CHAPTER 1

Overview of Cisco Media Gateway Controller Node Manager

Introduction

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

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

Terms Used in This Document

The following terms are used in this document:

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

- CiscoView—A graphical device management tool based on Simple Network Management Protocol (SNMP) that provides real-time views of networked Cisco Systems devices.
- CMM and VSPT—Cisco MGC Manager and Voice Services Provisioning Tool

  You can use two different Cisco VSC3000 and Cisco SC2200 provisioning tools, depending on the network architecture you are running. If you are running the Cisco SS7 PRI Gateway Solution or the Cisco Tandem Offload Solution, you use VSPT. For all other architectures, you use CMM.
- Web Viewer—A web-based device management tool that facilitates managing the Cisco MGX 8260 media gateway.

Overview of the Cisco MGC Node Architecture

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

The Cisco MGC node itself comprises the:

- Cisco MGC host—The Cisco MGC host is a suite of software running on a Sun Solaris server and is responsible for most of the Cisco MGC functionality, including (depending on the configuration) number analysis, routing, switching, and so on.
- Cisco Signaling Link Terminal (Cisco SLT)—The Cisco SLT is responsible for terminating SS7 signaling lines from the PSTN.
- LAN switch—The LAN switch acts as an Ethernet switch connecting the Cisco SLT and the Cisco MGC host to external equipment.

  The standard Cisco MGC node design defines that a Cisco 2611 should be configured as the Cisco SLT and that a Catalyst 2900XL, 5500, or 5000 should be used as the LAN switch.
- BAMS—BAMS is used for optional third-party accounting and billing packages.

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

Key Features of CMNM

The most common form of a CEMF installation includes plug-in modules referred to as Element Managers or Element Management Systems (EMS). In the Cisco MGC node architecture, CMNM is a CEMF-based EMS that is responsible for managing the Cisco MGC node. CMNM adds custom graphical user interface (GUI) windows and modeling behavior to the standard CEMF system to allow the management of specific types of network elements. For more information about the Element Managers installed with CMNM, see Table 2-12 in the "Verifying Element Managers" section on page 2-11.

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

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

The key features of CMNM are:

- Performance monitoring

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

  You can:

  – Graph and display the performance information

  – View performance data associated with a given object and graph that data over time

  – Configure the objects being polled and the frequency of the polling

  – Export the performance data for use by other applications

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

- Fault management

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

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

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

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

- Security

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

- Billing and Measurements

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

- Configuration

  You can launch the following configuration tools from CMNM:

  – Cisco MGC Manager (CMM), a generic Cisco MGC host configuration tool used in all network architectures except those using the Voice Services Provisioning Tool.

  – CiscoView, which allows you to configure the Cisco SLT (Cisco 2611) and the LAN switch (Catalyst 2900, 5000, and 5500) devices.

  – Voice Services Provisioning Tool, a Cisco MGC host configuration tool used in the Cisco SS7 PRI Gateway Solution and the Cisco Tandem Offload Solution. For all other architectures, use CMM.

  - Web Viewer, the tool used to view and configure the Cisco MGX 8260.
- Troubleshooting

  CMNM provides CDR Viewer, Log Viewer, Trace Viewer, and Translation Verification Viewer for diagnostic and troubleshooting information.

Overview of CEMF

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

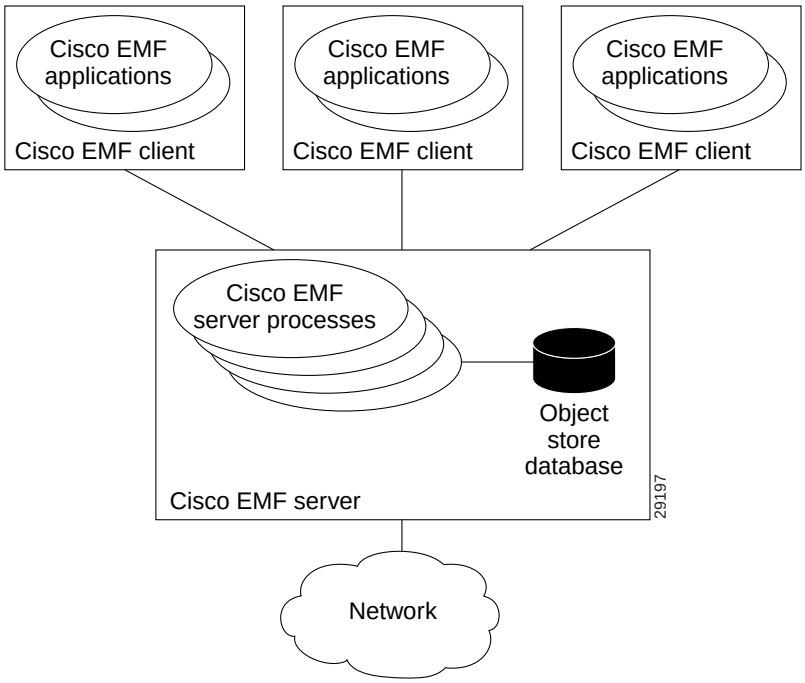
CEMF has been designed to overcome the limitations of traditional enterprise network management solutions, particularly in the broadband access market, and also in other network management applications where the aforementioned characteristics are important. CEMF is used to quickly develop and deploy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

CEMF Components

CEMF consists of:

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

Figure 1-1 CEMF Processes



CEMF comes with the following set of applications:

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

How CEMF Models the Network

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

The CEMF model of the network uses the following components:

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

  An object can represent:

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

  - An abstraction of the network, such as a site or a region
  - Some of the services provided by the network, such as a permanent virtual connection (PVC)
  - Something (or someone) that interacts with the network, such as a subscriber or a customer

- Object classes—Each object within CEMF has an associated object class. Each class of object simply indicates a different kind of element. Examples of classes are routers, line cards, sites, and so on. Each class of object has different data stored against it and displays different behavior.

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

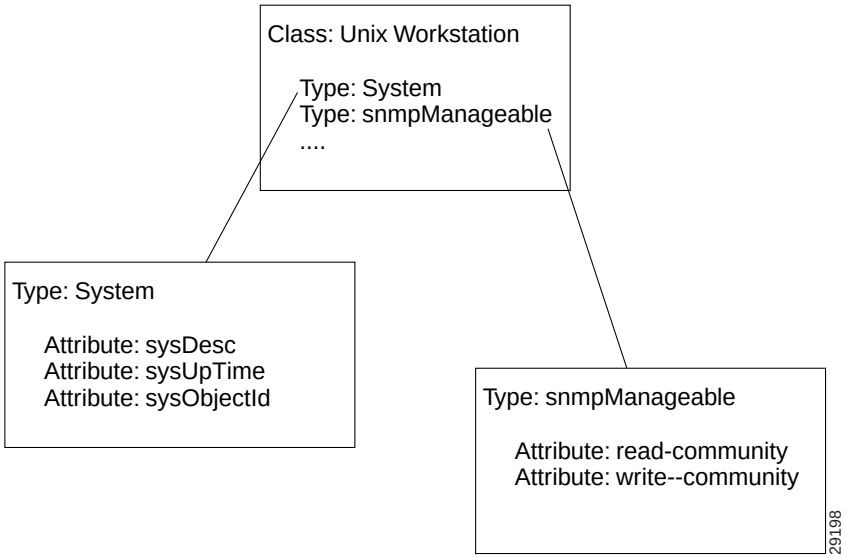
  The use of classes also allows powerful queries to be carried out based upon the kind of object. Examples of this type of query could be: show all events in the system from cable modems or create a group of router objects.

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

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

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

Figure 1-2 Example of Object Types and Attributes



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

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

You can access CEMF objects by navigating through one of the views to find the object. Each view represents a different way of containing and grouping the objects. The standard views provided are the Physical view and the Network view. CMNM adds additional views onto the standard set supplied by CEMF. CMNM views are summarized in Table 1-1.

Table 1-1 CMNM Views

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

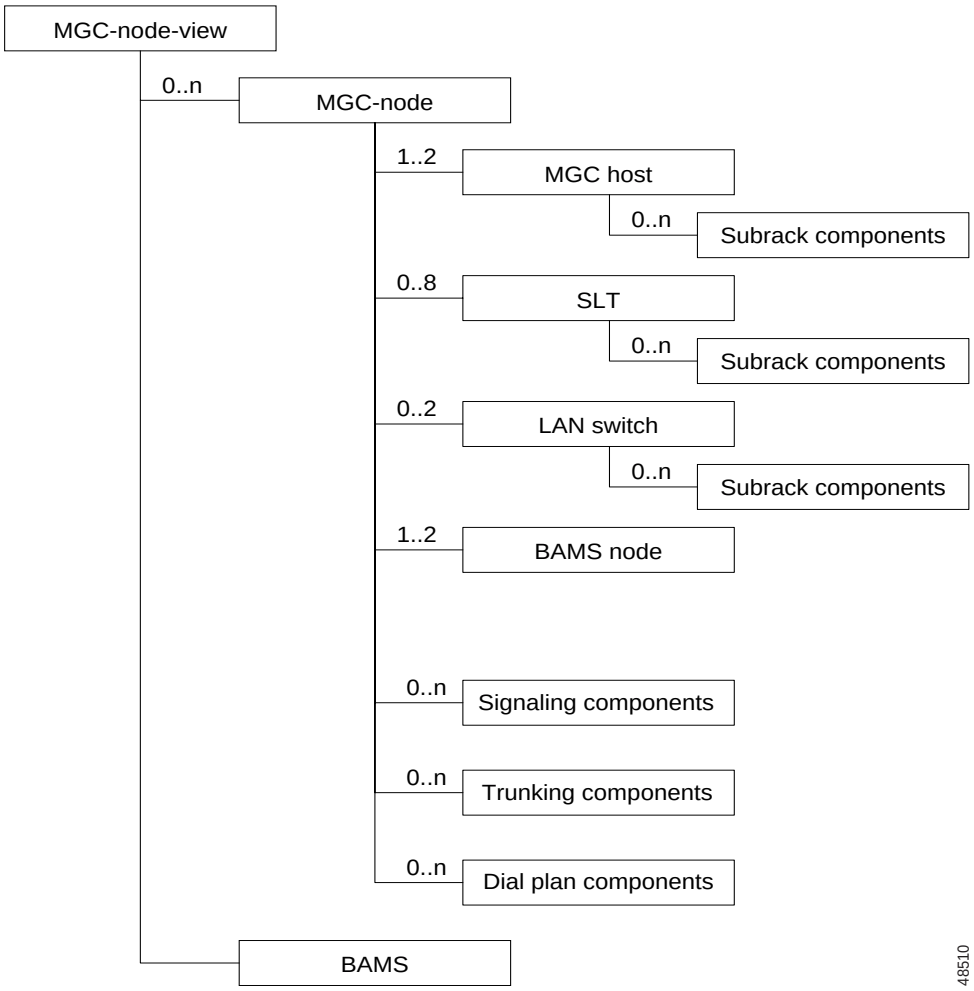
- Object groups—An object group is simply a collection of objects that are related in some way. They may all be the same type of equipment or all belong to the same customer.

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

MGC Node View

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

Figure 1-3 MGC Node View



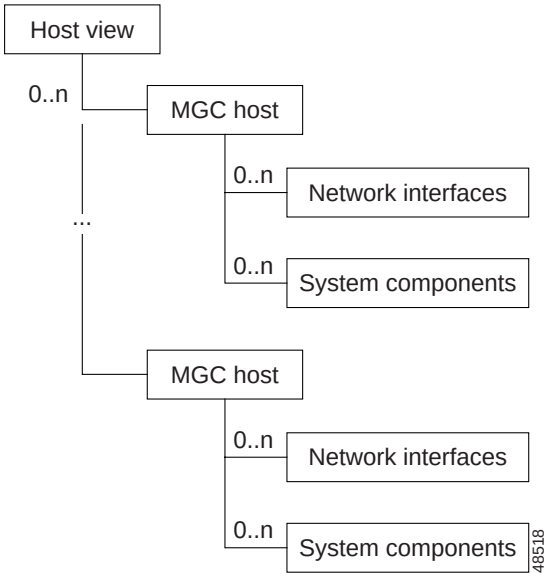
Each Cisco MGC node is represented with its logical child elements. These child elements include the Cisco MGC hosts, BAMS, Cisco SLTs, and LAN switches, and each device's network interfaces. Depending on the configuration, there can be up to two Cisco MGC host devices (active/standby pair), two BAMS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

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

Host View

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

Figure 1-4 Host View

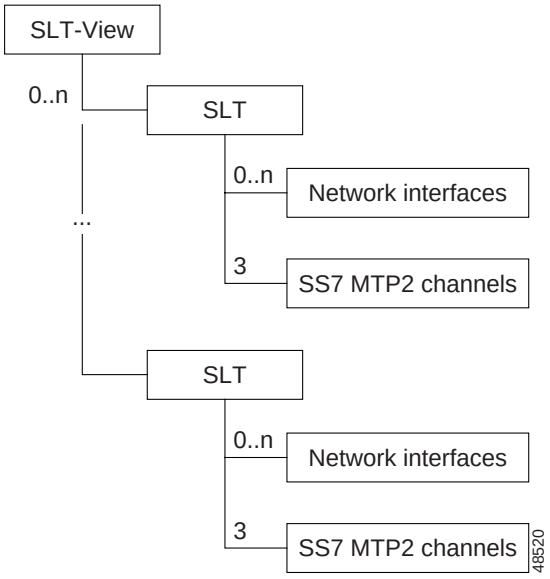


Each Cisco MGC host in the network is displayed along with its network interfaces and system components. This view is used to collect all Cisco MGC hosts in a single location where services can be launched.

SLT View

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

Figure 1-5 SLT View

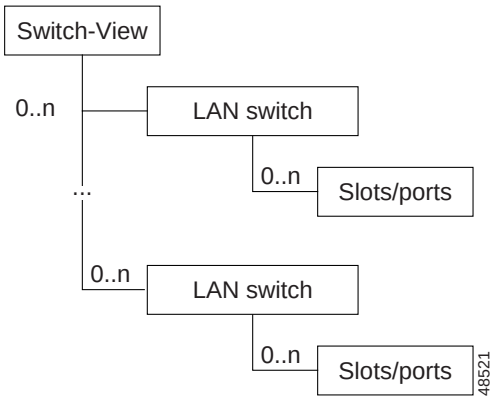


This view is used to collect all Cisco SLTs in a single location. From this view the user can monitor faults or launch Cisco SLT-specific services.

Switch View

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

Figure 1-6 LAN Switch View

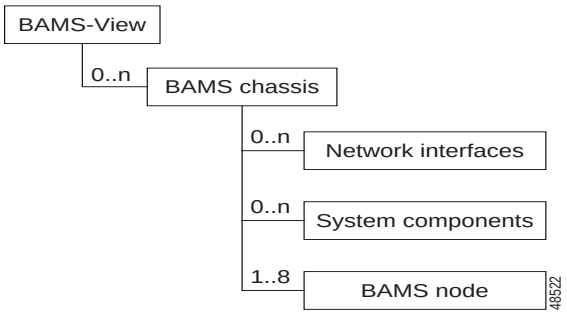


This view is used to collect all LAN switches in a single location for viewing faults or launching services.

BAMS View

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

Figure 1-7 BAMS View



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

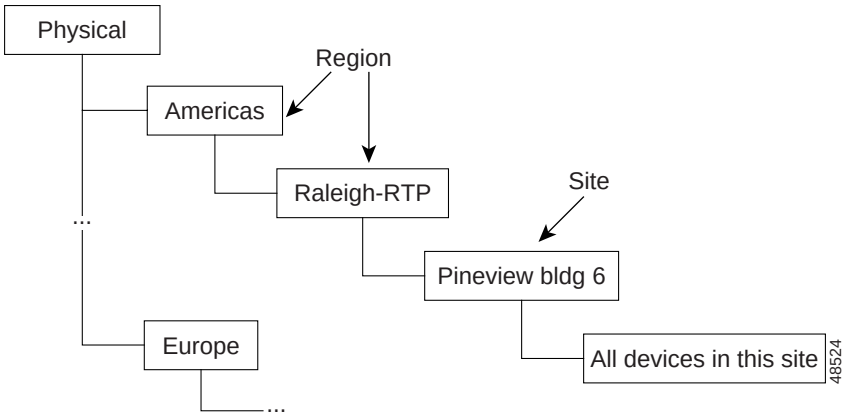
Physical View

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

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

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

Figure 1-8 Physical View



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

Network View

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

How CMNM Models the Cisco MGC Node

This section provides information about how CMNM models:

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

Cisco MGC Host Signaling Network

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

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

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

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

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

CMNM communicates to the Cisco MGC host using:

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

Cisco MGC Host Signaling Objects

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

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

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

The classes used to represent the signaling network in CMNM are described in Table 1-2.

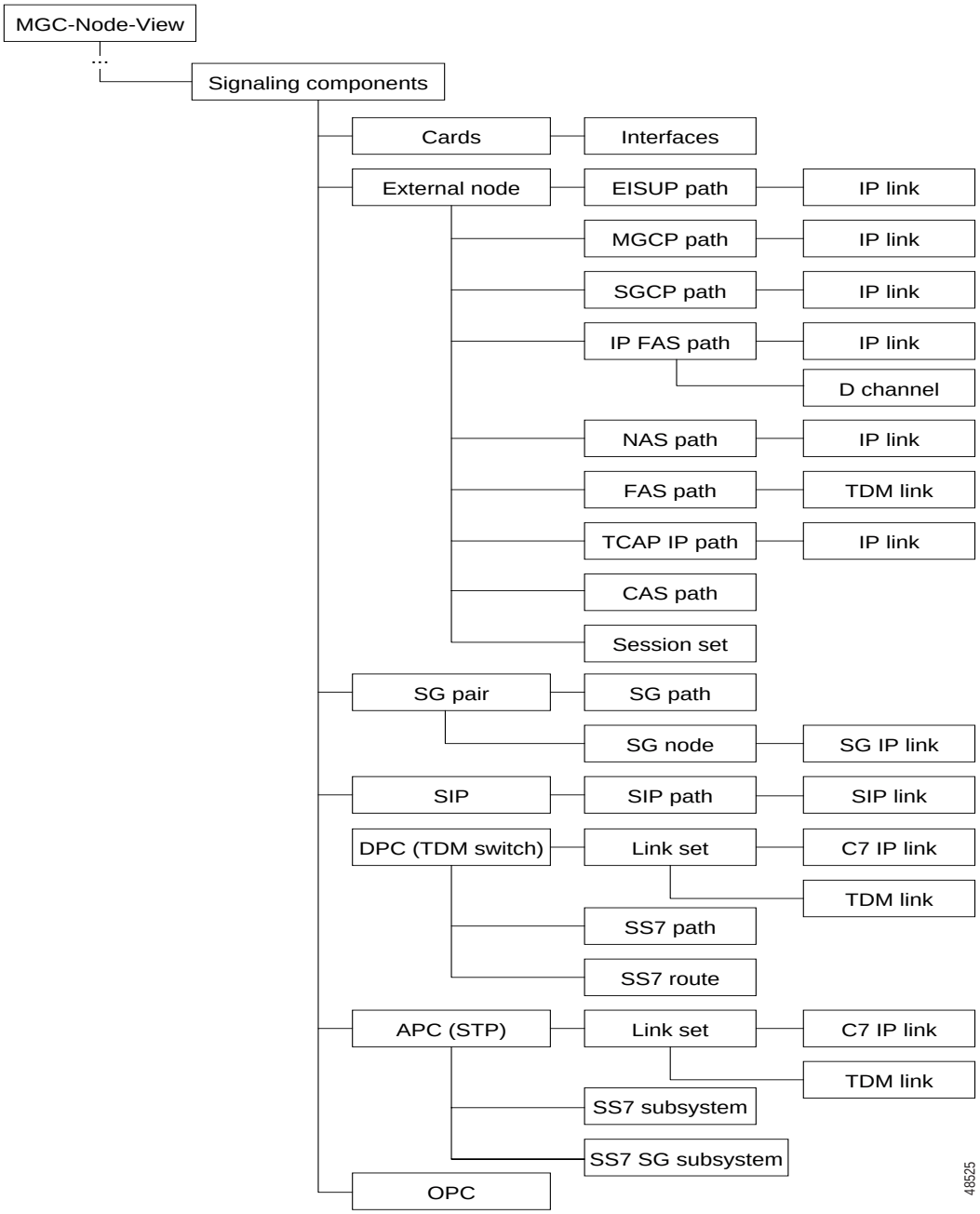
Table 1-2 Classes Representing Signaling Network

MML Type	Name	Description
apc	Adjacent point code	Defines an SS7 STP or external switch through which the Cisco MGC connects to external switches and other Service Switching Points (SSPs).
c7iplnk	C7 IP link	Identifies a link between a Cisco SLT IP address and port and the SS7 network.
card	Card	Network card or adapter that is operating in the Cisco MGC.
eisuppath	EISUP path	Signaling service or signaling path to an externally located Cisco MGC.
enetif	Ethernet interface	Physical line interface between a Cisco MGC Ethernet network card/adapter and the physical Ethernet network.
extnode	External node	Cisco MGW with which the Cisco MGC communicates.
faspath	FAS path	Service or signaling path to a particular destination using either ISDN-PRI or DPNSS.
ipfaspath	IP FAS path	Transport service or signaling path from a gateway to a Cisco MGC.
iplnk	IP link	IP connection between a Cisco MGC Ethernet interface and a Cisco MGW.
lnkset	Linkset	Group of all communication links that connect from the Cisco MGC to an adjacent STP.
mgcppath	MGCP path	Signaling service or signaling path to a trunking gateway.
naspath	NAS path	Q.931 protocol path between the Cisco MGC and the Cisco MGW.
ptcode	Point code	An SS7 network address that identifies an SS7 network node.
sgcpath	SGCP path	Protocol path between the Cisco MGC and the Cisco MGW.
ss7path	SS7 path	Specifies the protocol variant and the path that the Cisco MGC uses to communicate with a remote switch (SSP) sending bearer traffic to the Cisco MGWs.
ss7route	SS7 route	Path, by way of a linkset, from the Cisco MGC to another Cisco MGC or TDM switch.
ss7subsys	SS7 subsystem	Logical entity that mates two Signal Transfer Points (STPs).
tcapippath	TCAP IP path	Signaling service path to an STP or SCP.
tdmif	TDM interface	Physical line interface between a Cisco MGC TDM network card/adapter and the physical TDM network.
tdmlnk	TDM link	Communications link between a TDM interface card on the Cisco MGC and TDM hardware element.

Containment Hierarchy of the Signaling Network

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

Figure 1-9 Hierarchical Model Example



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

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

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

Cisco MGC Host Trunking Objects

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

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

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

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

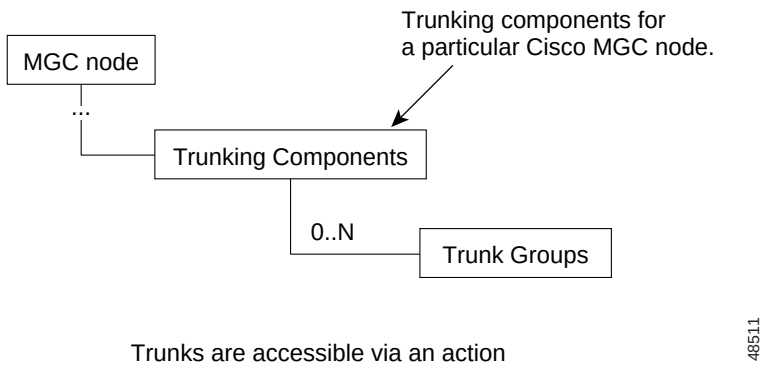
Table 1-3 Classes Representing Trunking Objects

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

Containment Hierarchy of the Trunking Objects

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

Figure 1-10 Hierarchical Model Example of Trunking Objects



Cisco MGC Host Dial Plan Objects

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

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

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

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

Table 1-4 Classes Representing Dial Plan Objects

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

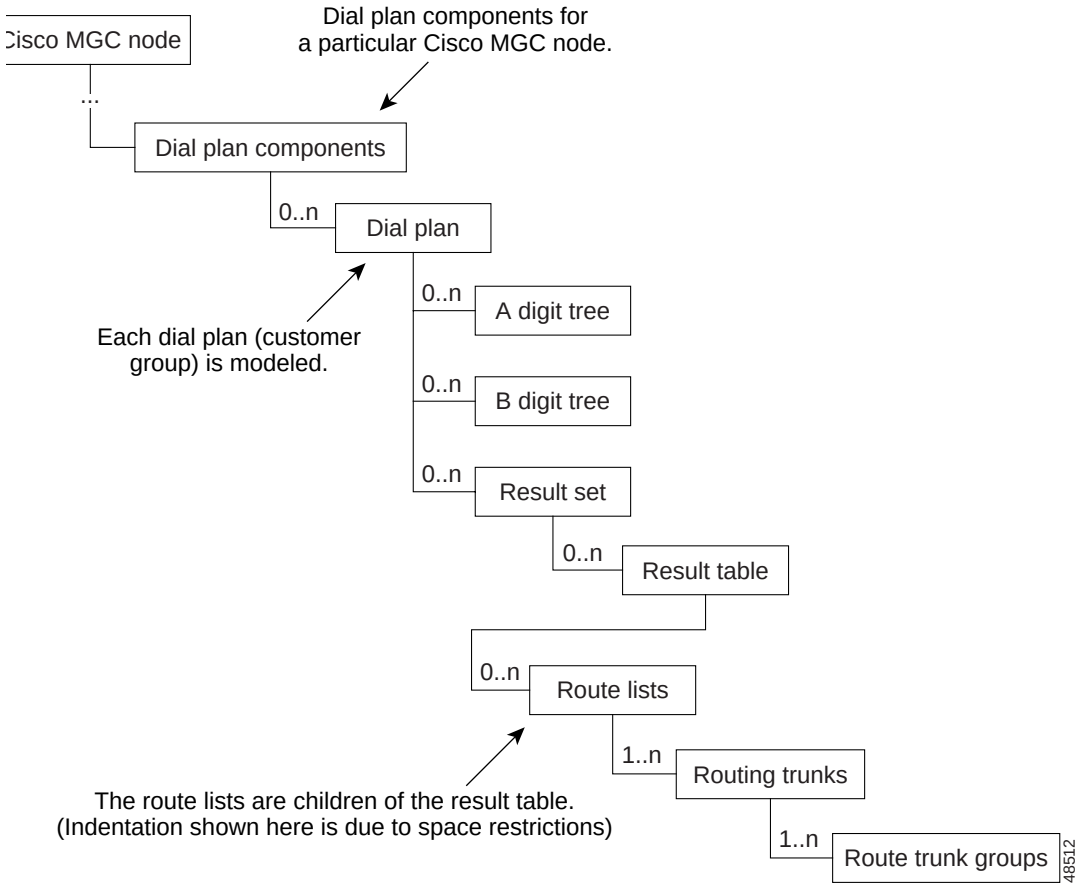
Table 1-4 Classes Representing Dial Plan Objects

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

Containment Hierarchy of the Dial Plan Objects

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

Figure 1-11 Hierarchical Model Example of Dial Plan Objects



Overview of Event Manager

There are three component parts to the Event Manager :

- Thresholding Regimes
- Notification Profiles
- Event Groups

The following sections provide an overview of these components.

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

Thresholding Regimes

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

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

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

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

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

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

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

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

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

Notification Profiles

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

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

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

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

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

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

Event Groups

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

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

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

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

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

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

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

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