked	Number of bearer channels in UNLOCKED state.
Shutdown	Number of bearer channels in SHUTDOWN state.
SIP tab	
Local Port	UDP port for SIP communication.
Unsolicited Notify Method	Enables or disables Subscribe/Notify method for solicited notification of SIP DTMF digits.
SIP IP Source	Tells MDL to use IP packet source address or IP address from SDP in INVITE message to do dial plan selection for SIP calls.
Max Redirection	The maximum number of SIP message redirects allowed.
T1 Timer	T1 timer (in milliseconds) for SIP messages other than INVITE messages.
Orig. Session Timer	The maximum session time (in milliseconds) for a SIP call originated by the Cisco PGW 2200 Softswitch.
INVITE Timer	T1 timer for INVITE messages.
Hold Timer	Maximum hold time for a SIP call.
MIN Event Subscribe Duration	Minimum duration for which an event can be subscribed, in msec. Range: 40-3600 msec.
MAX Subscription Duration	Maximum duration for which the subscription can exist before it needs a re-subscription, in msec. Range: 0-3600 msec.
ISUP Trans Early Backward Disabled	Sends the early backward message-183 session progress without the SDP MIME body. 0 - Enable, 1 - Disable. Default 1.

Table 8-17   Properties of Trunk Group Components (continued)

Field Name	Definition
Invite Attempts	The transmission times for INVITE requests. Valid values are 1–15. Default, 7.
Response Attempts	The transmission times for response. Valid values are 1–15. Default, 11.
Invite Wait Timer	The timer (in milliseconds) of waiting for final response of INVITE request. Valid values are 10000–500000. Default, 200000.
SIP Ingress Routing Control	The preferred SIP header used for the initial routing decisions(Initial INVITE)
Map CLI to SIP Header	Determines the mapping rule from calling line identity to SIP Headers. Values: 0,1,2,3,4
SIP MIME Body Support	Determines SIP-T and SIP-GTD related special processing of data (used by SS7 and SIP trunk groups). 0 - None, 1- SIP-T supported, 2 - SIP-GTD supported. Default 0.
MGC SIP Version	The version of SIP protocol supported by Cisco PGW 2200 Softswitch. Maps to trunk group property MGCSipVersion. Any valid SIP version, SIP2.0 default.
MGC Domain	Cisco PGW 2200 Softswitch's domain name used in SIP messages. Maps to trunk group property MGCDomain. Any valid domain name or NULL string.
Max SIP Forward	The maximum number of SIP forward allowed. Maps to trunk group property MaxForwards. Any value > 0, default 10.
T2 Timer	T2 timer (in milliseconds) for SIP messages other than INVITE messages.
EXPIRE Timer	Timer value (in milliseconds) in the EXPIRE header of SIP messages.
Term. Session Timer	The maximum session time (in milliseconds) for a SIP call terminated by the Cisco PGW 2200 Softswitch.
Retry Timer	The time (in milliseconds) that Cisco PGW 2200 Softswitch waits before retrying SIP calls.
GTD Cap Type	Used as a pointer to the subset of GTD configuration parameters. Values: 0 - No GTD parameter string. Any other string - points to entry in gtdParam.dat file. Default: 0.
Subscribe Notify Support	Enables or disables Unsolicited Notify method for solicited notification of SIP DTMF digits.
GTD Message Format	Selects GTD message format. C - Compact mode, V - verbose mode. Default C.
Non Invite Req Attempts	The transmission times for Non-INVITE requests. Valid values are 1–15. Default, 11.
Retrans Method	The re-transmission method. 1, exponential. 2, linear. Default, 1.
SIP Egress Routing Control	The preferred SIP header used for the initial routing decisions during sending of the Initial INVITE

Cisco Media Gateway Controller Node Manager User Guide

Table 8-17   Properties of Trunk Group Components (continued)

Field Name	Definition
Respect SIP URI User Parm	Determines whether or not respect user=phone in p-asserted-id and remote-party-id header. Values: 0 (no) or 1 (yes)
Profile tab	
Originating Line Information	Default originating line information.
Carrier Network ID	Default carrier identifier network identifier.
Carrier Network Type	Default carrier identifier national network type.
Carrier Network ID Plan	Default carrier network national network identifier plan.
Charge Number	Default charge number.
Charge Number NOA	Default charge number nature of address.
Charge Number NPI	Default charge number plan identification.
Charge Origin	Specifies the charge origin. It is up to the network engineer to decide what value of charge origin will be used.
Refer Redirecting NOA	NOA value in ITU SS7 REL message for bind transfer by sip REFER, use internal NOA value.
Directory Number Presentation	Default directory presentation indicator.
Directory Number Screening	Default directory screening indicator.
Directory Number	Default directory number.
Directory Number NOA	Default directory number nature of address.
Directory Number NPI	Default directory number plan identification.
LRN Digit CCrm	An egress trunk group-based property which, if enabled, prefix the destination Country code in CC_DIG for the call to the location routing number and changes the NOA code to international.
LRN Digit CCPrefix	An egress trunk group-based property which, if enabled, prefix the destination Country code in CC_DIG for the call to the location routing number and changes the NOA code to international.
Xmit Calling Name	Allows the Cisco PGW 2200 Softswitch to use the displayname in the INVITE or INFO header for the calling party name.
Refer Redirecting Ind	Redirecting indication in ITU SS7 REL message for bind transfer by sip REFER.
H.323 Tab	
Gateway Ring Back Tone	Indicates if the gateway ring back tone application is supported within the gateway that hosts the trunk group and the connection method that is applied.
Wait for Answer Timer	Duration, in seconds, that the Cisco PGW 2200 Softswitch waits to receive the Answer message after instructing the MGW to apply ring back tone.

Table 8-17   Properties of Trunk Group Components (continued)

Field Name	Definition
Wait for Originating SDP Timer	Duration, in seconds, that the Cisco PGW 2200 Softswitch waits for the originating SDP information after transiting the answer message.
Wait for Terminating SDP Time	Duration, in seconds, that the Cisco PGW 2200 Softswitch waits for the terminating SDP information after transiting the answer message.
Allow H.323 Hairpin	Whether to allow the HSI component connected through the EISUP path to make and receive H.323 calls to and from another HSI component.
Fax Support	What fax support, if any, is available on the incoming trunk group.
H.323 Adjunct Link	Identifies an EISUP link that is connected to an H.323 adjunct platform.
H323 Destination	HSI 323 Destination.
Characteristics Tab	
A Number National Prefix	National prefix string to be added to the national dialed number when NOA is enabled.
A Number International Prefix	International prefix string to be added to the international dialed number when NOA is enabled.
B Number National Prefix	B-number national prefix. Determines the prefix for outgoing called numbers when Nature of Address (NOA) is set to National.
B Number International Prefix	Determines the prefix for outgoing called numbers when NOA is set to International.
Apply Country Code to A Number	Controls functionality that applies a country code prefix to the calling party number before sending the call forward.
Apply Country Code to B Number	Controls functionality that applies a country code prefix to the called party number before sending the call forward.
B Digit Country Code to be Removed	Country Code for comparison with Called Party Leading Digits and removing them from the number.
Country Code to be Prefixed	Country code string to be prepended.
A-number Normalization	(European feature; ingress trunk groups) Indicates that A-number (Calling Party Number) normalization is appropriate based on the NOA value and the leading digits of the A-number. Leading digits 0: Remove 0 and set NOA to NATIONAL. 00: Remove 00 and set NOA to INTERNATIONAL.
B-Number Normalization	(European feature; ingress trunk groups) Indicates that B-number (Called Party Number) normalization is appropriate based on the NOA value and the leading digits of the B-number. Leading digits 0: Remove 0 and set NOA to NATIONAL. 00: Remove 00 and set NOA to INTERNATIONAL.

Cisco Media Gateway Controller Node Manager User Guide

Table 8-17   Properties of Trunk Group Components (continued)

Field Name	Definition
DPNSS RO Routing Number Length	For DPNSS - QSIG PR ROO inter-working, the DPNSS RO routing number and call reference are concatenated and in QSIG they are separate fields. An indication of where the divide point is between the fields is an optional parameter in the DPNSS spec. It is therefore necessary to provide a configurable definition of how to split these two fields.
QSIG Tunnel Variant	Allows the QSIG Tunnel capability to be enabled across outbound EISUP (HSI) interfaces and specifies which variant will be used.
SCP Credit Expired Timer	Time period before credit expiry that the SCP is notified.
SSF Credit Expired Timer	Time period before credit expiry that the SSF is notified.
Warning Credit Expired Timer	Time period before credit expiry that a warning tone or announcement is played.
Expiry Warning Tone Type	Type of warning tone.
Expiry Warning Tone Duration	Duration of warning tone.
CLI Select	Whether the Dual CLI feature is supported (default is N).
GW Default Codec String	Ordered series of codec choices, separated by semicolons.
A Digit Country Code to be Removed	A string of digits (maximum of 5 digits) which will be compared to the A-number, and if matches will be removed from the front of the number
H248 Gateway Reserve Value	Enable Megaco to send ADD commands with ReserveValue ON or OFF to indicate MG to reverse resource or not
Own Routing Number	To disable/enable RO service handling at point of interconnect. Value: NULL or a numeric string
Enable CCBS Path Reservation	Support for the Path Reservation option should be configurable against each QSIG destination. In the case of EISUP, this is valid for HSI destinations only.
Disable QSIG Release Method	This property indicates the QSIG release method. An H.225 signaling connection can be released with a single Release Complete message instead of a three-stage QSIG release sequence.
More Tab	
GW Default ATM Profile	Provides an initial list of profiles for use in ATM gateway profiles negotiation per trunkgroup. Default "NULL" type="string" size min="1" max="140".
Play Announcement	Contains announcement id. 0 means the functionality will be considered as switched off at the trunk group level. Default "0" type="int".

Table 8-17   Properties of Trunk Group Components (continued)

Field Name	Definition
ATM Connection Type	Populates connection type indicator (ct:) in local connection option parameters. This property is read for both originating and terminating legs of all ATM switched calls. Property Valid Values: 1-->AAL1,2--> AAL1_SDT, 3-->AAL1_UDT, 4-->AAL2, 5-->AAL 3/4, 6-->AAL5. default="4" type="int" range min="1" max="6".
B-number Tech Prefix	This property will provide a digit string to be used as a Tech Prefix to the B-number when sending the call forward.type="string" size min="1" max="16".
Loop Avoidance Support	This property will indicate whether to support Lop Avoidance feature in DPNSS or not. Default 0 not supported, 1 - supported.
Loop Avoidance Counter	Loop Avoidance counter for DPNSS. Min value is 0 and Max 25. default 0.
MWI String OFF	MWI OFF string as used by DPNSS PBX, Default = NULL.
MWI String ON	MWI ON string as used by DPNSS PBX, Default = NULL.
aocDefaultTariffId	Allows configuration of the default tariff ID to be applied when AOCInvokeType is configured for all calls (that is, AOCInvokeType = 2).
AOC Invoke Type	This property is used to configure whether the AOC Supplementary services should be applicable for all calls or for per call basis. ("1" = per call, "2" = All calls). Default = "1".
midCallCPInterval	A property to allow user to enable/disable mid-call checkpointing and when enabled, it specifies the interval between checkpointing event in the connected state. min = 0, max=60(in minute unit). value zero means disabled.
TG TagLabel	This property identifies name of the trunk group from which a call comes.
TG TagLabel Trans Enable	Indicates how the Cisco PGW 2200 Softswitch handles the ingress trunk group tag label (if present) in the outgoing SIP INVITE message.
Mid-Call Service Customer ID	Customer ID associated with mid-call service. Values are any alphanumeric with length of 4.
Network Type	Base on this property, Cisco PGW 2200 Softswitch will know if the underlying network is ATM or IP. Based on the network type retrieved, various network specific (eg,atm profiles) parameters would be sent down to gateway.

Table 8-17   *Properties of Trunk Group Components (continued)*

Field Name	Definition
CLI Selection For Code Of Practice3	A new PGW2200 Trunk Group Property called "CliSelectionForCodeOfPractice3" will be introduced in order to provision "per Trunk Group" which level of CLI selection should be employed when sending the Calling Line Identities (such as Calling Party Number or Generic Number parameter) to the succeeding exchange. 0 - Indicates no specific CLI selection. 1 - Indicates Single CLI selection 2 - Indicates Dual (double) CLI selection Property Valid Values: 0 to 2 Property Default Value: 0.
Inhibit Incoming Calling Name Display	This property inhibit the support of incoming calling name display in DPNSS and EISUP(HSI) protocols. "1" = inhibit incoming calling name display. "0" = enable incoming calling name display.
Inhibit Outgoing Calling Name Display	This property inhibit the support of outgoing calling name display in DPNSS and EISUP HSI) protocols. "1" = inhibit outgoing calling name display. "0" = enable outgoing calling name display.
Inhibit Incoming Connected Name Display	Enables or disables the inhibiting of the incoming connected name display in DPNSS and EISUP (HSI) protocols.
Inhibit Incoming Connected Number Display	This property inhibit the support of the incoming connected name display for call transfer in DPNSS and EISUP (HSI) protocols. "1" = inhibit incoming connected name display. "0" = enable incoming connected name display.
Inhibit Outgoing Connected Name Display	This property inhibit the support of the outgoing connected name display for call transfer in DPNSS and EISUP (HSI) protocols. "1" = inhibit outgoing connected name display. "0" = enable outgoing connected name display.
Inhibit Outgoing Connected Number Display	This property inhibit the support of the outgoing connected number display for call transfer in DPNSS and EISUP (HSI) protocols. "1" = inhibit outgoing connected number display. "0" = enable outgoing connected number display.
Orig Label	Origination Location Label
Term Label	Termination Location Label
DTMF Cap	The DTMF capability in A-number or B-number analysis.
ITP Action Request	The indication of the required ITP action
Inhibit Sip From Mapping	Decides the mapping from incoming SIP message to ISUP CLI
Map Redirecting Number Method	Decides the mapping from ISUP Redirecting Number and Original Called Number to outgoing SIP/EISUP message
Default	Default trunk group of SIP/EISUP PATH for incoming call
Propagate Delay Counter	Propagation Delay counter. Indicates the propagation delay value in ms that will be increased if propagation delay is available.

Using Diagnostic Tools

When you need to troubleshoot Cisco PGW 2200 Softswitch node devices, you can use the Diagnostics dialog box to access a variety of diagnostic tools. The Diagnostics dialog box provides shortcuts for common diagnostics that normally require using UNIX or MML commands. For example, you can use the ping application to determine if a device is not responding because of an SNMP agent failure or a true network connectivity failure.

After the command is run, the results in the Action Result window displays. If the diagnostic command generates more information than can be shown in the Action Result window, the results are written to a file and the name of that file displays. The file can be retrieved and analyzed by external systems.

Note Many diagnostic commands are time consuming to run. Take this into account when planning your use of diagnostic tools.

Related Topics

The "Using Cisco MNM To Launch Device Configuration" section on page 8-4 describes how to use various configuration and diagnostic tools such as Cisco VSPT, CiscoView, and launching Telnet (or ssh) or X-windows to a device.

The "Using the MGC Toolbar" section on page 8-67 describes how to use the Cisco PGW 2200 Softswitch Toolbar, a diagnostic component of the Cisco PGW 2200 Softswitch software.

Use the following procedure to run diagnostics on a Cisco PGW 2200 Softswitch node device:

Step 1 In the Map Viewer window, select the desired device and right-click.

Note Alternatively, if you have an Accounts, Properties, States, or File Systems dialog box open for the device, you can use the dialog box Navigation menu to open the Diagnostics dialog box.

Step 2 Choose **[Device Name] Diagnostics** or **Tools > [Device Name] Diagnostics**.

The Diagnostics dialog box for the selected device opens.

Note You can use the Navigation menu to open the Properties, File Systems (where applicable), Accounts, or States dialog box for the selected component.

Step 3 Select the desired diagnostic option. For details, see the "About the Diagnostics Dialog Box" section on page 8-66.

You are asked to confirm the operation.

Step 4 Click **Yes** to confirm or **No** if you decide not to continue.

An Action Report box displays containing the results of the diagnostic operation or the name of the file to which the results have been saved.

Step 5 Review the results, and then click **Close** to close the Action Report box.

About the Diagnostics Dialog Box

The Diagnostics dialog box lets you run common UNIX and MML diagnostic commands from Cisco MNM without knowing any UNIX or MML or having to launch an X window to connect to the device.

For the Cisco PGW 2200 Softswitch host and the HSI host, the dialog box contains two tabs: the Diagnostics tab and the Advanced tab, which provides status check functions. For all other devices, the dialog box contains the Diagnostics option only.

The Diagnostics dialog box includes a Navigation menu that allows navigating directly to Properties, Accounts, File Systems (where applicable), or States dialog boxes for the selected component, without having to reselect the component in the Map Viewer. See Chapter 3, "Getting Started with Cisco MNM," "Navigating between Dialog Boxes for a Given Component" on page 31 for details.

Table 8-18 describes the diagnostic tools available from the Diagnostics dialog box General tab. Table 8-19 describes the tools available for the Cisco PGW 2200 Softswitch host from its Diagnostics dialog box Advanced tab. Table 8-20 describes the tools available for the Cisco HSI host from its Diagnostics dialog box Advanced tab.

Table 8-18   Cisco PGW 2200 Softswitch Diagnostics Dialog Box General Tab

Diagnostic Tool	Command	Available Devices	Description
IP Ping	—	Cisco PGW 2200 Softswitch host, BAMS, Cisco ITP-L, Cisco LAN Switch	Performs standard UNIX ping application on the device to see if its management interface is reachable
SNMP Ping	—	All IP devices	Makes an SNMP request to the device to determine if its SNMP agent is running and accessible
Traceroute	—	All IP devices	Determines the route that packets take from Cisco MNM to the device's management interface
Alarm Log	rtrv-alms	Cisco PGW 2200 Softswitch host, HSI server, and BAMS	Displays and saves current alarm log information
Process Status	rtrv-softw:all	Cisco PGW 2200 Softswitch host, HSI server, and BAMS	Displays and saves current status of all device processes
System Log	RTRV-FILES:: /acec/files/syslog	BAMS	Displays the BAMS system log
Cross-Device Audit	prov-rtrv:trunkgrp	BAMS	Audits BAMS trunk groups against the Cisco PGW 2200 Softswitch host configuration, producing a list of discrepancies, if any

Table 8-19   Cisco PGW 2200 Softswitch Diagnostics Dialog Box Advanced Tab

Option	MML Command[1]	Description
1	rtrv-admin-state	Retrieves the administrative state for all (applicable) components
2	rtrv-dest	Retrieves state information for all DPCs[2] and signaling paths
3	rtrv-lnk-ctr	Retrieves the service state of all linksets
4	rtrv-lssn	Retrieves the state of all local SSNs
5	rtrv-ne-health	Retrieves CPU occupancy and disk utilization
6	rtrv-rssn	Retrieves the state of all remote SSNs[3]
7	rtrv-rte	Retrieves the SS7 routes for all point codes
8	rtrv-sc	Retrieves the state of all signaling channels and linksets
9	rtrv-tc	Retrieves the state of bearers for all signaling paths
10	rtv-association	Retrieves the state of all associations
11	rtrv-dest:all	Retrieves the state of all DPNSS paths
12	rtrv-lics	Retrieves the license status
13	rtrv-h248:cntxs:sigpath="all",cntxid="all"	Retrieves all the H.248 context information
14	rtrv-ovld	Retrieves information on overload level and number of messages in a queue
15	rtrv-loclabel	Retrieves location labels information

1. The MML command invoked by the Status Check options, which runs in the background

2. Destination point codes

3. Subsystem numbers

Table 8-20   Cisco HSI Host Diagnostics Dialog Box, Advanced Tab

Option	Description
Configuration	Displays current configuration of the HSI host using the rtrv-config command
HSI Link Status	Displays current status of the IP/EISUP links
HSI Host Status	Displays current status of the HSI host
HSI License Status	Display current status of the license

Using the MGC Toolbar

From Cisco MNM, you can access the MGC toolbar (see Figure 8-2), a standalone diagnostic component of the Cisco PGW 2200 Softswitch software. The toolbar contains a suite of tools for viewing diagnostic and troubleshooting information.

Figure 8-2   *MGC Toolbar*

From the MGC Toolbar you can access these viewers:

- Alarm and Measurement Viewer—Search and view alarms and system statistics.
- Call Detail Record (CDR) Viewer—Search and view call detail records (CDRs).
- CONFIG-LIB Viewer—Manage the contents of the configuration library.
- Log Viewer—Search and view system logs.
- Trace Viewer—View and navigate through call trace output.
- Translation Verification—View called number analysis results.
- File Options—A tool to manage these toolkit files.

Instructions for using the toolbar are provided in Chapter 3, "Using the Cisco MGC Viewer Toolkit" section in the *Cisco PGW 2200 Softswitch Release 9 Operations, Maintenance, and Troubleshooting Guide* at

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/maintenance/guide/omtguide.html

Cisco MNM System Administration

Revised: December 15, 2009, OL-18339-03

This chapter is intended for system administrators. After a short overview of Cisco Media Gateway Controller (MGC) Node Manager (MNM) system administration, this chapter provides information on common system administration tasks.

Related Topics

Appendix C, "Troubleshooting Cisco MNM"

System administration procedures related to Cisco MNM features are described in the relevant chapters. For example, system administration related to performance management is described in "Managing the Performance of Cisco MNM Devices," "System Administration for Performance Management" section on page 7-17.

Note There is no special system administration related to implementing a secure shell (SSH) security policy. Define a component's security policy during deployment (see Chapter 5, "Deploying Your Network in Cisco MNM") and change it in the Accounts dialog box (see Chapter 8, "Other Network Management Tasks," "Viewing or Modifying Account and SNMP Information" section on page 8-6). To enable SSH on Cisco MNM, see the *Cisco Media Gateway Controller Node Manager Installation Guide* at http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/prod_installation_guides_list.html.

Overview of Cisco MNM System Administration

The Cisco MNM system administrator typically performs the following tasks:

- In initial implementation of Cisco MNM:
  - Installation of the software, including planning the necessary hardware for your site. This is described in the installation guide.
  - Configuration of the managed network devices for management by Cisco MNM. This is described in Chapter 2, "Configuring Network Devices for Management."
  - Setting up system security. This is described in Chapter 4, "Setting Up Cisco MNM Security."
- In day-to-day network management:
  - Stopping and Starting Cisco PGW 2200 Softswitch Node Devices, page 9-2
  - Backing Up and Restoring the Cisco MNM Database, page 9-3

> **Note** The Network Operations Center (NOC) operator uses Cisco MNM to monitor the network and respond to events and alarms. In this document, this role is called the user.

Stopping and Starting Cisco PGW 2200 Softswitch Node Devices

From Cisco MNM, a system administrator can reboot, shut down, or restart the Cisco PGW 2200 Softswitch host, the Cisco HSI server, the Cisco Billing and Measurements Server (BAMS), the Cisco ITP-L, or the Cisco LAN switch.

> **Note** Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, ITP-L will replace SLT in publications and the product.

Use the following procedure to stop, start, or reboot a device:

Step 1 In the Map Viewer window, right-click the desired device, and choose **Tools > Administration Tool**.

> **Note** You must have system administrator privileges to access the Administration Tool.

Step 2 The Administration dialog box for the selected device displays (Figure 9-1), showing the current state of the device.

Figure 9-1   Administration Dialog Box Example
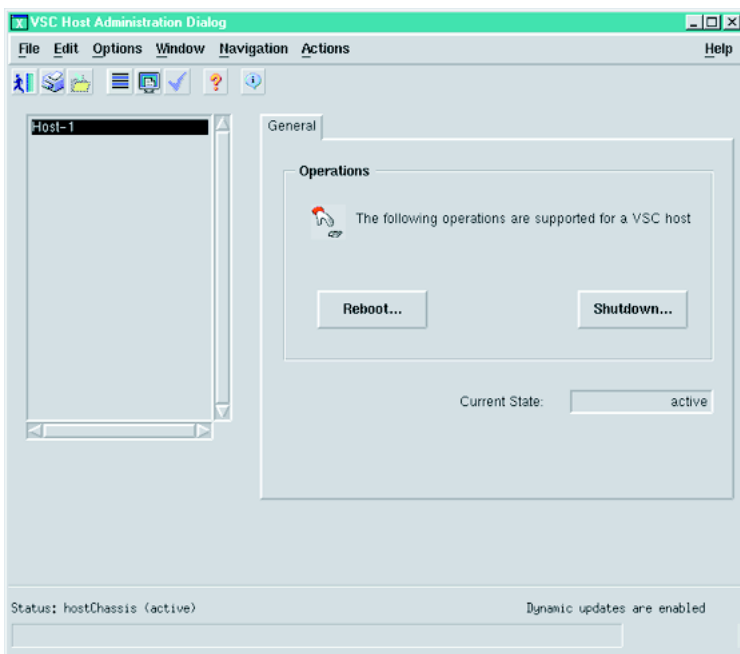
Step 3 Do one of the following:

- To reboot, click **Reboot**.

- To shut down, click **Shutdown**.

You are asked to confirm the operation

Step 4   Click **Yes** to proceed.

Cisco MNM executes the operation.

Step 5   When you are done, press **Alt-F4** or choose **File > Close** to close the dialog box.

Backing Up and Restoring the Cisco MNM Database

Cisco MNM maintains information about your network in database and configuration files that are together referred to as the Cisco MNM database. Use the backup and restore features of the Cisco EMF to back up or restore the Cisco MNM database. For details, see the *Cisco Element Management Framework Installation and Administration Guide* for your release of Cisco EMF at

http://www.cisco.com/en/US/docs/net_mgmt/element_manager_system/3.2/installation/guide/install_1.html

Alarm Message Reference

Revised: December 15, 2009, OL-18339-03

This section provides reference information about alarm messages displayed in the Cisco Media Gateway Controller (MGC) Node Manager (MNM) Event Browser. Specifically:

- For the Cisco PGW 2200 Softswitch and the Cisco Billing and Measurements Server (BAMS), this section provides:

   – References from which you can navigate to the relevant document to find the message you are interested in (see the "Cisco PGW 2200 Softswitch Host Alarm Messages" section on page A-2 and the "Cisco BAMS Alarm Messages" section on page A-3). A short description of each document is included.

   – Instructions for looking up the desired message in the referenced document (see the "Looking Up Cisco PGW 2200 Softswitch and Cisco BAMS Alarm Messages" section on page A-2).

   – A list and short description of application-related alarm messages (see the "Cisco PGW 2200 Softswitch Host and Cisco BAMS Resource Alarms" section on page A-4).

- For the Cisco ITP-L and Cisco LAN Switches, this section lists messages and provides short descriptions (see the "Cisco ITP-L Alarm Messages" section on page A-5).

Note Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, ITP-L will replace SLT in publications and the product.

Overview of Cisco MNM Alarm Management

Cisco MNM converts traps received from managed devices to alarms which are displayed in the Event Browser. For the Cisco ITP-L and the Cisco LAN switches, each trap has a corresponding Cisco MNM alarm. For example, the linkDown trap from the Cisco ITP-L corresponds to the "Link down" event description in the Cisco MNM Event Browser. For the Cisco BAMS and the Cisco PGW 2200 Softswitch, the trap serves as an envelope that can carry any one of numerous alarm messages.

Note Cisco MNM 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 as they are deployed to support the Cisco PGW 2200 Softswitch node configuration.

In addition to device-specific traps, Cisco MNM generates internal alarms. Appendix C, "Troubleshooting Cisco MNM" provides an explanation of these internal messages.

Looking Up Cisco PGW 2200 Softswitch and Cisco BAMS Alarm Messages

Use this procedure to locate information for a specific alarm message.

Step 1 In the Event Browser, check the Object Name to determine the network object that generated the event, and note the event description.

Step 2 In this document, go to the section that applies to that object.

Step 3 Click 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.

Step 5 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 match exactly the generated message. You can search on a different part of the description string, or scroll through the document to find the message.

Cisco PGW 2200 Softswitch Host Alarm Messages

Cisco MNM handles the traps in Table A-1 from the Cisco PGW 2200 Softswitch hosts. Each trap is used as an envelope for alarms of that type.

Table A-1   Cisco PGW 2200 Softswitch Host Traps

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

For system messages information, see the *Cisco PGW 2200 Softswitch Release 9 Messages Reference* at

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/system/message/errmsg.html

The alarm documentation includes the following information on each event:

- Alarm category—Alarm/event message, corresponding to the event description in the Cisco MNM Event Browser.

- Description—Brief description of the 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. (The Event Browser lists 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 = Do not send an SNMP trap
  - 1 = Communication alarm
  - 2 = Quality of service alarm
  - 3 = Processing error alarm
  - 4 = Equipment error alarm
  - 5 = Environment error alarm
- Suggested Action—Recommendations for resolving the problem.

Cisco BAMS Alarm Messages

All Cisco BAMS alarms are carried on a single trap, the AlarmTrap, as shown in Table A-2.

Table A-2   BAMS Traps

Trap	MIB
nusageAlarmTrap	ACECOMM-NUSAGE-MIB

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

The *Cisco Billing and Measurements Server User's Guide* at http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/bams/3.30/guide/330_ug.html includes an appendix (Appendix A. Troubleshooting) 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 the 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, which generally corresponds to the event description in the Cisco MNM 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 might also describe how the BAMS responds to the specified error condition.

✎ **Note** The BAMS File Rename Failure alarm (POL115) must be manually cleared not only in Cisco MNM but also on the BAMS before new alarms of that type can be generated.

Cisco HSI Server Alarm Messages

The Cisco HSI adjunct generates autonomous messages, or events, to notify you of problems or atypical network conditions. Depending on the severity level, events are considered alarms or informational events. The Cisco HSI adjunct captures minor, major, and critical events and forwards them to the Cisco MNM.

The *Cisco H.323 Signaling Interface User Guide* at http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/hsi/4.3/guide/43ug.html provides details on these messages and their use in troubleshooting. The following information is provided for each alarm message:

- Description
- Severity Level and Trap Type
- Cause
- Troubleshooting Procedure

Cisco PGW 2200 Softswitch Host and Cisco BAMS Resource Alarms

Cisco MNM traps application-related events that occur on the Cisco PGW 2200 Softswitch host or the Cisco BAMS, as shown in Table A-3.

✎ **Note** You can also monitor the performance of the following Cisco PGW 2200 Softswitch host and Cisco BAMS system components: fixed disk storage used, processor load, RAM, and virtual memory used. See Appendix B, "Performance Measurements Reference," "Performance Data Collected for System Components" section on page B-11.

Table A-3   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 A-3   Resource Alarms (continued)

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 ITP-L Alarm Messages

Table A-4   Cisco ITP-L 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.
authenthicationFailure	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)

Cisco LAN Switch Alarm Messages

Catalyst 5500 and 6509 Alarms

Table A-5   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.

Table A-5   Catalyst 5500 Alarms (continued)

Alarm/Trap	MIB	Explanation
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 A-6   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.
authenthicationFailure	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)

Cisco PGW 2200 Softswitch Alarm Messages

The Cisco PGW 2200 Softswitch generates messages, or events, to notify you of problems or atypical network conditions. Depending on the severity level, events are considered alarms or informational events. Events with a severity level of critical, major, or minor are classified as alarms, and then reported to the built-in alarm relay unit (ARU). The alarms can be retrieved through MML and a Simple Network Management Protocol (SNMP) manager.

Alarms and informational events follow the Telcordia Transaction Language 1 (TL1) message format.

Alarms and informational events produce different system responses. An alarm is reported when an alarm state changes (assuming the alarm does not have a non-reported severity). It is a significant violation of existing management systems to report consecutive state changes, active or clear, for a particular alarm on a single entity.

An informational event is reported without a state change being required. It is a warning that an abnormal condition has occurred that does not require corrective action by the management center. An invalid protocol call state transition is an example of an informational event. The event needs to be reported, and if it is transient, there is no corrective action that can be initiated by the management center to fix the problem.

An informational event is reported once, upon occurrence, through the MML and SNMP interfaces. The MML interface must be in the RTRV-ALMS::CONT mode for the event to be displayed; it is not displayed in subsequent RTRV-ALMS requests.

Table A-7 defines the Cisco PGW 2200 Softswitch message components that are displayed by means of the RTRV-ALMS::CONT command in its state of listening for alarm events.

Table A-7   Cisco PGW 2200 Softswitch Message Components

Element	Description
systemid	The name of your device and its identifier.
YYYY-MM-DD	Year, month, and day of alarm or event.
hh-mm-ss-ms	Hour, minute, second, and millisecond of alarm or event, displayed in system time.
timezone	Time zone for which the system time is configured.
severity	Two-character indicator with the following descriptions: • *C—Critical alarm. Reported to the built-in ARU. • **—Major alarm. Reported to the built-in ARU. • *^—Minor alarm. Reported to the built-in ARU. • A^—Informational event. Research if you receive the same event frequently, because it may be an indicator of a more significant problem. • —(empty spaces in two leftmost columns.) Alarm/event has been cleared. "STATE=CLEARED" is displayed. These alarms are not reported to the built-in ARU. They can be obtained from your SNMP manager or by issuing the RTRV-ALMS::CONT MML command.
comp	MML name of the component that is generating the alarm/event. See the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* for more information about components.
almCat	Alarm category (or event category)—A text string that indicates whether the message is an alarm or an informational event and lists the MML alarm or event message. **Note** Despite its name, the alarm category field is used for both alarms and information events.
params	Supplemental parameters used to further clarify the alarm or event.
comment	Supplemental comment used to indicate cause or appropriate action. See the *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* for more information on clearing alarms.

Performance Measurements Reference

Revised: December 15, 2009, OL-18339-03

This appendix provides details on the performance measurements you might see in the Cisco Media Gateway Controller (MGC) Node Manager (MNM) Performance Manager. It includes:

Note The above is an exhaustive list of performance data on Cisco PGW 2200 Softswitch, Cisco BAMS, Cisco HSI, Cisco ITP, and Cisco LAN Switches. The performance data is available only when the objects or components to which the performance data is associated are supported and provisioned on the device and discovered by Cisco MNM.

Common Performance Data Collected for Several Devices

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

Common Performance Data Available on

- BAMS object
- HSI object
- Cisco PGW 2200 Softswitch host object

- SLT object

- LAN Switch object

✎

Note   A Cisco PGW 2200 Softswitch host object, which you can access in Host-View in Map Viewer, contains host devices along with the associated interfaces and system components. A Cisco PGW 2200 Softswitch node object, which you can access in MGC-Node-View in Map Viewer, contains all the logical components of the node and the Cisco PGW 2200 Softswitch host object.

Table B-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
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 B-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
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 B-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 PGW 2200 Softswitch

Performance Data Collected on Cisco PGW 2200 Softswitch Host Object

- IP performance counters (see Table B-1)
- TCP performance counters (see Table B-2)
- UDP performance counters (see Table B-3)
- The usage attributes (see Table B-4)

Performance Data Collected on Cisco PGW 2200 Softswitch Node Object

- The CALL measurement group, that tracks call processing volume (see Table B-5)
- The OVL (overload) group, that tracks overload statistics (see Table B-7)
- The STATE group, that tracks user-defined statistics (see Table B-8)

Performance Data Collected on Cisco PGW 2200 Softswitch Node Object > Signaling > Label Components

- The LABEL measurement group, that tracks rejected and successful calls per location (see Table B-6)

Other Performance Data Collected on Cisco PGW 2200 Softswitch

- Data on system components, such as RAM and disk space (see the "Performance Data Collected for System Components" section on page B-11).
- Data on signaling and trunk group components (see the "Performance Data Collected for Signaling and Trunk Group Components" section on page B-12).

Table B-4   Cisco PGW 2200 Softswitch 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 the system

Table B-5   CALL Measurement Group

Counter	Description
CALL: SuccCall TOT	Number of successful calls.
CALL: FailCall TOT	Number of failed calls.
CALL: RUFailCall TOT	Number of failed calls due to resource unavailable.
CALL: ORFailCall TOT	Number of failed calls due to other reasons.
CALL: OLFailCall TOT	Number of failed calls due to overload.
CALL: SuccRedirected TOT	Number of successful redirected call initiated by Cisco PGW 2200 Softswitch.
CALL: PrepaidAccess	This counter is incremented each time a prepaid IN service is invoked.

Table B-5   CALL Measurement Group (continued)

Counter	Description
CALL:PrepaidComplet	This counter is incremented each time a prepaid call reaches the connected state.
CALL:RLFailCall TOT	Total number of failed calls due to route list exhaustion.
CALL:INC T38 FAX REQUEST	This counter is incremented each time T.38 Fax tone is reported for H.323 – SS7 calls.
CALL:INC T38 FAX USED	This counter is incremented for each T.38 Fax Call successfully completed for H.323 – SS7 calls.
CALL:OTG T38 FAX REQUEST	This counter is incremented each time T.38 Fax tone is reported for SS7 – H.323 calls.
CALL:OTG T38 FAX USED	This counter is incremented for each T.38 Fax Call successfully completed for SS7 – H.323 calls.
CALL: CoFailCallTOT	Number of calls that failed due to a codec being unavailable.
CALL:RoInvokesSent	This counter is incremented each time an RO invocation request is internally generated and sent out over the DPNSS interface.
CALL:RoInvokesReceived	This counter is incremented each time an RO invocation request is received over the DPNSS interface at a point of inter-working.
CALL:RoCompleted	This counter is incremented each time the RO feature is actioned and concludes successfully.
CALL:RoDenialsSent	This counter is incremented each time an RO invocation request is refused by the PGW and sent out over the DPNSS interface.
CALL:RoDenialsReceived	This counter is incremented each time an RO rejection/refusal is received over the DPNSS interface.
CALL:InvalidMsgDestination	This counter is incremented each time an internal message cannot be delivered because the destination call reference does not exist (or no longer exists).
CALL: CallBackFeatureReq	This counter is incremented each time a CallBackRequest comes to PGW from DPNSS/CallManager.
CALL: CallBackFeatureReqCancel	This counter is incremented each time a CallBackRequestCancel comes to PGW from DPNSS/CallManager.
CALL: CallBackFeatureReqExpired	This counter is incremented each time a CallBackRequest from CallManager expires from its time to live value.
CALL:RoInvokesSent	This counter is incremented each time an RO invocation request is internally generated and sent out over the DPNSS interface.
CALL:RoInvokesReceived	This counter is incremented each time an RO invocation request is received over the DPNSS interface at a point of inter-working.
CALL:RoCompleted	This counter is incremented each time the RO feature is actioned and concludes successfully.

Table B-5   CALL Measurement Group (continued)

Counter	Description
CALL:RoDenialsSent	This counter is incremented each time an RO invocationrequest is refused by the PGW and sent out over the DPNSS interface.
CALL:RoDenialsReceived	This counter is incremented each time an RO rejection/refusal is received over the DPNSS interface.
CALL:InvalidMsgDestination	This counter is incremented each time an internal message cannot be delivered because the destination call reference does not exist (or no longer exists).
CALL: CallBackFeatureReq	This counter is incremented each time a CallBackRequest comes to PGW from DPNSS/CallManager.
CALL: CallBackFeatureReqCancel	This counter is incremented each time a CallBackRequestCancel comes to PGW from DPNSS/CallManager.
CALL: CallBackFeatureReqExpired	This counter is incremented each time a CallBackRequest from CallManager expires from its time to live value.
CALL:CTICBReq	This counter is incremented each time a Call Back request is received by the PGW from DPNSS, QSIG or Tunneled QSIG interfaces.
CALL:CTICBCancel	This counter is incremented each time a Call Back Cancellation is received by the PGW from DPNSS, QSIG, or Tunneled QSIG interfaces.
CALL:CallBackFreeNotification	This counter is incremented each time a Call Back Line Free Notification is received by the PGW from DPNSS, QSIG, or Tunneled QSIG interfaces.
CALL:CallBackCallSetup	This counter is incremented each time a Call Back Call set up request is received by the PGW from DPNSS, QSIG, or EISUP interfaces (with tunneled QSIG).
CALL:MessageWaitingIndication	This counter is incremented each time a Message Waiting Indication is received by the PGW over DPNSS, QSIG, Tunneled QSIG, or SIP.

Table B-6   Label Measurement Group

Counter	Description
LABEL:LabelRej TOT	Rejected calls per location
LABEL:LabelSucc TOT	Successful calls per location

Table B-7   OVL Group Performance Counters

Counter	Description
OVL:LVL1 Duration	Minutes in Level1 Overload Condition
OVL:LVL2 Duration	Minutes in Level2 Overload Condition

Table B-7   OVL Group Performance Counters

Counter	Description
OVL:LVL3 Duration	Minutes in Level3 Overload Condition
OVL:LVL0 Duration	Minutes in Level0 Overload Condition
OVL:LVL0-LVL1 TOT	Transitions from Level0 to Level1 Overload Condition
OVL:LVL0-LVL2 TOT	Transitions from Level0 to Level2 Overload Condition
OVL:LVL0-LVL3 TOT	Transitions from Level0 to Level3 Overload Condition

Table B-8   STATE Group Performance Counters

Counter	Description
STATE: CDB ReCord Xmit	Number of CDBs transmitted
STATE: User Count1	User-defined count 1
STATE: User Count2 ... User Count25	User-defined counts 2 through 25

Performance Data Collected for the Cisco BAMS

Performance Data Collected on Billing and Measurements Server (BAMS) Object

- IP performance counters (see Table B-1)
- TCP performance counters (see Table B-2)
- UDP performance counters (see Table B-3)
- The usage attributes (see Table B-9)

Other Performance Data Collected on BAMS

- Data on system components, such as RAM and disk space (see the "Performance Data Collected for System Components" section on page B-11).
- Trunk group data (see the "Performance Data Collected for Signaling and Trunk Group Components" section on page B-12).

Table B-9   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

Note   In the Map Viewer, access the Performance Manager for the trunk groups by selecting the Trunk Groups folder under the Cisco PGW 2200 Softswitch Node.

Performance Data Collected for the Cisco HSI Server

Performance Data Collected on HSI Object

- IP performance counters (see Table B-1)
- TCP performance counters (see Table B-2)
- UDP performance counters (see Table B-3)
- The usage attributes (see Table B-4)
- RAS Statistics (see Table B-37 on page B-35)
- Q931 Statistics (see Table B-38 on page B-35)
- H245 Statistics (see Table B-39 on page B-36)

Performance Data Collected for the Cisco ITP-L

Note Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, ITP-L will replace SLT in publications and the product.

Performance Data Collected on Cisco ITP-L Object

- IP performance counters (see Table B-1)
- TCP performance counters (see Table B-2)
- UDP performance counters (see Table B-3)
- other performance counters (see Table B-10)

Table B-10   Cisco ITP-L Performance Counters

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

Performance Data Collected for Cisco ITP-L TDM Interfaces

Performance Data Collected on Cisco ITP-L > TDM Interface Components

- Performance counters of TDM interface to the SS7 network (see Table B-11)

Note Data can be viewed only in raw, not summarized, form.

Table B-11   TDM Interface Performance Counters

Counter	Description
SNMP:RFC1406-MIB.dsx1*Table*BESs[1]	Number of bursty errored seconds
SNMP:RFC1406-MIB.dsx1*Table*CSSs	Number of controlled slip seconds

Table B-11   TDM Interface Performance Counters (continued)

SNMP:RFC1406-MIB.dsx1*Table*DMs	Number of degraded minutes
SNMP:RFC1406-MIB.dsx1*Table*ESs	Number of errored seconds
SNMP:RFC1406-MIB.dsx1*Table*LCVs	Number of line code violations
SNMP:RFC1406-MIB.dsx1*Table*LESs	Number of line errored seconds
SNMP:RFC1406-MIB.dsx1*Table*PCVs	Number of path coding violations
SNMP:RFC1406-MIB.dsx1*Table*SEFSs	Number of severely errored framing seconds
SNMP:RFC1406-MIB.dsx1*Table*SESs	Number of severely errored seconds
SNMP:RFC1406-MIB.dsx1*Table*UASs	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 LAN Switch

Performance Data Collected on Cisco LAN Switch Object

- IP performance counters (see Table B-1)
- TCP performance counters (see Table B-2)
- UDP performance counters (see Table B-3)

Performance Data Collected on Cisco IOS LAN Switch (Cisco 2900XL Switch)

- IP performance counters (see Table B-1)
- TCP performance counters (see Table B-2)
- UDP performance counters (see Table B-3)
- other performance data (see Table B-12)

Table B-12   IOS LAN Switch Performance Counters

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

Performance Data Collected on Cisco LAN Switch (Cisco Catalyst 5500 Switch and Catalyst 6509 Switch)

- IP performance counters (see Table B-1)
- TCP performance counters (see Table B-2)
- UDP performance counters (see Table B-3)
- other performance data (see Table B-13)

Table B-13   Catalyst LAN Switch Performance Counters

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

Performance Data Collected for the Cisco 2900XL LAN Switch Port

Performance Data Collected on Cisco 2900XL LAN Switch > Port Components

- Performance counts for port components (see Table B-14)

Note   Data can be viewed only in raw, not summarized form.

Table B-14   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 64kb
SNMP:CISCO-C2900-MIB.c2900PortTxMulticastFrames	Frames successfully transmitted (multicast)
SNMP:CISCO-C2900-MIB.c2900PortTxBroadcastFrames	Frames successfully transmitted (broadcast)

Performance Data Collected for Network Interfaces

Performance Data Collected on Cisco PGW 2200 Softswitch Host/ITP-L/BAMS/Catalyst Switch/HSI > Ethernet/Serial/Generic Interfaces

- Ethernet, serial, and generic interface performance data on Cisco PGW 2200 Softswitch Host, ITP-L, BAMS, Catalyst Switch and HSI object (see Table B-15)

Note   The TDM interface data applies only to the Cisco ITP-L. See Table B-11 on page B-8 for those measurements.

Table B-15   Network Interface Performance Counters[1]

Counter	Description
SNMP:IF-MIB.ifInErrors	Number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol
SNMP:IF-MIB.ifInOctets	Total number of octets received on the interface, including framing characters

Table B-15   Network Interface Performance Counters[1] (continued)

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 System Components

The performance of the Cisco PGW 2200 Softswitch host and BAMS system components (fixed disks, processors, RAM, and virtual memory) is monitored as described in the following tables.

Note
- Data can be viewed only in raw, not summarized form. Performance measurements on system components are collected by the CIAgent application, resident in Cisco MNM.

- Cisco MNM also traps application- and file-system-related events (resource alarms) that occur on the Cisco PGW 2200 Softswitch host and the BAMS. See Appendix A, "Alarm Message Reference."

Tip   System component measurements can be used for threshold crossing alarms. See Chapter 6, "Managing Faults with Cisco MNM."

Fixed Disk Measurements

Performance Data Collected on Cisco PGW 2200 Softswitch Host/BAMS > Fixed Disk Components
- Performance counts for each fixed disk object (see Table B-16)

Table B-16   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 Measurements

Performance Data Collected on Cisco PGW 2200 Softswitch Host/BAMS > Processor Components
- Performance counts for each processor object (see Table B-17)

Table B-17   Processor Performance Counters

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

RAM Measurements

Performance Data Collected on Cisco PGW 2200 Softswitch Host/BAMS > RAM Components

- Performance counts for each RAM object (see Table B-18)

Table B-18   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 Measurements

Performance Data Collected on Cisco PGW 2200 Softswitch Host/BAMS > Virtual Memory Components

- Performance counts for each virtual memory object (see Table B-19)

Table B-19   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

Performance Data Collected for Signaling and Trunk Group Components

Cisco MNM collects extensive performance information on most signaling and trunk group components. Use Table B-20 to find the measurement groups for **MGC Node Object > Signaling and Trunk Group Components**. See the appropriate measurement group heading for measurement descriptions. If you are viewing this document online, you can click the table number to go to the measurement group.

Unless otherwise stated, measurement units are occurrences.

Note The release of the Cisco PGW 2200 Softswitch you are using determines which components are supported. The table identifies which components are supported only in Release 9.x.

Table B-20   Lookup Table for Signaling and Trunk Group Measurement Groups

Component	Description	Measurement Groups
hostAssociation	Association between SCTP (Stream Control Transmission Protocol) end points	SCTP Association (Table B-40) IUA Association (Table B-41)
hostC7IpLink	C7 IP link	C7LNK (Table B-22) SC (Table B-28)
hostCASPath	CAS path	CAS (Table B-31)
hostDPNSSPath	DPNSS path	CALL (Table B-24)
hostDPC	Destination point code	SP (Table B-29) C7SP (Table B-23) ISUP (Table B-25) TUP (Table B-30) NUP (Table B-26)
hostEISUPPath	EISUP path	ACC (Table B-21) CALL (Table B-24) ISUP (Table B-25) SP (Table B-29)
hostIpFASPath	IP FAS path	ACC (Table B-21) PRI (Table B-27) SP (Table B-29)
hostLabel	Label	LABEL (Table B-6)
hostMGCPPath	MGCP path	ACC (Table B-21) SP (Table B-29)
hostNASPath	NAS path	ACC (Table B-21) SP (Table B-29)
hostSGP	SGP (SS7 Signaling Gateway Process), the representation of a local SCTP endpoint	M3UA SGP (Table B-42) SUA SGP (Table B-43)
hostSIPLink	SIP signal channel	SIPSP (Table B-32)
hostSIPPath	SIP signal path	SP (Table B-29) SIP (Table B-33) SIPSP (Table B-32)
hostSS7Path	SS7 path	ACC (Table B-21) C7SP (Table B-23) ISUP (Table B-25) NUP (Table B-26) SP (Table B-29) TUP (Table B-30)
hostTrunkGroup	Trunk group	ACC (Table B-21) BAM (Table B-34)
hostH248Path	H.248 Path	ACC (Table B-21) SP (Table B-29)

Measurement Groups for Signaling and Trunk Group Components

Performance Data Collected on Cisco PGW 2200 Softswitch Node Object > Signaling and Trunk Group Components

- Performance data for a signaling or trunk group component (see to)

To find out which measurement groups apply to the network component you are interested in, see .

Table B-21   Automatic congestion control (ACC) Measurement Group

Measurement	Description
ACC: CALL REJ	Number of calls rejected by ACC
ACC: CALL RE-RTE	Number of calls rerouted by ACC

Table B-22   C7 Link (C7LNK) Measurement Group

Measurement	Description
C7LNK: DUR IS	Duration in-server (in seconds)
C7LNK: DUR UNAVAIL	Duration unavailable (in seconds)
C7LNK: MSU DROP-CONG	Total messages dropped due to congestion
C7LNK: RCV SIO TOT	Total realignments (SIF/SIO) received
C7LNK: RCV SU ERR	Total number of signaling units received
C7LNK: XMIT SIO TOT	Total realignments (SIF/SIO) transmitted

Table B-23   C7SP Measurement Group

Measurement	Description
C7SP: SP DUR UNAVAIL	Duration unavailable (in seconds)
C7SP: XMIT MSU DROP/RTE	Total number of messages dropped due to routing failure

Table B-24   Call Measurement Group

Measurement	Description
CALL: CallBackCallSetup	This counter increments each time a Call Back Call set up request is received by the Cisco PGW 2200 Softswitch from DPNSS, QSIG, or EISUP (with tunneled QSIG) interfaces.
CALL: CallBackFreeNotification	This counter increments each time a Call Back Line Free Notification is received by the Cisco PGW 2200 Softswitch from DPNSS, QSIG, or Tunneled QSIG interfaces.
CALL: CTICBCancel	This counter increments each time a Call Back Cancellation comes to the Cisco PGW 2200 Softswitch from DPNSS, QSIG, or Tunneled QSIG interfaces.

Table B-24   Call Measurement Group (continued)

CALL: CTICBReq	This counter increments each time a Call Back request comes to the Cisco PGW 2200 Softswitch from DPNSS, QSIG, or Tunneled QSIG interfaces.
CALL: FailCall TOT	Number of failed called
CALL: MessageWaitingIndication	This counter increments each time a Message Waiting Indication is received by the Cisco PGW 2200 Softswitch over DPNSS, QSIG, Tunneled QSIG, or SIP.
CALL: OLFailCall TOT	Failed calls due to an overload
CALL: ORFailCall TOT	Failed calls due to other reasons
CALL: RUFailCall TOT	Failed calls due to unavailable resources
CALL: SuccCall TOT	Number of successful calls
CALL: TimesTenLicRej TOT	Number of Timesten call rejected because of licensing

Table B-25   ISDN User Part (ISUP) Measurement Group

Measurement	Description
ISUP: ABN REL TOT	Total number of abnormal clears
ISUP: AOC TOT	Total number of calls that have invoked the Advice-of-Charge feature
ISUP: CHAN MATE UNAVAILABLE	Total number of channel mates that are unavailable
ISUP: FAIL_H323_ORIG	Number of failed calls that originated in an H323 network
ISUP: FAIL_H323_TERM	Number of failed calls that terminated in an H323 network
ISUP: RCV ACM TOT	Number of ACMs received
ISUP: RCV ANM TOT	Number of ANMs received
ISUP: RCV APM TOT	Number of APMs received
ISUP: RCV BELGACOM1 TOT	Number of BELGACOM1s received
ISUP: RCV BELGACOM1 TOT	ISDN UserPart: BELGACOM1 rcv total
ISUP: RCV BELGACOM2 TOT	Number of BELGACOM2s received
ISUP: RCV BELGACOM2 TOT	ISDN UserPart: BELGACOM2 rcv total
ISUP: RCV BLA TOT	Number of BLAs received
ISUP: RCV BLO TOT	Number of BLOs received
ISUP: RCV CCL TOT	Number of CCLs received
ISUP: RCV CCR TOT	Number of CCRs received
ISUP: RCV CFN TOT	Number of CFNs received
ISUP: RCV CGB TOT	Number of CGBs received
ISUP: RCV CGBA TOT	Number of CGBAs received
ISUP: RCV CGU TOT	Number of CGUs received

Table B-25   ISDN User Part (ISUP) Measurement Group (continued)

Measurement	Description
ISUP: RCV CGUA TOT	Number of CGUAs received
ISUP: RCV CHG TOT	Number of CHGs received
ISUP: RCV CHG TOT	ISDN UserPart: CHG rcv total
ISUP: RCV COM TOT	Number of COMs received
ISUP: RCV CON TOT	Number of CONs received
ISUP: RCV COT TOT	Number of COTs received
ISUP: RCV CPG TOT	Number of CPGs received
ISUP: RCV CQM TOT	Number of CQMs received
ISUP: RCV CQR TOT	Number of CQRs received
ISUP: RCV CRA TOT	Number of CRAs received
ISUP: RCV CRG TOT	Number of CRGs received
ISUP: RCV CRM TOT	Number of CRMs received
ISUP: RCV CVR TOT	Number of CVRs received
ISUP: RCV CVT TOT	Number of CVTs received
ISUP: RCV EOH TOT	ISDN UserPart: EOH rcv total
ISUP: RCV EOHA TOT	ISDN UserPart: EOHA rcv total
ISUP: RCV EXM TOT	Number of EXMs received
ISUP: RCV FAA TOT	Number of FAAs received
ISUP: RCV FAC TOT	Number of FACs received
ISUP: RCV FAD TOT	Number of FADs received
ISUP: RCV FAR TOT	Number of FARs received
ISUP: RCV FLA TOT	Number of FLAs received
ISUP: RCV FOT TOT	Number of FOTs received
ISUP: RCV FRJ TOT	Number of FRJs received
ISUP: RCV FWT TOT	ISDN UserPart: FWT rcv total
ISUP: RCV GRA TOT	Number of GRAs received
ISUP: RCV GRS TOT	Number of GRSs received
ISUP: RCV IAM TOT	Number of IAMs received
ISUP: RCV IDR TOT	ISDN UserPart: IDR rcv total
ISUP: RCV INF TOT	Number of INFs received
ISUP: RCV INR TOT	Number of INRs received
ISUP: RCV IRS TOT	ISDN UserPart: IRS rcv total
ISUP: RCV ITX TOT	Number of ITXs received
ISUP: RCV LPA TOT	Number of LPAs received
ISUP: RCV LPM TOT	ISDN UserPart: LPM rcv total
ISUP: RCV MCID TOT	ISDN UserPart: MCID rcv total

Table B-25   ISDN User Part (ISUP) Measurement Group (continued)

Measurement	Description
ISUP: RCV MCP TOT	ISDN UserPart: MCP rcv total
ISUP: RCV MCT TOT	Number of MCTs received
ISUP: RCV MPM TOT	Number of MPMs received
ISUP: RCV MSG TOT	Total messages received
ISUP: RCV NRM TOT	ISDN UserPart: NRM rcv total
ISUP: RCV OFR TOT	Number of OFRs received
ISUP: RCV OPR TOT	ISDN UserPart: OPR rcv total
ISUP: RCV PAM TOT	Number of PAMs received
ISUP: RCV PRI TOT	ISDN UserPart: PRI rcv total
ISUP: RCV REL TOT	Number of RELs received
ISUP: RCV RES TOT	Number of RESs received
ISUP: RCV RLC TOT	Number of RLCs received
ISUP: RCV RNG TOT	Number of RNGs received
ISUP: RCV RSC TOT	Number of RSCs received
ISUP: RCV SAM TOT	Number of SAMs received
ISUP: RCV SDM TOT	Number of SDMs received
ISUP: RCV SGM TOT	Number of SGMs received
ISUP: RCV SUS TOT	Number of SUSs received
ISUP: RCV TKO TOT	Number of TKOs received
ISUP: RCV TOF TOT	Number of TOFs received
ISUP: RCV TXA TOT	Number of TXAs received
ISUP: RCV UBA TOT	Number of UBAs received
ISUP: RCV UBL TOT	Number of UBLs received
ISUP: RCV UCIC TOT	Number of UCICs received
ISUP: RCV UPA TOT	Number of UPAs received
ISUP: RCV UPT TOT	Number of UPTs received
ISUP: RCV USR TOT	Number of USRs received
ISUP: SUCC_H323_ORIG	Number of successful calls that originated in an H323 network
ISUP: SUCC_H323_TERM	Number of successful calls that terminated in an H323 network
ISUP: UNEX MSG TOT	Total number of unexpected messages
ISUP: UNREC MSG TOT	Total number of unrecognized messages
ISUP: XMIT ACM TOT	Number of ACMs transmitted
ISUP: XMIT ANM TOT	Number of ANMs transmitted
ISUP: XMIT APM TOT	Number of APMs transmitted
ISUP: XMIT BELGACOM1 TOT	ISDN UserPart: BELGACOM1 xmitted total

Table B-25   ISDN User Part (ISUP) Measurement Group (continued)

Measurement	Description
ISUP: XMIT BELGACOM2 TOT	ISDN UserPart: BELGACOM2 xmitted total
ISUP: XMIT BLA TOT	Number of BLAs transmitted
ISUP: XMIT BLO TOT	Number of BLOs transmitted
ISUP: XMIT CCL TOT	Number of CCLs transmitted
ISUP: XMIT CCR TOT	Number of CCRs transmitted
ISUP: XMIT CFN TOT	Number of CFNs transmitted
ISUP: XMIT CGB TOT	Number of CGBs transmitted
ISUP: XMIT CGBA TOT	Number of CGBAs transmitted
ISUP: XMIT CGR TOT	Number of CGRs transmitted
ISUP: XMIT CGU TOT	Number of CGUs transmitted
ISUP: XMIT CGUA TOT	Number of CGUAs transmitted
ISUP: XMIT CHG TOT	ISDN UserPart: CHG xmitted total
ISUP: XMIT COM TOT	Number of COMs transmitted
ISUP: XMIT CON TOT	Number of CONs transmitted
ISUP: XMIT COT TOT	Number of COTs transmitted
ISUP: XMIT CPG TOT	Number of CPGs transmitted
ISUP: XMIT CQM TOT	Number of CQMs transmitted
ISUP: XMIT CQR TOT	Number of CQRs transmitted
ISUP: XMIT CRA TOT	Number of CRAs transmitted
ISUP: XMIT CRG TOT	Number of CRGs transmitted
ISUP: XMIT CRM TOT	Number of CRMs transmitted
ISUP: XMIT CVR TOT	Number of CVRs transmitted
ISUP: XMIT CVT TOT	Number of CVTs transmitted
ISUP: XMIT EOH TOT	ISDN UserPart: EOH xmitted total
ISUP: XMIT EOHA TOT	ISDN UserPart: EOHA xmitted total
ISUP: XMIT EXM TOT	Number of EXMs transmitted
ISUP: XMIT FAA TOT	Number of FAAs transmitted
ISUP: XMIT FAC TOT	Number of FACs transmitted
ISUP: XMIT FAD TOT	Number of FADs transmitted
ISUP: XMIT FAR TOT	Number of FARs transmitted
ISUP: XMIT FLA TOT	Number of FLAs transmitted
ISUP: XMIT FOT TOT	Number of FOTs transmitted
ISUP: XMIT FRJ TOT	Number of FRJs transmitted
ISUP: XMIT FWT TOT	ISDN UserPart: FWT xmitted total
ISUP: XMIT GRA TOT	Number of GRAs transmitted
ISUP: XMIT GRS TOT	Number of GRSs transmitted

Table B-25   ISDN User Part (ISUP) Measurement Group (continued)

Measurement	Description
ISUP: XMIT IAM TOT	Number of IAMs transmitted
ISUP: XMIT IDR TOT	ISDN UserPart: IDR xmitted total
ISUP: XMIT INF TOT	Number of INFs transmitted
ISUP: XMIT INR TOT	Number of INRs transmitted
ISUP: XMIT IRS TOT	ISDN UserPart: IRS xmitted total
ISUP: XMIT ITX TOT	Number of ITXs transmitted
ISUP: XMIT LPA TOT	Number of LPAs transmitted
ISUP: XMIT LPM TOT	ISDN UserPart: LPM xmitted total
ISUP: XMIT MCID TOT	ISDN UserPart: MCID xmitted total
ISUP: XMIT MCP TOT	ISDN UserPart: MCP xmitted total
ISUP: XMIT MCT TOT	Number of MCTs transmitted
ISUP: XMIT MPM TOT	Number of MPMs transmitted
ISUP: XMIT MSG TOT	Total messages transmitted
ISUP: XMIT NRM TOT	ISDN UserPart: RNG xmitted total
ISUP: XMIT OFR TOT	Number of OFRs transmitted
ISUP: XMIT OPR TOT	Number of OPRs transmitted
ISUP: XMIT OPR TOT	ISDN UserPart: OPR xmitted total
ISUP: XMIT PAM TOT	Number of PAMs transmitted
ISUP: XMIT PRI TOT	ISDN UserPart: PRI xmitted total
ISUP: XMIT REL TOT	Number of RELs transmitted
ISUP: XMIT RES TOT	Number of RESs transmitted
ISUP: XMIT RLC TOT	Number of RLCs transmitted
ISUP: XMIT RSC TOT	Number of RSCs transmitted
ISUP: XMIT SAM TOT	Number of SAMs transmitted
ISUP: XMIT SDM TOT	Number of SDMs transmitted
ISUP: XMIT SGM TOT	Number of SGMs transmitted
ISUP: XMIT SUS TOT	Number of SUSs transmitted
ISUP: XMIT TKO TOT	Number of TKOs transmitted
ISUP: XMIT TOF TOT	Number of TOFs transmitted
ISUP: XMIT TXA TOT	Number of TXAs transmitted
ISUP: XMIT UBA TOT	Number of UBAs transmitted
ISUP: XMIT UBL TOT	Number of UBLs transmitted
ISUP: XMIT UCIC TOT	Number of UCICs transmitted
ISUP: XMIT UPA TOT	Number of UPAs transmitted
ISUP: XMIT UPT TOT	Number of UPTs transmitted
ISUP: XMIT USR TOT	Number of USRs transmitted

Table B-26   National User Part (NUP) Measurement Group

Measurement	Description
NUP: RCV MSG TOT	Total number of messages received
NUP: UNEX MSG TOT	Total number of unexpected messages
NUP: XMIT MSG TOT	Total number of messages transmitted

Table B-27   PRI Measurement Group

Measurement	Description
PRI: CHAN MATE UNAVAILABLE	Total number of channel mates unavailable

Table B-28   Signal Channel (SC) Measurement Group

Measurement	Description
SC: RCV BAD CRC	Number of frames received with bad CRC
SC: RCV BAD TOT	Total number of bad frames received
SC: RCV FRMR	Number of bad FRMR responses
SC: RCV FRM TOT	Total number of frames received
SC: RCV RESET	Total number of resets received
SC: XMIT FRM TOT	Total number of frames transmitted

Table B-29   Signal Path (SP) Measurement Group

Measurement	Description
SP: Blacklist Call Ctr	Black list threshold counter
SP: CBReqExpired	Call Back request from the Cisco CallManager expires from its ttl
SP: cInit in	Number of call-init messages received
SP: cInit out	Number of call-init messages sent
SP: COT Failure	Number of COT failures
SP: PDU in	Number of messages received
SP: PDU out	Number of messages sent
SP: IPIN REJ TOT	Only available to hostSIPPath and hostEISUPPath components. Total number of rejected calls due to IPIN screening

Table B-30   Telephone User Part (TUP) Measurement Group

Measurement	Description
TUP: ABN REL TOT	Total number of abnormal clears
TUP: CHAN MATE UNAVAILABLE	Total number of channel mates that are unavailable
TUP: RCV ACB TOT	Number of ACBs received
TUP: RCV ACC TOT	Number of ACCs received
TUP: RCV ACF TOT	Number of ACFs received
TUP: RCV ACM TOT	Number of ACMs received
TUP: RCV ADI TOT	Number of ADIs received
TUP: RCV ANC TOT	Number of ANCs received
TUP: RCV ANN TOT	Number of ANNs received
TUP: RCV ANU TOT	Number of ANUs received
TUP: RCV AUU TOT	Number of AUUs received
TUP: RCV BLA TOT	Number of BLAs received
TUP: RCV BLO TOT	Number of BLOs received
TUP: RCV CBK TOT	Number of CBKs received
TUP: RCV CBU TOT	Number of CBUs received
TUP: RCV CCF TOT	Number of CCFs received
TUP: RCV CCL TOT	Number of CCLs received
TUP: RCV CCR TOT	Number of CCRs received
TUP: RCV CFL TOT	Number of CFLs received
TUP: RCV CGC TOT	Number of CGCs received
TUP: RCV CHA TOT	Number of CHAs received
TUP: RCV CHG TOT	Number of CHGs received
TUP: RCV CHP TOT	Number of CHPs received
TUP: RCV CHT TOT	Number of CHTs received
TUP: RCV CLF TOT	Number of CLFs received
TUP: RCV CLU TOT	Number of CLUs received
TUP: RCV COT TOT	Number of COTs received
TUP: RCV DPN TOT	Number of DPNs received
TUP: RCV EUM TOT	Number of EUMs received
TUP: RCV FOT TOT	Number of FOTs received
TUP: RCV GRA TOT	Number of GRAs received
TUP: RCV GRQ TOT	Number of GRQs received
TUP: RCV GRS TOT	Number of GRSs received
TUP: RCV GSE TOT	Number of GSEs received
TUP: RCV GSM TOT	Number of GSMs received
TUP: RCV HBA TOT	Number of HBAs received

Table B-30   Telephone User Part (TUP) Measurement Group (continued)

Measurement	Description
TUP: RCV HGB TOT	Number of HGBs received
TUP: RCV HGU TOT	Number of HGUs received
TUP: RCV HUA TOT	Number of HUAs received
TUP: RCV IAF TOT	Number of IAFs received
TUP: RCV IAI TOT	Number of IAIs received
TUP: RCV IAM TOT	Number of IAMs received
TUP: RCV ICF TOT	Number of ICFs received
TUP: RCV LOS TOT	Number of LOSs received
TUP: RCV MAL TOT	Number of MALs received
TUP: RCV MBA TOT	Number of MBAs received
TUP: RCV MGB TOT	Number of MGBs received
TUP: RCV MGU TOT	Number of MGUs received
TUP: RCV MPM TOT	Number of MPMs received
TUP: RCV MPR TOT	Number of MPRs received
TUP: RCV MSG TOT	Total number of messages received
TUP: RCV MUA TOT	Number of MUAs received
TUP: RCV NNC TOT	Number of NNCs received
TUP: RCV OPR TOT	Number of OPRs received
TUP: RCV RAN TOT	Number of RANs received
TUP: RCV RLG TOT	Number of RLGs received
TUP: RCV RSC TOT	Number of RSCs received
TUP: RCV SAM TOT	Number of SAMs received
TUP: RCV SAO TOT	Number of SAOs received
TUP: RCV SBA TOT	Number of SBAs received
TUP: RCV SCN TOT	Number of SCNs received
TUP: RCV SEC TOT	Number of SECs received
TUP: RCV SGB TOT	Number of SGBs received
TUP: RCV SGU TOT	Number of SGUs received
TUP: RCV SLB TOT	Number of SLBs received
TUP: RCV SNA TOT	Number of SNAs received
TUP: RCV SSB TOT	Number of SSBs received
TUP: RCV SST TOT	Number of SSTs received
TUP: RCV STB TOT	Number of STBs received
TUP: RCV SUA TOT	Number of SUAs received
TUP: RCV UBA TOT	Number of UBAs received
TUP: RCV UBL TOT	Number of UBLs received

Table B-30   Telephone User Part (TUP) Measurement Group (continued)

Measurement	Description
TUP: RCV UNN TOT	Number of UNNs received
TUP: RCV USR TOT	Number of USRs received
TUP: UNEX MSG TOT	Total number of unexpected messages
TUP: UNREC MSG TOT	Total number of unrecognized messages
TUP: XMIT ACB TOT	Number of ACBs transmitted
TUP: XMIT ACC TOT	Number of ACCs transmitted
TUP: XMIT ACF TOT	Number of ACFs transmitted
TUP: XMIT ACM TOT	Number of ACMs transmitted
TUP: XMIT ADI TOT	Number of ADIs transmitted
TUP: XMIT ANC TOT	Number of ANCs transmitted
TUP: XMIT ANN TOT	Number of ANNs transmitted
TUP: XMIT ANU TOT	Number of ANUs transmitted
TUP: XMIT AUU TOT	Number of AUUs transmitted
TUP: XMIT BLA TOT	Number of BLAs transmitted
TUP: XMIT BLO TOT	Number of BLOs transmitted
TUP: XMIT CBK TOT	Number of CBKs transmitted
TUP: XMIT CBU TOT	Number of CBUs transmitted
TUP: XMIT CCF TOT	Number of CCFs transmitted
TUP: XMIT CCL TOT	Number of CCLs transmitted
TUP: XMIT CCR TOT	Number of CCRs transmitted
TUP: XMIT CFL TOT	Number of CFLs transmitted
TUP: XMIT CGC TOT	Number of CGCs transmitted
TUP: XMIT CHA TOT	Number of CHAs transmitted
TUP: XMIT CHG TOT	Number of CHGs transmitted
TUP: XMIT CHP TOT	Number of CHPs transmitted
TUP: XMIT CHT TOT	Number of CHTs transmitted
TUP: XMIT CLF TOT	Number of CLFs transmitted
TUP: XMIT COT TOT	Number of COTs transmitted
TUP: XMIT DPN TOT	Number of DPNs transmitted
TUP: XMIT EUM TOT	Number of EUMs transmitted
TUP: XMIT FOT TOT	Number of FOTs transmitted
TUP: XMIT GRA TOT	Number of GRAs transmitted
TUP: XMIT GRQ TOT	Number of GRQs transmitted
TUP: XMIT GRS TOT	Number of GRSs transmitted
TUP: XMIT GSE TOT	Number of GSEs transmitted
TUP: XMIT GSM TOT	Number of GSMs transmitted

Table B-30   Telephone User Part (TUP) Measurement Group (continued)

Measurement	Description
TUP: XMIT HBA TOT	Number of HBAs transmitted
TUP: XMIT HGB TOT	Number of HGBs transmitted
TUP: XMIT HGU TOT	Number of HGUs transmitted
TUP: XMIT HUA TOT	Number of HUAs transmitted
TUP: XMIT LAF TOT	Number of LAFs transmitted
TUP: XMIT IAI TOT	Number of IAIs transmitted
TUP: XMIT IAM TOT	Number of IAMs transmitted
TUP: XMIT ICF TOT	Number of ICFs transmitted
TUP: XMIT LOS TOT	Number of LOSs transmitted
TUP: XMIT MAL TOT	Number of MALs transmitted
TUP: XMIT MBA TOT	Number of MBAs transmitted
TUP: XMIT MGB TOT	Number of MGBs transmitted
TUP: XMIT MGU TOT	Number of MGUs transmitted
TUP: XMIT MPM TOT	Number of MPMs transmitted
TUP: XMIT MPR TOT	Number of MPRs transmitted
TUP: XMIT MSG TOT	Number of messages transmitted
TUP: XMIT MUA TOT	Number of MUAs transmitted
TUP: XMIT NNC TOT	Number of NNCs transmitted
TUP: XMIT OPR TOT	Number of OPRs transmitted
TUP: XMIT RAN TOT	Number of RANs transmitted
TUP: XMIT RLG TOT	Number of RLGs transmitted
TUP: XMIT RSC TOT	Number of RSCs transmitted
TUP: XMIT SAM TOT	Number of SAMs transmitted
TUP: XMIT SAO TOT	Number of SAOs transmitted
TUP: XMIT SBA TOT	Number of SBAs transmitted
TUP: XMIT SCN TOT	Number of SCNs transmitted
TUP: XMIT SEC TOT	Number of SECs transmitted
TUP: XMIT SGB TOT	Number of SGBs transmitted
TUP: XMIT SGU TOT	Number of SGUs transmitted
TUP: XMIT SLB TOT	Number of SLBs transmitted
TUP: XMIT SNA TOT	Number of SNAs transmitted
TUP: XMIT SSB TOT	Number of SSBs transmitted
TUP: XMIT SST TOT	Number of SSTs transmitted
TUP: XMIT STB TOT	Number of STBs transmitted
TUP: XMIT SUA TOT	Number of SUAs transmitted
TUP: XMIT UBA TOT	Number of UBAs transmitted

Table B-30   Telephone User Part (TUP) Measurement Group (continued)

Measurement	Description
TUP: XMIT UBL TOT	Number of UBLs transmitted
TUP: XMIT UNN TOT	Number of UNNs transmitted
TUP: XMIT USR TOT	Number of USRs transmitted

Table B-31   CAS Measurement Group

Measurement	Description
CAS: IN CALL ATMPT TOT	Number of incoming CAS call attempt
CAS: IN CALL SUCC TOT	Number of incoming CAS call successes
CAS: IN SZR ATMPT TOT	Number of incoming CAS seizure attempt
CAS: IN SZR SUCC TOT	Number of incoming CAS seizure success
CAS: IN UNEXPECTED MSG	Number of incoming unexpected messages
CAS: OUT CALL ATMPT TOT	Number of outgoing CAS call attempt
CAS: OUT CALL SUCC TOT	Number of outgoing CAS call successes
CAS: OUT SZR ATMPT TOT	Number of outgoing CAS seizure attempts
CAS: OUT SZR SUCC TOT	Number of outgoing CAS seizure successes

Table B-32   SIP Link Measurement Group

Measurement	Description
SIPSP: BAD URL TOT	Total unresolved URL
SIPSP: DNS CACHE NEW TOT	Total new DNS cache entries
SIPSP: DNS CACHE PURGE TOT	Total purged DNS cache entries
SIPSP: DNS CACHE REFRESHED TOT	Total refreshed DNS cache entries
SIPSP: DNS QUERY TOT	Total DNS queries
SIPSP: DNS TIMEOUT TOT	Total DNS query timeouts
SIPSP: ICMP ERR TOT	Total ICMP errors
SIPSP: RCV FAIL TOT	Total failed received message
SIPSP: RCV MSG TOT	Total received message
SIPSP: RCV TCP MSG TOT	The total number of messages received though TCP.
SIPSP: RCV UDP MSG TOT	The total number of messages received through UDP.
SIPSP: XMIT FAIL TOT	Total failed transmitted message
SIPSP: XMIT MSG TOT	Total transmitted message
SIPSP: XMIT TCP MSG TOT	The total number of messages sent through TCP.
SIPSP: XMIT UDP MSG TOT	The total number of messages sent using UDP.

Table B-33   SIP Path Measurement Group

Measurement	Description
SIP: RCV 100 TOT	Total 100 (TRYING) messages received
SIP: RCV 180 TOT	Total 180 (RINGING) messages received
SIP: RCV 181 TOT	Total 181 (CALL FORWARDED) messages received
SIP: RCV 182 TOT	Total 182 (QUEUED) messages received
SIP: RCV 183 TOT	Total 183 (SESSION PROGRESS) messages received
SIP: RCV 200 TOT	Total 200 (OK) messages received
SIP: RCV 300 TOT	Total 300 (MULTIPLE CHOICES) messages received
SIP: RCV 301 TOT	Total 301 (MOVED PERMANENTLY) messages received
SIP: RCV 302 TOT	Total 302 (MOVED TEMPORARYLY) messages received
SIP: RCV 305 TOT	Total 305 (USE PROXY) messages received
SIP: RCV 380 TOT	Total 380 (ALTERNATIVE SERVICE) messages received
SIP: RCV 400 TOT	Total 400 (BAD REQUEST) messages received
SIP: RCV 401 TOT	Total 401 (UNAUTHORIZES) messages received
SIP: RCV 402 TOT	Total 402 (PAYMENT REQUIRED) messages received
SIP: RCV 403 TOT	Total 403 (FORBIDDEN) messages received
SIP: RCV 404 TOT	Total 404 (NOT FOUND) messages received
SIP: RCV 405 TOT	Total 405 (METHOD NOT ALLOWED) messages received
SIP: RCV 406 TOT	Total 406 (NOT ACCEPTABLE) messages received
SIP: RCV 407 TOT	Total 407 (PROXY AUTHENTICATION REQUIRED) messages received
SIP: RCV 408 TOT	Total 408 (REQUEST TIMEOUT) messages received
SIP: RCV 409 TOT	Total 409 (CONFLICT) messages received
SIP: RCV 410 TOT	Total 410 (GONE) messages received
SIP: RCV 411 TOT	Total 411 (LENGTH REQUIRED) messages received
SIP: RCV 413 TOT	Total 413 (REQUEST ENTITY TOO LARGE) messages received
SIP: RCV 414 TOT	Total 414 (REQUEST-URI TOO LONG) messages received
SIP: RCV 415 TOT	Total 415 (UNSUPPORTED MEDIA TYPE) messages received
SIP: RCV 420 TOT	Total 420 (BAD EXTENSION) messages received
SIP: RCV 480 TOT	Total 480 (TEMPORARILY UNAVAILABLE) messages received

Table B-33   *SIP Path Measurement Group (continued)*

Measurement	Description
SIP: RCV 481 TOT	Total 481 (CALL LEG/TRANSACTION DOES NOT EXIST) messages received
SIP: RCV 482 TOT	Total 482 (LOOP DETECTED) messages received
SIP: RCV 483 TOT	Total 483 (TOO MANY HOPS) messages received
SIP: RCV 484 TOT	Total 484 (ADDRESS INCOMPLETE) messages received
SIP: RCV 485 TOT	Total 485 (AMBIGUOUS) messages received
SIP: RCV 486 TOT	Total 486 (BUSY HERE) messages received
SIP: RCV 487 TOT	Total 487 (REQUEST CANCELED) messages received
SIP: RCV 500 TOT	Total 500 (INTERNAL SERVER ERROR) messages received
SIP: RCV 501 TOT	Total 501 (NOT IMPLEMENTED) messages received
SIP: RCV 502 TOT	Total 502 (BAD GATEWAY) messages received
SIP: RCV 503 TOT	Total 503 (SERVICE UNAVAILABLE) messages received
SIP: RCV 504 TOT	Total 504 (GATEWAY TIMEOUT) messages received
SIP: RCV 505 TOT	Total 505 (SIP VERSION NOT SUPPORTED) messages received
SIP: RCV 600 TOT	Total 600 (BUSY EVERYWHERE) messages received
SIP: RCV 603 TOT	Total 603 (DECLINE) messages received
SIP: RCV 604 TOT	Total 604 (DOES NOT EXIST ANYWHERE) messages received
SIP: RCV 606 TOT	Total 606 (NOT ACCEPTABLE) messages received
SIP: RCV ACK TOT	Total ACK messages received
SIP: RCV BYE TOT	Total BYE messages received
SIP: RCV CAN TOT	Total CANCEL messages received
SIP: RCV INV TOT	Total INVITE messages received
SIP: RCV INVALID MSG TOT	Total invalid messages received
SIP: RCV MSG TOT	Total messages received
SIP: RCV OPT TOT	Total OPTION messages received
SIP: RCV REG TOT	Total REGISTER messages received
SIP: RETX BYE TOT	Total BYE messages retransmitted
SIP: RETX CAN TOT	Total CANCEL messages retransmitted
SIP: RETX INV TOT	Total INVITE messages transmitted
SIP: RETX MSG TOT	Total messages retransmitted
SIP: RETX REG TOT	Total REGISTER messages retransmitted
SIP: RETX RESP TOT	Total RESPONSE messages retransmitted

Table B-33   SIP Path Measurement Group (continued)

Measurement	Description
SIP: SIP2SIP CALLS ATTEMPT	Total number of SIP to SIP calls attempted
SIP: SIP2SIP CALLS COMPL	Total number of SIP to SIP calls completed
SIP: XMIT 100 TOT	Total 100 (TRYING) messages transmitted
SIP: XMIT 180 TOT	Total 180 (RINGING) messages transmitted
SIP: XMIT 181 TOT	Total 181 (CALL FORWARDED) messages transmitted
SIP: XMIT 182 TOT	Total 182 (QUEUED) messages transmitted
SIP: XMIT 183 TOT	Total 183 (SESSION PROGRESS) messages transmitted
SIP: XMIT 200 TOT	Total 200 (OK) messages transmitted
SIP: XMIT 300 TOT	Total 300 (MULTIPLE CHOICES) messages transmitted
SIP: XMIT 301 TOT	Total 301 (MOVED PERMANENTLY) messages transmitted
SIP: XMIT 302 TOT	Total 302 (MOVED TEMPORARILY) messages transmitted
SIP: XMIT 305 TOT	Total 305 (USE PROXY) messages transmitted
SIP: XMIT 380 TOT	Total 380 (ALTERNATIVE SERVICE) messages transmitted
SIP: XMIT 400 TOT	Total 400 (BAD REQUEST) messages transmitted
SIP: XMIT 401 TOT	Total 401 (UNAUTHORIZES) messages transmitted
SIP: XMIT 402 TOT	Total 402 (PAYMENT REQUIRED) messages transmitted
SIP: XMIT 403 TOT	Total 403 (FORBIDDEN) messages transmitted
SIP: XMIT 404 TOT	Total 404 (NOT FOUND) messages transmitted
SIP: XMIT 405 TOT	Total 405 (METHOD NOT ALLOWED) messages transmitted
SIP: XMIT 406 TOT	Total 406 (NOT ACCEPTABLE) messages transmitted
SIP: XMIT 407 TOT	Total 407 (PROXY AUTHENTICATION REQUIRED) messages transmitted
SIP: XMIT 408 TOT	Total 408 (REQUEST TIMEOUT) messages transmitted
SIP: XMIT 409 TOT	Total 409 (CONFLICT) messages transmitted
SIP: XMIT 410 TOT	Total 410 (GONE) messages transmitted
SIP: XMIT 411 TOT	Total 411 (LENGTH REQUIRED) messages transmitted
SIP: XMIT 413 TOT	Total 413 (REQUEST ENTITY TOO LARGE) messages transmitted
SIP: XMIT 414 TOT	Total 414 (REQUEST-URI TOO LONG) messages transmitted

Table B-33 SIP Path Measurement Group (continued)

Measurement	Description
SIP: XMIT 415 TOT	Total 415 (UNSUPPORTED MEDIA TYPE) messages transmitted
SIP: XMIT 420 TOT	Total 420 (BAD EXTENSION) messages transmitted
SIP: XMIT 480 TOT	Total 480 (TEMPORARILY UNAVAILABLE) messages transmitted
SIP: XMIT 481 TOT	Total 481 (CALL LEG/TRANSACTION DOES NOT EXIST) messages transmitted
SIP: XMIT 482 TOT	Total 482 (LOOP DETECTED) messages transmitted
SIP: XMIT 483 TOT	Total 483 (TOO MANY HOPS) messages transmitted
SIP: XMIT 484 TOT	Total 484 (ADDRESS INCOMPLETE) messages transmitted
SIP: XMIT 485 TOT	Total 485 (AMBIGUOUS) messages transmitted
SIP: XMIT 486 TOT	Total 486 (BUSY HERE) messages transmitted
SIP: XMIT 487 TOT	Total 487 (REQUEST CANCELED) messages transmitted
SIP: XMIT 500 TOT	Total 500 (INTERNAL SERVER ERROR) messages transmitted
SIP: XMIT 501 TOT	Total 501 (NOT IMPLEMENTED) messages transmitted
SIP: XMIT 502 TOT	Total 502 (BAD GATEWAY) messages transmitted
SIP: XMIT 503 TOT	Total 503 (SERVICE UNAVAILABLE) messages transmitted
SIP: XMIT 504 TOT	Total 504 (GATEWAY TIMEOUT) messages transmitted
SIP: XMIT 505 TOT	Total 505 (SIP VERSION NOT SUPPORTED) messages transmitted
SIP: XMIT 600 TOT	Total 600 (BUSY EVERYWHERE) messages transmitted
SIP: XMIT 603 TOT	Total 603 (DECLINE) messages transmitted
SIP: XMIT 604 TOT	Total 604 (DOES NOT EXIST ANYWHERE) messages transmitted
SIP: XMIT 606 TOT	Total 606 (NOT ACCEPTABLE) messages transmitted
SIP: XMIT ACK TOT	Total ACK messages transmitted
SIP: XMIT BYE TOT	Total BYE messages transmitted
SIP: XMIT CAN TOT	Total CANCEL messages transmitted
SIP: XMIT INV TOT	Total INVITE messages transmitted
SIP: XMIT MSG TOT	Total messages transmitted
SIP: XMIT OPT TOT	Total OPTION messages transmitted
SIP: XMIT REG TOT	Total REGISTER messages transmitted

.

Table B-34   Trunk Group (BAM) Measurement Group

Measurement[1]	Description	Derivation for Selected Measurements
BAM:EGR CALL ATT	Outgoing call attempts	Pegged when a 1010 CDB is recorded w/4015 or when 1030 is recorded w/4015.
BAM:EGR CALL BLKD	Outgoing attempts blocked	4015 populated, 1030 or 1040 with (Cause Code) Tag {2008, 3008}== {21, 25, 27, 29, 34, 38, 41, 42, 44, 46, 47, 53, 63}.
BAM:EGR CONV DURATION	Conversation duration egress	—
BAM:EGR OFL BLKD	Overflow, outgoing attempts blocked	—
BAM:EGR PCT TRK USE	Percent trunk group usage outgoing	Measured as a percentage of time that circuits are occupied based on the total number of circuits belonging to a trunk group over the provisioned interval of measurement. Any circuit on Tag 4015 triggers this measurement from CDB Tag 1010. The starting time point is the earlier of 4100 or 4101; the end time point is in the 1040 CDB, the later of tag 4108 or 4109.
BAM:EGR SETUP DURATION	Setup duration egress	—
BAM:ERG SUCCESSFUL H.323	—	—
BAM:EGR TANDEM ATT	Tandem routing attempts, outgoing	—
BAM:EGR TANDEM COMPLT	Tandem completions, outgoing	—
BAM:EGR TANDEM DUR	Tandem duration, outgoing	—
BAM:EGR TEARDOWN DURATION	Teardown duration egress	—
BAM:EGR TERM NORM	Successful calls outgoing	Pegged when 1030 or 1040 CDB recorded with 4015 populated and {2008 or 3008} == {16, 17, 18, 19}.
BAM:ERG UNSUCCESSFUL H3.323	—	—
BAM:TTL FAILED CONGEST	—	Peg for all 1030 or 1040 where {2008 or 3008} == {42, 44, 47}.
BAM:IGR CALL ATT	Call attempts incoming	Pegged when a 1010 CDB is recorded w/4008 or when 1030 is recorded w/4008.
BAM:IGR CONV DURATION	Conversation duration ingress	—

Table B-34   Trunk Group (BAM) Measurement Group (continued)

Measurement[1]	Description	Derivation for Selected Measurements
BAM:IGR PCT TRK USE	Percent trunk group usage incoming	Measured as a percentage of time that circuits are occupied based on the total number of circuits belonging to a trunk group over the provisioned interval of measurement. Any circuit on Tag 4008 triggers this measurement from CDB Tag 1010. The starting time point is the earlier of 4100 or 4101; the end time point is in the 1040 CDB, the later of tag 4108 or 4109.
BAM:IGR SETUP DURATION	Setup duration ingress	—
BAM:IRG SUCCESSFUL H.323	—	—
BAM:IGR TANDEM ATT	—	—
BAM:IGR TANDEM COMPLT	Tandem completions, outgoing	—
BAM:IGR TANDEM DUR	Tandem duration, incoming	—
BAM:IGR TEARDOWN DURATION	Teardown duration ingress	—
BAM:IGR TERM NORM	Successful calls incoming	Peg for all 1030 or 1040 CDB where 4008 is populated and {2008 or 3008} == {16, 17, 18, 19}.
BAM:IRG UNSUCCESSFUL H.323	—	—
BAM:TTL CALL ROUTING I	—	—
BAM:TTL CALL ROUTING II	—	—
BAM:TTL CALL ROUTING III	—	—
BAM:TTL CALLS REJECTED	Calls rejected	—
BAM:TTL CARRIERSELECT PRESUBSCRIBED NIPT	—	—
BAM:TTL CARRIERSELECT PRESUBSCRIBED INPT	—	—
BAM:TTL CARRIERSELECT PRESUBSCRIBED WNI	—	—
BAM:TTL CARRIERSELECT NOTPRESUBSCRIBED	—	—
BAM:TTL ERLANGS	Total traffic in erlangs	—

Table B-34   Trunk Group (BAM) Measurement Group (continued)

Measurement[1]	Description	Derivation for Selected Measurements
BAM:TTL CIC DEFINED	Average number of defined CICs during the measurement period.	Number of circuits provisioned in the trunkgroup table.
BAM:TTL AVLBL CIC	Average number of available CICs during the measurement period.	= total - maintDuration / intervalLengthwheretotal = Total number of circuitsmaintDuration = total maintenance duration, see BAM:TTL MAINT USE below for details; intervalLength = total number of seconds for the measurement period.
BAM:TTL MAINT USE	Maintenance duration per trunk group	Measured as a percentage of time that circuits are unavailable, based on the total number of circuits belonging to a trunk.
BAM:TTL REJECTED DIALNUM	Calls rejected, unknown dialed number	—
BAM:TTL REJECTED OTHER	Calls rejected, other reasons	—
BAM:TTL TERM ABNORM	Calls terminated abnormally	—
BAM:TTL TERM FAILED MGW	Calls terminated, failed MGW or NAS	—
BAM:TTL TERM NORM	Total calls terminated normally	—
BAM:TTL TRAFFIC USAGE PEGS	Total sum of usage pegs per trunk group (not including maintenance pegs)	—
BAM:IGR CALL ANS	Answered Calls Incoming Pegged when a 1010 CDB is recorded with 4008, 4104, and 4105 populated	—
BAM:EGR CALL ANS	Answered Calls Outgoing egged when a 1010 CDB is recorded with 4015, 4104, and 4105 populated; not pegged for MGCP dial/script calls	—

Table B-34   Trunk Group (BAM) Measurement Group (continued)

Measurement[1]	Description	Derivation for Selected Measurements
BAM:TTL CALL ANS	Answered Calls Total	This equals the sum of "IGR CALL ANS" and "EGR CALL ANS" for the trunk group.
BAM:TTL CALL ATT	Call Attempts Total	This equals the sum of "IGR CALL ATT" and "EGR CALL ATT" for the trunk group.
BAMS:IGR ASR	Answer Seizure Ratio Incoming	This is calculated as percentage of "IGR CALL ANS" divided by "IGR CALL ATT", precision to 1 digit after the decimal point. For example, 92/96 = 95.8%. If the "IGR CALL ATT" is 0, then the value should be 100%.
BAMS:EGR ASR	Answer Seizure Ratio Outgoing	This is calculated as percentage of "EGR CALL ANS" divided by "EGR CALL ATT", precision to 1 digit after the decimal point. For example, 92/96 = 95.8%. If the "EGR CALL ATT" is 0, then the value should be 100%.
BAMS:TTL ASR	Answer Seizure Ratio Total	This is calculated as percentage of "TTL CALL ANS" divided by "TTL CALL ATT", precision to 1 digit after the decimal point. For example, 92/96 = 95.8%. If the "TTL CALL ATT" is 0, then the value should be 100%.
BAMS:TTL BH	Busy Hour	The hour during the day in which the hourly "TTL ERLANG" is greatest. This is displayed in the format of HHMM (in UTC). For example, 1400. This is based on the BAMS hourly measurements from the acc_h files.
BAMS:TTL BP	Busy Period	The measurement interval during the day in which "TTL ERLANG" (#13) is greatest among all acc_r files. This is displayed in the format of HHMM UTC, for the starting time of the interval. For example, with 15 minute intervals, 1415.

1. For a complete description of BAMS, see the Billing and Measurements Server User's Guide for your version of the BAMS.

Table B-35   TCAP (Transaction Capabilities Application Part) Measurement Group

Counter	Description
TCAP: MSG XMIT	Total TCAP messages transmitted.
TCAP:QWP XMIT	Total query with permission transmitted.

Table B-35   TCAP (Transaction Capabilities Application Part) Measurement Group (continued)

Counter	Description
TCAP:RSP XMIT	Total response messages transmitted.
TCAP:UNI XMIT	Total unidirectional messages transmitted.
TCAP:ABT XMIT	Total abort messages.
TCAP:MSG RCV	Total TCAP messages received.
TCAP:QWP RCV	Total query with permission received.
TCAP:RSP RCV	Total response messages received.
TCAP:UNI RCV	Total unidirectional messages received.
TCAP:MSG DROP	Total messages dropped.
TCAP:MSG UNREC	Total unrecognized messages.
TCAP:ABT RCV	Total abort messages received.
TCAP:BEGIN XMIT	Total number of TCAP BEGIN messages transmitted. This measurement is valid only for ETSI and ITU TCAP.
TCAP:BEGIN RCV	Total number of TCAP BEGIN messages received. This measurement is valid only for ETSI and ITU TCAP.
TCAP:END XMIT	Total number of TCAP END messages transmitted. This measurement is valid only for ETSI and ITU TCAP.
TCAP:END RCV	Total number of TCAP END messages received. This measurement is valid only for ETSI and ITU TCAP.
TCAP:CONTINUE XMIT	Total number of TCAP CONTINUE messages transmitted. This measurement is valid only for ETSI and ITU TCAP.
TCAP:CONTINUE RCV	Total number of TCAP CONTINUE messages received. This measurement is valid only for ETSI and ITU TCAP.
TCAP:CONV XMIT	Total number of TCAP CONVERSATION messages transmitted. This measurement is valid only for ETSI and ITU TCAP.
TCAP:CONV RCV	Total number of TCAP CONVERSATION messages received. This measurement is valid only for ETSI and ITU TCAP.

Table B-36   SCCP (Signaling Connection Control Part) Measurement Group

Counter	Description
SCCP:ROUTING FAILURE	Total routing failure
SCCP:UDT XMIT	Total unit data messages transmitted
SCCP:UDTS XMIT	Total unit data service messages transmitted
SCCP:UDT RCV	Total unit data messages received
SCCP:UDTS RCV	Total unit data service messages received
SCCP:TOTAL MSG	Total messages handled

Table B-37   RAS Measurement Group

Measurement	Description
RAS:GK DISC ATT TOT	Gatekeeper Discovery Attempts
RAS: GK REG ATT TOT	Registration Request Attempts
RAS:GK REG SUCC TOT	Registration Request Successes
RAS:GK RCV UNR ATT TOT	GK Initiated Unregistration Attempts
RAS:GK XMIT UNR SUCC TOT	GK Initiated Unregistration Successes
RAS:GK XMIT UNR ATT TOT	TC Initiated Unregistration Attempts
RAS: GK RCV UNR SUCC TOT	TC Initiated Unregistration Successes
RAS:GK RLS ATT TOT	Disengage Attempts
RAS:GK RLS SUCC TOT	Disengage Successes
RAS:GK INFO REPORT TOT	Information Reports

Table B-38   Q.931 Measurement Group

Measurement	Description
Q931:FC INC CALL ATT TOT	H.225 Incoming Fast Connect Call Attempts.
Q931:FC INC CALL SUCC TOT	H.225 Incoming Fast Connect Call Successes.
Q931:FC OTG CALL ATT TOT	H.225 Incoming Fast Connect Call Successes.
Q931:FC OTG CALL SUCC TOT	H.225 Outgoing Fast Connect Call Successes.
Q931:V1 INC CALL ATT TOT	H.225 Incoming Version 1 Call Attempts.
Q931:V1 INC CALL SUCC TOT	H.225 Incoming Version 1 Call Successes.
Q931:V1 OTG CALL ATT TOT	H.225 Outgoing Version 1 Call Attempts.
Q931:V1 OTG CALL SUCC TOT	H.225 Outgoing Version 1 Call Successes.
Q931:INC NORM REL TOT	H.225 Incoming Call Normal Releases.
Q931:INC ABNORM REL TOT	H.225 Incoming Call Abnormal Releases.
Q931:OTG NORM REL TOT	H.225 Outgoing Call Normal Releases.
Q931:OTG ABNORM REL TOT	H.225 Outgoing Call Abnormal Releases.
Q931:H323 INTERWORK SUCC TOT	H323-H323 hairpinned calls.
Q931:PGW T38 FAX ATT TOT	T.38 fax call requests.
Q931:PGW T38 FAX SUCC TOT	T.38 fax calls successfully reconfigured.
Q931:INC_ANNEX_M1_REJ_TOT	This counter is incremented each time an incoming H.323 call using Annex M1 is rejected by the HSI because it is disabled.
Q931: OTG_ANNEX_M1_REJ_TOT	This counter is incremented each time an outbound H.323 call using Annex M1 is rejected by the destination.

Table B-38   Q.931 Measurement Group (continued)

Measurement	Description
Q931: INC_ANNEX_M1_TOT	This counter is incremented each time an incoming H.323 call using Annex M1 is rejected by the HSI because it is disabled.
Q931: OTG_ANNEX_M1_TOT	This counter is incremented each time an incoming H.323 call using Annex M1 is rejected by the HSI because it is disabled.

Table B-39   H.245 Measurement Group

Measurement	Description
H245:MASTER SLAVE ATT TOT	H.245 Master Slave Determination Attempts
H245:MASTER SLAVE SUCC TOT	H.245 Master Slave Determination Successes
H245:TERM CAP XCHG ATT TOT	H.245 Terminal Capability Exchange Attempts
H245:TERM CAP XCHG SUCC TOT	H.245 Terminal Capability Exchange Successes
H245:OPEN CH ATT TOT	H.245 Open Logical Channel Attempts
H245:OPEN CH SUCC TOT	H.245 Open Logical Channel Successes
H245:CLOSE CH ATT TOT	H.245 Close Logical Channel Attempts
H245:CLOSE CH SUCC TOT	H.245 Close Logical Channel Successes
H245:AVG ROUND TRIP DELAY	H.245 Round Trip Delay Determination
H245:EMPTY CAP SET TOT	Total number of empty TCS exchanges
H245:H323 T38 FAX ATT TOT	Total of T.38 fax call requests from remote peer
H245:H323 T38 FAX SUCC TOT	Total of successfully reconfigured T.38 fax call requests from remote peer
H245:ASYMMETRIC TOT	Total of asymmetric conditions encountered
H245:DTMF RELAY TOT	Total calls using DTMF relay

Table B-40   SCTP Association Measurement Group

Counter	Description
SCTP: OOTB	Out of Blue Packets Received (ootb)
SCTP: InvalidChksum	Checksum Error Packets Received (invalidAdler)
SCTP: CtrlTx	Control Chunks Sent (numControlChunksSent)
SCTP: OrdDataTx	Ordered Data Chunks Sent (numDataChunksSentOrdered)
SCTP: UnordDataTx	Unordered Data Chunks Sent (numDataChunksSentUnordered)
SCTP: CtrlRx	Control Chunks Received (numControlChunksRcvd)
SCTP: OrdDataRx	Ordered Data Chunks Received (numDataChunksRcvdOrdered)
SCTP: UnordDataRx	Unordered Data Chunks Received (numDataChunksRcvdUnordered)
SCTP: DataSegTx	SCTP Data Segments Sent (numSctpDataDgramsSent)
SCTP: DataSegRx	SCTP Data Segments Received (numSctpDataDgramsRcvd)

Table B-40   SCTP Association Measurement Group (continued)

Counter	Description
SCTP: AssocFailures	Count of Association Failures (assocCommLost)
SCTP: DestFailures	Count of Destination Failures (destAddrFailed)
SCTP: PeerRestarted	Count of Peer Restarts (peerRestarted)

Table B-41   IUA Association Measurement Group

Counter	Description
IUA: ASPUpTx	Number of ASP Up messages sent from Cisco PGW 2200 Softswitch to the gateway on this SCTP association, indicating to gateway that it is ready to receive traffic or maintenance messages.
IUA: ASPUpAckRx	Numbers of ASP Up Acknowledgement messages received by the Cisco PGW 2200 Softswitch from the gateway on this SCTP association. These messages acknowledge ASP Up messages.
IUA: ASPDnTx	Number of ASP Down Sent messages sent from the Cisco PGW 2200 Softswitch to the gateway on this SCTP association, indicating to the gateway that it is NOT ready to receive traffic or maintenance messages.
IUA: ASPDnAckRx	Numbers of ASP Down Acknowledgement messages received by the Cisco PGW 2200 Softswitch from the gateway on this SCTP association. These messages acknowledge ASP Down messages.
IUA: ASPActTx	Number of ASP Active messages sent from Cisco PGW 2200 Softswitch to the gateway on this SCTP association, indicating to gateway that it is Active and ready to be used.
IUA: ASPActAckRx	Numbers of ASP Active Acknowledgement messages received by the Cisco PGW 2200 Softswitch from the gateway on this SCTP association. These messages acknowledge ASP Active messages.
IUA: ASPInactTx	Number of ASP Inactive messages sent from Cisco PGW 2200 Softswitch to the gateway on this SCTP association, indicating to gateway that it is no longer an active ASP.
IUA: ASPInactAckRx	Numbers of ASP Inactive Acknowledgement messages received by the Cisco PGW 2200 Softswitch from the gateway on this SCTP association. These messages acknowledge ASP Inactive messages.
IUA: ErrorRx	Numbers of Error messages received by the Cisco PGW 2200 Softswitch from the gateway on this SCTP association. These messages indicate various errors. See the platform log for information on individual errors.
IUA: NotifyRx	Numbers of Notify messages received by the Cisco PGW 2200 Softswitch from the gateway on this SCTP association. These messages provide autonomous indications of IUA events on the gateway.
IUA: DataRqt	Number of Data messages sent from Cisco PGW 2200 Softswitch to the gateway on this SCTP association, which are to be transmitted by the Q.921 layer using the acknowledged information transfer service.

Table B-41   IUA Association Measurement Group (continued)

Counter	Description
IUA: DataInd	Number of Data messages received by the Cisco PGW 2200 Softswitch from the gateway on this SCTP association, which have been received by the Q.921 layer using the acknowledged information transfer service.
IUA: UnitDataRqt	Number of Data messages sent from Cisco PGW 2200 Softswitch to the gateway on this SCTP association, which are to be transmitted by the Q.921 layer using the unacknowledged information transfer service.
IUA: UnitDataInd	Number of Data messages received by the Cisco PGW 2200 Softswitch from the gateway on this SCTP association, which have been received by the Q.921 layer using the unacknowledged information transfer service.
IUA: EstRqt	Number of requests to establish this SCTP association.
IUA: EstConf	Number of confirms that IUA has established an SCTP association with the gateway.
IUA: EstInd	Number of times the gateway has informed Link Management that the Cisco PGW 2200 Softswitch has established an SCTP association.
IUA: RelRqt	Number of requests to release an SCTP association with gateway.
IUA: RelConf	Number of confirms that IUA has released an SCTP association with the gateway.
IUA: RelInd	Number of times the gateway has informed Link Management that the Cisco PGW 2200 Softswitch has released an SCTP association.

Table B-42   M3UA SGP Measurement Group

Counter	Description
M3UA: ErrorTx	Number of error messages transmitted.
M3UA: ErrorRx	Number of error messages received.
M3UA: NotifyTx	Number of notify messages transmitted.
M3UA: NotifyRx	Number of notify messages received.
M3UA: DunaRx	Number of DUNA messages received.
M3UA: DavaRx	Number of DAVA messages received.
M3UA: DaudTx	Number of DAUD messages transmitted.
M3UA: SconRx	Number of SCON messages received.
M3UA: DrstRx	Number of DRST messages received.
M3UA: DupuRx	Number of DUPU messages transmitted.
M3UA: ASPUpTx	Number of ASP UP messages transmitted.
M3UA: ASPDnTx	Number of ASP DOWN messages transmitted.
M3UA: ASPUpAckRx	Number of ASP UP acknowledgements received.
M3UA: ASPDnAckRx	Number of ASP DOWN acknowledge messages received.
M3UA: ASPActTx	Number of ASP ACTIVE messages transmitted.
M3UA: ASPInactTx	Number of ASP INACTIVE messages transmitted.

Table B-42   M3UA SGP Measurement Group (continued)

Counter	Description
M3UA: ASPActAckRx	Number of ASP ACTIVE ACK messages received.
M3UA: ASPInactAckRx	Number of ASP INACTIVE ACK messages received.
M3UA: DataXferTx	Number of DATA transfer messages transmitted.
M3UA: DataXferRx	Number of DATA transfer messages received.
M3UA: DataBytesTx	Number of M3UA data bytes transmitted.
M3UA: DataBytesRx	Number of M3UA data bytes received.
M3UA: InvSctpSig	Number of invalid SCTP signals received by M3UA.
M3UA: AssocFail	Number of SCTP association failures.
M3UA: AssocTxFail	Number of transmit SCTP failures.
M3UA: RxVersionErr	Number of messages received with an invalid version.
M3UA: RxMsgClassErr	Number of received messages with an unexpected or unsupported Message Class.
M3UA: RxMsgTypeErr	Number of messages received with an unexpected or unsupported Message Type.
M3UA: RxMsgLenErr	Number of messages received with message length error.
M3UA: RxStrmIdErr	Number of messages received with stream ID error - when a message is received on an unexpected SCTP stream (for example, a Management message was received on a stream other than "0").
M3UA: RxUnexpMsgErr	Number of unexpected messages received. A defined and recognized message is received that is not expected in the current state.
M3UA: RxProtErr	Number of messages received with protocol errors - for any protocol anomaly (for example, a reception of a parameter that is syntactically correct but unexpected in the current state).
M3UA: RxParValErr	Number of messages received with parameter value errors.
M3UA: RxParmFieldErr	Number of messages received with a parameter having a wrong length field.
M3UA: RxUnexpParmErr	Number of messages received that contain one or more invalid parameters.
M3UA: RxNtwkAppErr	Number of messages received with an invalid (unconfigured) Network Appearance.
M3UA: RouteCntxErr	Number of messages received with an invalid (unconfigured) Routing Context.
M3UA: RxNoMemErr	Number of messages that were dumped because memory ran out (buffer overflow).

Table B-43   SUA SGP Measurement Group

Counter	Description
SUA: ErrorTx	Number of error messages transmitted.
SUA: ErrorRx	Number of error messages received.

Cisco Media Gateway Controller Node Manager User Guide

Table B-43   SUA SGP Measurement Group (continued)

Counter	Description
SUA: NotifyTx	Number of notify messages transmitted.
SUA: NotifyRx	Number of notify messages received.
SUA: DunaRx	Number of DUNA messages received.
SUA: DavaRx	Number of DAVA messages received.
SUA: DaudTx	Number of DAUD messages transmitted.
SUA: SconRx	Number of SCON messages received.
SUA: DrstRx	Number of DRST messages received.
SUA: DupuRx	Number of DUPU messages transmitted.
SUA: ASPUpTx	Number of ASP UP messages transmitted.
SUA: ASPDnTx	Number of ASP DOWN messages transmitted.
SUA: ASPUpAckRx	Number of ASP UP acknowledgements received.
SUA: ASPDnAckRx	Number of ASP DOWN acknowledge messages received.
SUA: ASPActTx	Number of ASP ACTIVE messages transmitted.
SUA: ASPInactTx	Number of ASP INACTIVE messages transmitted.
SUA: ASPActAckRx	Number of ASP ACTIVE ACK messages received.
SUA: ASPInactAckRx	Number of ASP INACTIVE ACK messages received.
SUA: CldtTx	Connectionless Data Transfers sent.
SUA: CldrRx	Connectionless Data Responses received.
SUA: DataBytesTx	Number of SUA data bytes transmitted.
SUA: DataBytesRx	Number of SUA data bytes received.
SUA: InvSctpSig	Number of invalid SCTP signals received by SUA.
SUA: AssocFail	Number of SCTP association failures.
SUA: AssocTxFail	Number of transmit SCTP failures.
SUA: RxVersionErr	Number of messages received with an invalid version.
SUA: RxMsgClassErr	Number of received messages with an unexpected or unsupported Message Class.
SUA: RxMsgTypeErr	Number of messages received with an unexpected or unsupported Message Type.
SUA: RxMsgLenErr	Number of messages received with message length error.
SUA: RxStrmIdErr	Number of messages received with stream ID error. When a message is received on an unexpected SCTP stream (for example, a Management message was received on a stream other than "0").
SUA: RxUnexpMsgErr	Number of unexpected messages received. A defined and recognized message is received that is not expected in the current state.
SUA: RxProtErr	Number of messages received with protocol errors - for any protocol anomaly (for example, a reception of a parameter that is syntactically correct but unexpected in the current state).
SUA: RxParmValErr	Number of messages received with parameter value errors.

Table B-43   SUA SGP Measurement Group (continued)

Counter	Description
SUA: RxParmFieldErr	Number of messages received with a parameter having a wrong length field.
SUA: RxUnexpParmErr	Number of messages received that contain one or more invalid parameters.
SUA: RxNtwkAppErr	Number of messages received with an invalid (unconfigured) Network Appearance.
SUA: RouteCntxErr	Number of messages received with an invalid (unconfigured) Routing Context.
SUA: RxNoMemErr	Number of messages that were dumped because memory ran out (buffer overflow).

APPENDIX C

Troubleshooting Cisco MNM

Revised: December 15, 2009, OL-18339-03

This section provides troubleshooting information for Cisco Media Gateway Controller (MGC) Node Manager (MNM) internal messages and for other common Cisco MNM issues.

Troubleshooting Cisco MNM Internal Messages

The following messages may be generated by Cisco MNM that reflect errors in deployment, discovery, or configuration. See the "Solving Deployment and Discovery Errors" section on page C-5 for information on how to correct deployment and discovery errors.

Table C-1   Cisco MNM Internal Events

Message	Explanation	Action
(Cisco PGW 2200 Softswitch host) Failed to collect active configuration	(1) FTP failed and the information is not getting to Cisco MNM. (2) The device is not generating the information.	On the Cisco PGW 2200 Softswitch host, run the **prov-exp** command to view the configuration information being generated. If it is OK, there is an FTP problem. If it is not OK, there is a problem with the Cisco PGW 2200 Softswitch host.
<Host name>: Could not collect inventory: Login ID or password or security policy is invalid.	Login or password is invalid for the deployed device, or the security policy attribute is mis-set. As a result, Cisco MNM cannot fully discover the device. See Troubleshooting SSH-Related Errors, page C-7, for help in pinpointing the problem.	Correct the login, password, or security policy attribute information (Accounts dialog box) and rediscover the device.

Table C-1   Cisco MNM Internal Events (continued)

Message	Explanation	Action
\<Host name>: Could not collect inventory: Password not specified.	Password is not specified for the deployed device. As a result, Cisco MNM cannot fully discover the device.	Correct the password information and rediscover the device.
\<Host name>: Could not get Host Device table. Check IP address and read-community string.	Cisco MNM 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 not running 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.
\<Host name>: Could not get Host Files System. Check IP address and read-community string.	Cisco MNM 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 not running 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.	Cisco MNM failed to retrieve the device table from the device. The problem may (1) Wrong SNMP community strings. (2) SNMP Agent or the hostagt process not running 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 C-1   *Cisco MNM Internal Events (continued)*

Message	Explanation	Action
Billing and Measurements Server (BAMS) is not configured to receive Call Data Records from any Cisco PGW 2200 Softswitch Host.	Since the BAMS is not configured to collect data from any Cisco PGW 2200 Softswitch Host, Cisco MNM cannot deploy the device to the right Cisco PGW 2200 Softswitch node, and its alarm status will not be propagated in the MGC-Node-View.	Check your BAMS configuration and check the Cisco PGW 2200 Softswitch status.
Cannot get IF description from the interface table.	The appropriate processes may not be running on the device.	On the Cisco PGW 2200 Softswitch host, determine the process IDs by entering this command **ps-ef|grep agt** Check that critagt, mibagt, hostagt, and snmpagt are running. If not, kill critagt and restart the processes. If the problem is not resolved, check if the interface type is one of Serial, Ethernet, Loopback, and SCO/SLO.
Could not get BAMS Poll table.	Cisco MNM failed to retrieve the 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, Cisco MNM cannot deploy the device to the correct Cisco PGW 2200 Softswitch node. Therefore, 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_ROOT>*/logs/mgcController.log.

Table C-1   Cisco MNM Internal Events (continued)

Message	Explanation	Action
Could not get IP Address table from <device name>. Check IP address and read-community string.	Cisco MNM 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. (4) Check if the interface type is one of Serial, Ethernet, Loopback, and SCO/SLO.
Could not get password for host <IP Address>.	Password is not specified for the deployed Cisco PGW 2200 Softswitch host. As a result, Cisco MNM cannot fully discover the device.	Correct the password information and rediscover the device.
Failed to launch action <Action name>. Perhaps hostController is not running.	The most probable cause is that the Cisco MNM process *hostController* is down while Cisco MNM is trying to discover a Cisco PGW 2200 Softswitch.	Verify that the hostController process is running. For example, enter: **ps -ef	grep hostController** If the hostController is running, rediscover the device. If not, contact the TAC.
Miscellaneous error messages upon deployment, such as demons not running...	—	(1) Verify that the correct software release and patch are installed on the device. See Chapter 1 of the installation guide for details and links to up-to-date information. (2) Make sure that the device is running. For example, for Cisco PGW 2200 Softswitch enter **/etc/init.d/CiscoMGC start** If the device is already running, a message displays. Otherwise it should start.
No IP addresses defined on this device. All traps from it will be ignored.	Cisco MNM 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.

Table C-1   Cisco MNM Internal Events (continued)

Message	Explanation	Action
Subrack discovery failed. Check logs	Cisco MNM 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 Cisco PGW 2200 Softswitch or Cisco 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_ROOT>*/logs/mgcController.log. Verify that the correct software release and patch are installed on the device. See Chapter 1 of the installation guide for details and links to up-to-date information.
The IP Address <IP Address> is not reachable.	Cisco MNM failed to do SNMP ping with this address.	Check the network connection.
This device is not reachable.	Cisco MNM 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.

Table C-2   Seed File Deployment Errors

Message	Explanation	Action
Unknown device specified	—	—
Unbalanced braces	—	—
Duplicate object names	—	—
Missing required attribute: *Attribute*	A required attribute is missing.	—
Component is not valid: *COMPONENT*	Device information supplied is syntactically incorrect.	Check and fix device syntax in seed file.
Expected attribute value. Found	A required value is missing	—

Solving Deployment and Discovery Errors

If you receive errors when deploying a seed file, check the information in Table C-2 and correct the problem in the file. See Chapter 5, "Deploying Your Network in Cisco MNM," "Deploying a Network Using a Seed File" section on page 5-9 for details.

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

Changing Password or Community Strings

Use the following procedure to change the password or community strings for a device:

Step 1   In the Map Viewer window, select the object and right-click.

Step 2   From the pull-down menu, choose **Accounts**.

The Accounts dialog box opens.

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 **Save** on the toolbar, and close the dialog box.

Step 6   If you changed the community strings on any device or the password for the
Cisco PGW 2200 Softswitch host, rediscover the device as described in the "Rediscovering a Device
After a Problem" section on page C-6.

Changing IP Address

If the wrong IP address was entered, the device must be redeployed. Use the following steps to redeploy
a device:

Step 1   In the Map Viewer window, select the object and right-click.

Step 2   From the pull-down menu, choose **Deployment > Delete Objects**.

The Deployment Wizard dialog box opens with the message, "Ready to delete 1 object."

Step 3   Click **Finish**. A message displays that the object has been deleted.

Step 4   Click **OK**.

Step 5   Redeploy the device by following the instructions in Chapter 5, "Deploying Your Network in
Cisco MNM," "Manual Deployment" section on page 5-10.

Step 6   After deployment, rediscover the device as described in the "Rediscovering a Device After a Problem"
section on page C-6.

Rediscovering a Device After a Problem

Follow these steps to rediscover a device after correcting a problem that interfered with discovery. This
synchronizes the Cisco MNM network object model with the real-world network.

Step 1   In the Map Viewer window, select the object and right-click.

Step 2   Choose **States**.

The States dialog box opens.

Step 3   On the States tab, choose **Rediscover**.

You are asked if you want to rediscover the device.

Step 4   Click **Yes**. Cisco MNM 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.

Troubleshooting SSH-Related Errors

If you suspect an SSH security-policy error, such as a mismatch between the security policy defined for a component at deployment and its actual security policy, you can do one of two things:

*   Check SSH-related alarms in the Event Browser. You can see SSH-related alarms, such as a mismatched security policy or an incorrect password, for the BAMS, Cisco PGW, and HSI server, in the Event Browser. These are Warning alarms. For a description of Cisco PGW 2200, the BAMS, and HSI alarms caused by login failures related to SSH problems, see the "Cisco PGW 2200 Security Enhancements" chapter in the *Cisco Media Gateway Controller Software Installation and Configuration Guide* (Release 9.7) at

    http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/installation/software/SW1/97.html

*   For an IOS device, check the ssh protocol version or configuration with this command:

    show ip ssh

    ```
    SSH Enabled - version 1.5
    Authentication timeout: 120 secs; Authentication retries: 3
    ```

    To see ssh users that are logged on, use this command

    show ssh

    ```
    Connection   Version Encryption      State     Username
    1              1.5    DES              Session started       lab
    ```

Troubleshooting Other Issues

Table C-3 lists common problems you may encounter along with suggested corrective actions. Other troubleshooting information is provided in the Installation Guide, Chapter 2, Troubleshooting Common Installation Problems.

Table C-3   Troubleshooting Symptoms and Suggested Steps

Problem	Action
Alarms are not being received from a device.	Check that SNMP trap forwarding has been configured. To configure SNMP trap forwarding, see Chapter 2, "Configuring Network Devices for Management."
	If trap forwarding has been configured, check the snmpd.cnf file (Cisco PGW 2200 Softswitch host or the BAMS) against the instructions in Chapter 2 for possible typing errors.
Cisco MNM cannot automatically clear some alarms of the Cisco BAMS.	Manually clear these alarms in Cisco MNM. To manully clear alarms, see Chapter 6, "Managing Faults with Cisco MNM."
Cisco MNM intermittently fails to discover BAMS Node 1 association between the BAMS and PGW.	Check if the Cisco BAMS has been configured to collect CDRs for the relevant Cisco PGW 2200 Softswitch host.
	Check if the Cisco BAMS actively polls CDRs from that Cisco PGW 2200 Softswitch host
	Check if *<IP Address> <hostname>* for Cisco PGW 2200 Softswitch is added to the /etc/inet/hosts file.
	Rediscover the Cisco BAMS if needed.
	See Chapter 5, "Deploying Your Network in Cisco MNM," "Discovery of Cisco PGW 2200 Softswitch Host, Cisco HSI Server, and Cisco BAMS Components" section on page 5-15 for details.

INDEX

E

F

G

N

WebViewer, launching **8-4**

X

X-terminal window, opening **8-4**

X window, launching **8-66**