Basic Concepts

This chapter covers the details the basic concepts of Cisco MGM, including the following topics:

- 2.1 How Do I Navigate within Cisco MGM?
- 2.2 What Basic Functions Can I Perform in Cisco MGM?
- 2.3 What Are the General Features of Cisco MGM?

2.1 How Do I Navigate within Cisco MGM?

This section helps you understand Cisco MGM navigation tools and actions, including:

- 2.1.1 Using the Domain Explorer
- 2.1.2 Navigating Physical Views
- 2.1.3 Using Network Maps
- 2.1.4 Using Control Panel
- 2.1.5 Using Wizards
- 2.1.6 Paging through Data
- 2.1.7 Finding Data
- 2.1.8 Navigating the Client Desktop
- 2.1.9 Using Mnemonics
- 2.1.10 Using the Online Help
- 2.1.11 Using the Pin Tool

Note When you switch to a different program and then return to Cisco MGM, the Cisco MGM dialog boxes might be hidden behind another Cisco MGM window or dialog box. The Cisco MGM client might appear frozen because the hidden dialog box requires user action. On a Windows workstation, press **Alt-Tab** to display all running processes. Continue to press **Tab** (while keeping **Alt** depressed) to select the icon for the Java process. This will position the Cisco MGM dialog box as the top active window. On a Solaris workstation, minimize the open windows until the Cisco MGM dialog box is visible.

2.1.1 Using the Domain Explorer

The Domain Explorer is the Cisco MGM home window and provides a logical view of the network plus alarm, connectivity, and operational status.

The Domain Explorer displays a hierarchical view of all NEs and groups currently being monitored by Cisco MGM. Domain Explorer windows are divided into two sections: a tree (at left) and a pane (at right). The tree organizes the resources (domain, groups, and NEs), which are displayed in a hierarchical format. The top level of the hierarchy is the management domain, followed by groups and NEs. You can access information about each resource by browsing the tree section. The pane provides specific information about the selected object.

Tip The Domain Explorer only provides a high-level view of the network. To view the entire managed network, access the Physical View hierarchy tree from the Configuration Center, Chassis View, Statistics Report, or Diagnostic Center.

To check the connection status of a selected NE, run a diagnostic check at the node level in the Diagnostic Center. See 5.2.10.2 Running a Diagnostic Check at the Node Level.

Note You can drag and drop NEs to reposition them in the topology tree.

The Domain Explorer has three properties panes:

- 2.1.1.1 Management Domain Properties, page 2-2
- 2.1.1.2 Group Properties, page 2-4
- 2.1.1.3 Network Element Properties, page 2-5

Tip See Appendix A, “Icons and Menus” for an explanation of the Domain Explorer legend and icons.

2.1.1.1 Management Domain Properties

The Management Domain Properties pane displays information about the management domain that is currently selected in the Domain Explorer tree. The Cisco MGM management domain consists of all the NEs managed by the Cisco MGM server where the Cisco MGM client connects.

The management domain can also contain groups that give you the flexibility to subdivide the domain you are monitoring. For example, a group can represent all NEs within a geographical location.

To display all of the first-level nodes under the management domain, click the expand icon (+) next to the management domain name in the topology tree. If any of the groups or NEs have an alarm condition, an icon representing that condition is displayed next to the management domain name.

The Management Domain Properties pane has two tabs: Status and Identification.

2.1.1.1.1 Status Tab

Table 2-1 describes the Status tab fields.

Table 2-1 Field Descriptions for the Status Tab

Field	Description
Domain Name	User-defined name of the management domain.
Description	User-defined description of the management domain.
Total NEs	Total number of NEs within the management domain.
Unavailable NEs	Number of NEs within the management domain that Cisco MGM cannot currently connect to.
NEs in Alarm	Total number of NEs within the management domain that have an active alarm.
Unmanaged NEs	Total number of unmanaged NEs within the management domain.
Alarm Status	Total number of NE and EMS alarms by severity. In addition, this field lists how many of the total NEs with active alarms are experiencing a critical, major, minor, or warning alarm. **Note** If the same NE is experiencing more than one type of alarm simultaneously, that NE is counted for each severity level.
NE Count by Operational State	Total number of NEs within the management domain according to operational state: • In Service: The NE is currently deployed and requires monitoring. • Out of Service: The NE has been marked out of service and does not require monitoring. • NEs In Initialization: The NE is initializing, and you can perform the following actions: – Open the Alarm Browser and Alarm Log. – Open the PM tables. • Under Maintenance: The NE is temporarily under maintenance but requires monitoring. • NEs in Sync Configuration: The NE is in Sync Configuration state, and you can perform the following actions: – Open the Alarm Browser and Alarm Log. – Open the PM tables.

2.1.1.1.2 Identification Tab

Table 2-2 describes the Identification tab fields.

Table 2-2 Field Descriptions for the Identification Tab

Field	Description
Domain Name	Name of the management domain.
Description	Description of the management domain.
EMS ID	EMS ID (Cisco Media Gateway Manager).
Server	Name or IP address of the Cisco MGM server to which the user is connected.
Vendor Name	Vendor name (Cisco Systems).
Software Version	Cisco MGM release that is running.

2.1.1.2 Group Properties

The Group Properties pane displays information about the group that is currently selected in the topology tree.

A group consists of other groups or NEs. Groups give you the flexibility of subdividing the management domain you are monitoring. For example, a group can represent all NEs within a geographical location.

Click the expand icon (+) next to a group in the topology tree to view the objects that are assigned to that group. The same group can have multiple instances in the topology tree. The contents of all instances of a group are always the same. Any changes to one instance of a group will be reflected in all instances of that group.

You can add and delete groups; however, the option to delete a group is not available until all objects are removed from the group. If the group has multiple instances in the topology tree, you can delete all but the last instance of the group.

The Group Properties pane has two tabs: Status and Identification.

2.1.1.2.1 Status Tab

Table 2-3 describes the Status tab fields.

Table 2-3 Field Descriptions for the Status Tab

Field	Description
Group ID	User-defined name of the selected group.
Description	User-defined description of the selected group.
Total NEs	Total number of NEs within the selected group.
Unavailable NEs	Number of NEs within the selected group that the Cisco MGM server cannot currently reach.
NEs in Alarm	Total number of NEs within the selected group that currently have an active alarm.
Unmanaged NEs	Number of NEs within the selected group that are currently unmanaged.
Alarm Status	Total number of alarms within the selected group, by severity. In addition, this field lists how many of the total NE alarms have a critical, major, minor, or warning status. If the same NE experiences more than one type of alarm simultaneously, that NE is included in the count for each severity level.
NE Count by Operational State	Total number of NEs within the selected group according to operational state. Values are In Service, Under Maintenance, and Out of Service. Also shows the number of NEs within the selected group that are initializing or synchronizing their configuration.

2.1.1.2.2 Identification Tab

Table 2-4 describes the Identification tab fields. Only users with the appropriate user access profile can edit these fields.

Table 2-4 Field Descriptions for the Identification Tab

Field	Description
Group ID	Unique user-defined name of the selected group.
Description	User-defined description of the selected group.
Location Name	User-defined geographic location of the selected group.

2.1.1.3 Network Element Properties

The Network Element Properties pane displays information about the NE that is currently selected in the tree. An NE represents a Cisco MGX 8880 or a Cisco MGX 8850.

The same NE can have multiple instances in the tree. The contents of all instances of the same NE are always the same. Any changes to one NE instance are reflected in all instances of that NE. Regardless of the number of instances an NE has in the tree, you can delete one or all instances of that NE. When the final instance of an NE is deleted, the deleted NE moves to the Deleted NEs group.

The Network Element Properties panes for most NEs have the following tabs: Status, Identification, and NE Authentication.

2.1.1.3.1 Status Tab

Table 2-5 describes the Status tab fields.

Table 2-5 Field Descriptions for the Status Tab

Field	Description
NE ID	Name of the selected NE.
Description	Information that a user entered to describe the NE.
NE Model	Model of the selected NE.
Alarm Status	Total number of critical, major, minor, and warning alarms currently existing on the selected NE.
Communication State	Current communication state of the selected NE (Available or Unavailable).
Operational State	Current operational state of the selected NE. You can change the operational state.
PM Collection	You can enable or disable PM data collection.

2.1.1.3.2 Identification Tab

Table 2-6 describes the fields in the Identification tab.

Table 2-6 Field Descriptions for the Identification Tab

Field	Description
NE ID	Name of the selected NE.
Description	Information that a user entered to describe the NE. You can edit this field.
NE Model	Model of the selected NE.
NE Type	Type of NE. You can edit this field.
Vendor Name	Vendor name.
Software Version	Software version that is running on the NE.
Active IP Address	Active IP address of the selected NE.

2.1.1.3.3 NE Authentication Tab

The NE Authentication tab allows you to specify usernames and passwords for Cisco MGM server. Table 2-7 describes the fields in the NE Authentication tab. Fields shown depend on the type of NE selected.

Table 2-7 Field Descriptions for the NE Authentication Tab

Field	Subfield	Description
MGM Server - NE Connection	NE Service Level Username	Username that the Cisco MGM server uses to connect to NEs.
	NE Service Level Password	Password to use for Cisco MGM server-to-NE connections.
	Confirm NE Service Level Password	Re-enter the password to confirm it.
	SNMP Community String	Community string name used in SNMP messages. You must provide the community string name to give the user SNMP read access to the device. This field is unavailable if it does not apply to the selected NE.
	SNMP Set Only Community String	Community string used in SNMP messages for setting the attributes on the device.

2.1.2 Navigating Physical Views

The Physical View is a hierarchical tree that can be found in certain Cisco MGM applications; namely, the Chassis View, Statistics Report, Configuration Center, and Diagnostic Center (for details about these applications, see section 2.3 What Are the General Features of Cisco MGM?, page 2-14.)

The Physical View shows the entire managed network. To expand or minimize the hierarchy, click the looking glass icon next to any node. Nodes are color-coded to represent the highest severity alarm on each node.

2.1.3 Using Network Maps

The Network Map window allows you to display how the network is partitioned graphically. It is organized into a multilevel hierarchy that corresponds to the structure of the Domain Explorer trees. The Network Map hierarchy consists of management domains, groups, and NEs, which are displayed graphically.

You can launch the Network Map either by clicking on the **Open Network Map** tool in the Domain Explorer toolbar, or by choosing **File > Network Map**. A map appears with individual groups and NE icons.

Double-clicking a group expands that group to show its contents. Clicking **Show Parent Network Map** returns you to the parent map. When you launch the Network Map from a particular group in the Domain Explorer, the Network Map opens with the contents of the group displayed.

After zooming in on a region on the map, scroll bars at the bottom and right side of the screen allow you to pan the view to a different region. You can also use the focus box in the top left panel to pan and zoom the view. All groups are shown on a single map, and it is the zoom level and pan position that determine what groups are visible at any time. Depending on the selected layer rate, certain NEs are shown. You can open multiple map windows to compare different views.

Note Sometimes one node can overlap another in the maps. This occurs when a new node is added and other existing nodes have already been assigned a location. The solution is to change the layout to make sure that no two nodes are overlapping.

All groups, NEs, and labels are zoomed when you zoom in or zoom out. Cisco MGM allows you to save the zoom level and framing of the map. Also, you can specify a fixed pixel size for icons so that regardless of the zoom level, the map icon size does not change. By default, the icon size is variable based on the zoom level. The icon size setting is saved with the other map settings.

When you open the Network Map from an NE in the Domain Explorer, the selected NE is centered on the map.

Note The Refresh Data tool in the Network Map toolbar flashes when updates are available.

The following scenarios describe the actions of the Refresh Data tool in the Network Map toolbar.

- The Refresh Data tool flashes when:
  - The map background is changed
  - The topology structure changes (a node is added or deleted) in a group or area
  - A node is forced invalid
- The Refresh Data tool does not flash when:
  - The alarm counts change on the node
  - The node connectivity state changes
  - The node admin state changes
  - The node name changes
  - The node data properties change
  - The discovery state changes
  - The data reference changes

2.1.4 Using Control Panel

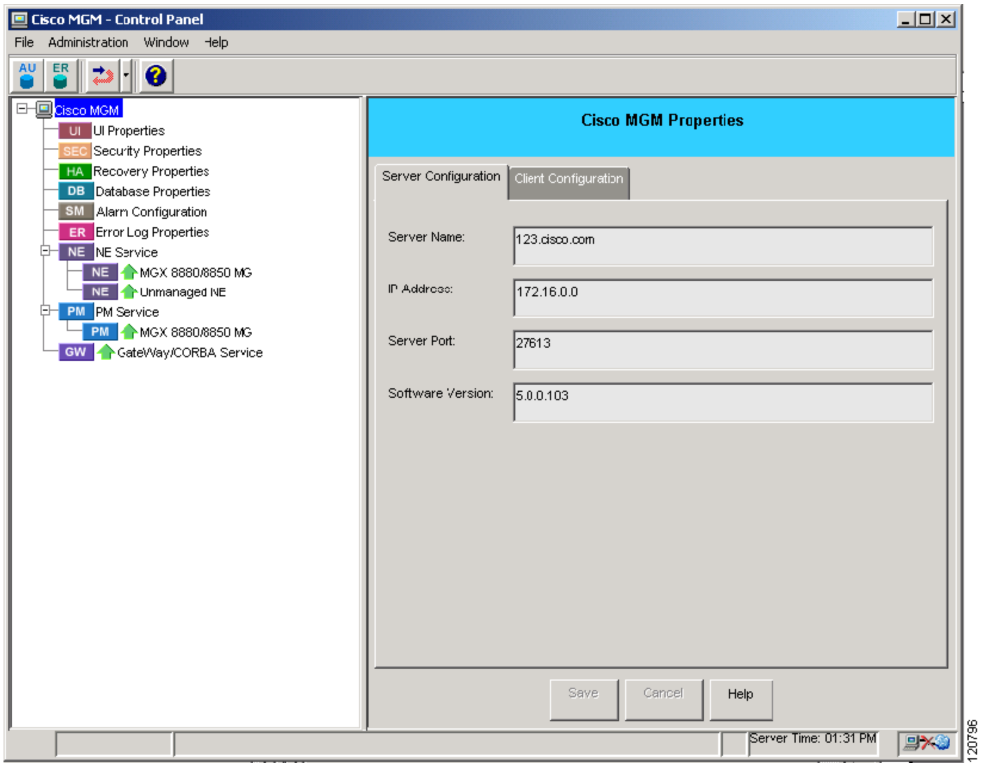
Most client and server configuration parameters are viewed and modified in the Control Panel window. To view the Control Panel, choose **Administration > Control Panel** in the Domain Explorer. The left side of the window displays the tree, which contains the following Cisco MGM functions and services:

- UI Properties—for Fault Management and Domain Management
- Security Properties—for Password Aging, Maximum Retries, Login Disable Period and Client Inactivity Timer Settings
- Recovery Properties—for Session Recovery and Process Monitoring using High Availability

- Database Properties—for Configuration, Pruning and Database Backup
- Alarm Properties—for Threshold EMS Alarms and Non Threshold EMS Alarms
- Error Log Properties—for the Cisco MGM Server and Gateway/SNMP, SM Service and SNMP Trap Service
- NE Service—for NE Poller, NE AutoBackup and NE Manual Backup
- PM Service—for PM Status and Properties
- Gateway CORBA Service—for Global and OSS Clients

The right side of the window displays the property sheet that corresponds to the selected client or server component. See Figure 2-1.

Figure 2-1 Control Panel



Server Name: 123.cisco.com

IP Address: 172.16.0.0

Server Port: 27613

Software Version: 5.0.0.103

Server Time: 01:31 PM

2.1.5 Using Wizards

Wizards are used to guide users through complex operations. Each wizard presents a sequence of dialog boxes which the user can move forward and backward through, filling in the details required by choosing radio buttons, checking boxes and entering information by keyboard.

In Cisco MGM, wizards are used to simplify involved configuration management tasks such as:

- NE user access administration
- Broadcast software download
- Native equipment/facility provisioning

- Topology management
- Automatic NE memory backup, on-demand restoration
- General operation on multiple NEs

2.1.6 Paging through Data

Some Cisco MGM tables return large numbers of rows. To support large tables, Cisco MGM provides a paging feature. If more than 1,000 rows of data are returned, data is grouped in pages of up to 1,000 rows. You can page forward and page back to view the entire set of data.

2.1.7 Finding Data

There are two methods of finding data in Cisco MGM:

- 2.1.7.1 Finding Data in the Domain Explorer, page 2-9
- 2.1.7.2 Finding Data in the Diagnostic Center, Statistics Report, Chassis View, and Configuration Center, page 2-9

2.1.7.1 Finding Data in the Domain Explorer

In the Domain Explorer window, use the **Edit > Find** dialog box to search for NEs or groups. To search for a particular NE or group, specify the NE or group name, IP address, or description. The search always starts from the root node and returns to the root node after reaching the last node.

2.1.7.2 Finding Data in the Diagnostic Center, Statistics Report, Chassis View, and Configuration Center

In the Diagnostics Center, Statistics Report, Chassis View, and Configuration Center, enter the object name or the IP address in the text box at the left side of the window above the Hierarchy tree. The object name or IP address can be entered in full or partially. Click the **Find** button. If found, the Hierarchy Tree displays the node or the trunk. If there are multiple matches, click the **Find Next** or **Find Previous** button to show the next node or trunk.

2.1.8 Navigating the Client Desktop

The client desktop provides a menu bar and a toolbar that correspond to the principal Cisco MGM applications. You click on a particular icon to launch the corresponding application you need for element management, monitoring, report generation, and administrative tasks. You can launch all applications from the menu bar or you can right-click a specific object and choose the popup menu option.

All objects can be moved from one application to another.

Appendix A, "Icons and Menus" describes the icons and menus used in Cisco MGM.

2.1.8.1 Using Popup Menus

The popup menus are available from any application.

The popup menu options are enabled based on your security profile. To display the popup menus, you can right-click from the following options:

- Away from the network in Graphical View.
- A network from the Hierarchical Tree or Graphical View.
- A node from the Hierarchical Tree or Graphical View.
- A card, line, path, or port from the Hierarchical Tree or Graphical View.

Table 2-8 describes the popup menu options available in Configuration Center, Diagnostic Center, Chassis View, and Statistics Report applications.

Table 2-8 Popup Menu Options in Configuration Center, Diagnostic Center, Chassis View, and Statistics Report applications

Option	Description
Chassis View	Launches Chassis View after you select a node from the Hierarchical Tree.
Configuration Center	Launches Configuration Center with or without selecting an object.
Diagnostics Center	Launches Diagnostics Center. You must select an object from the Hierarchical Tree.
Statistics Report	Launches the Statistics Report Tool with or without selecting an object.
Administration	
Cisco MGM Audit Trail	Launches Cisco MGM Audit Trail to view the audit trail viewer.
Telnet	Establishes a telnet session with the switch.
SSH[1]	Connects to a node by using a secured shell.
View Management	
Sort	Sorts the tree.

[1] SSH = secured shell

2.1.9 Using Mnemonics

All Cisco MGM menus and menu options have a uniquely assigned mnemonic to support keyboard access to menu items in addition to the mouse. For example, to exit the Cisco MGM application, enter **Alt+f** (for the File menu); then, enter **x** (Exit).

2.1.10 Using the Online Help

The online help provides a detailed explanation of each Cisco MGM GUI window and dialog box.

To view the online help for the current Cisco MGM window, you have two options:

- Choose **Help > Current Window**
- Click the **Help** tool.

To view the online help for any Cisco MGM dialog box, click the **Help** tool within the dialog box.

Tip Use the print option in the browser that displays the online help to print the selected page.

2.1.11 Using the Pin Tool

The Dashboard, Configuration Center, Diagnostic Center, Chassis View, and Statistics Report applications have a pin tool. The pin point is up when the tool in *pinned up,* and down when the tool is *pinned down*. The function of the pin tool differs depending on where it is used:

- If you click the pin tool in the Dashboard window, the window is pinned down, meaning that it is not brought to the foreground by default. If you click the pin tool again, the Dashboard window is pinned up, meaning that it is brought to the foreground each time an update occurs (alarm counts change, NE count changes, and so on).
- If you click the pin tool in the Configuration Center, Diagnostic Center, Chassis View, and Statistics Report windows, that instance of the application window is pinned down, and another instance of that application can be opened (for example from the Tools menu). If the pin tool is pinned up, then another instance of the application cannot be opened.
- If you click the pin tool in the Configuration pane in the Configuration Center, Diagnostic Center, Chassis View, and Statistics Report applications, that pane is pinned down, and an additional Configuration pane can be opened without overwriting the open pane.

2.2 What Basic Functions Can I Perform in Cisco MGM?

This section outlines basic functions that you can perform within Cisco MGM, including:

- 2.2.1 Launching Context-Sensitive Information
- 2.2.2 Filtering Data
- 2.2.3 Exporting Data
- 2.2.4 Exporting Alarms and Events
- 2.2.5 Refreshing Data
- 2.2.6 Pruning the Database

2.2.1 Launching Context-Sensitive Information

Many Cisco MGM views have a specific selection context, meaning that the same window will have a different look depending on where it was launched.

For example, if you launch the Alarm Browser from the management domain node, the browser shows all NE and EMS alarms (if you have permission to see EMS alarms). If you launch the Alarm Browser from a group or NE node, the browser shows only NE alarms. If you launch the Alarm Browser from the Dashboard, the browser shows all NE alarms for the Cisco MGM domain.

2.2.2 Filtering Data

Filter dialog boxes filter user-specified data. Many Cisco MGM tables have Filter dialog boxes that enable you to filter data in different ways and display the results in a table.

2.2.3 Exporting Data

Most Cisco MGM tables support an export function to export the table contents to a flat file. The Export dialog box allows you to export the data as comma-separated values (CSVs) or tab-separated values (TSVs), which are formats commonly used to import data into spreadsheet and database applications for further analysis and manipulation. Click the **Other** radio button if you want to separate the Cisco MGM data values with a different character. If you specify a character as a separator and your data contains the same character, the character in the data is automatically enclosed in double quotes. This allows the spreadsheet or database application to understand that the character is part of your data. Regardless of whether you select Comma-Separated, Tab-Separated, or Other, Cisco MGM automatically encloses text in double quotes if it has a separator.

Note If you export data to Microsoft Excel, save the exported file with ".csv" as the filename extension.

To export only the selected row(s), click the **Selected row(s)** radio button. To export all rows in the page, click the **All rows in current page** radio button.

By default, exported data is stored in the C:\Cisco\CiscoMGMClient<*version_number*>\exports or /opt/CiscoMGM<*version_number*>/exports directory under the name that you provide in the "Export data to file" text box. Click **Browse** to change the file location.

Note The default directory /opt/CiscoMGMServer may have been changed during installation of the Cisco MGM server.

2.2.4 Exporting Alarms and Events

In addition to exporting directly from the Alarm Browser or the Alarm Log, Cisco MGM provides an Event Export Manager that allows you to export alarms and events as they occur to the file of your choice. You can also set various export parameters to refine the export. You can choose to export events continuously or to export a specific number of events.

To export events continuously, in the Diagnostic Center, choose **Fault > Event Export Manager**, then click **Start Export**.

The Event Export Manager will export events continuously until you click **Stop Export**, or until the current Cisco MGM session ends, whichever occurs first.

To export a specific number of events, check the **Stop export when** check box, enter a number of records, and click **Start Export**. The export will stop after the specified number of events are logged.

Table 2-9 describes the fields in the Event Export window.

Table 2-9 Field Descriptions for the Event Export Manager

Field	Description
Network Elements	Allows you to export alarms (NE alarms and Cisco MGM-specific EMS alarms) and events for selected NEs. Choose from the list of available NEs and add them to the Selected list. If you have the appropriate user permission and you want to export EMS alarms and events, check the **Export MGM EMS Alarms/Events** check box.
Severity	Allows you to export events that have a severity of Critical, Major, Minor, Warning, Indeterminate, and/or Cleared.
Export To	Allows you to export the file to a given destination. Click **Browse** to browse for a particular destination. You can also overwrite or append the file.
Export Options	Allows you to specify the field separator type. Types include Comma, Tab, Semicolon, or Other, an option you use to specify a different separator. You can also check the **Stop export when** check box and enter a number of records to instruct the Event Export Manager to stop exporting after the user-specified number of records are logged.

2.2.5 Refreshing Data

Many Cisco MGM windows have a Refresh Data tool that refreshes all data being displayed by Cisco MGM. There are two versions of the Refresh Data tools, and both refresh data from either the server or the database.

- The Refresh Data tool flashes when updates are available. This tool has two modes: manual refresh and autorefresh.
- The Refresh Data tool does not notify you that updates are available. You must click the tool to retrieve updated data.

Note Clicking Refresh Data in the Domain Explorer window refreshes all data for the entire Cisco MGM client. Depending on the number of NEs in your network, you might experience a delay while the data refreshes.

2.2.6 Pruning the Database

Cisco MGM automatically prunes various categories of Cisco MGM data that tend to accumulate over time and would otherwise exhaust the available disk space. See 5.1.4 Pruning the Database. You can configure the following categories of data for automatic pruning:

- PM data
- FM data
- Audit log data
- Error log data
- Self-monitor data
- Job monitor data

The following options are provided to control the pruning for each category of data:

- Enable/disable
- Retention period
- Time of day to perform the pruning

2.3 What Are the General Features of Cisco MGM?

This section describes some of the general Cisco MGM features, including:

- 2.3.1 What is FCPS?
- 2.3.2 Understanding Fault Management
- 2.3.3 Understanding Configuration Management
- 2.3.4 Understanding Performance Management
- 2.3.5 Understanding Security Management
- 2.3.6 Using the Diagnostic Center
- 2.3.7 Managing Cisco MGM CORBA Interfaces

2.3.1 What is FCPS?

Cisco MGM's strategy is to provide a carrier-class fault, configuration, performance, and security (FCPS) EMS.

FCPS refers to the different types of information handled by management systems. A fifth area, accounting, is often included, making the acronym *FCAPS*. However, Cisco MGM does not support accounting management currently. Table 2-10 describes the FCPS functions.

Table 2-10 FCPS Framework Functionality

Function	Description	For More Information, See
Fault management	Detects, isolates, corrects, and reports faults for the network and service. Fault management tracks the correlation of related services; for example, reliability, availability, survivability, quality assurance, alarm surveillance, alarm management, fault localization, fault correction, testing, and trouble administration. Fault management in Cisco MGM can be performed in the Diagnostic Center or in the Configuration Center. The Alarm Browser, Alarm Log, and Dashboard also provide information on fault management.	Chapter 9, "Managing Faults"
Configuration management	Configures and controls NEs, identifies resources, collects information about a resource, and manages intra-chassis connections. Configuration management deals not only with the state of NEs, but also with the provisioning of resources and services. Generally, configuration management involves network planning, installation, service planning and negotiation, service provisioning, equipment provisioning, status and control, and network topology. The Configuration Center is your primary resource for configuration management.	Chapter 6, "Configuring Hardware"

Table 2-10 FCPS Framework Functionality (continued)

Function	Description	For More Information, See
Performance management	Gathers and reports the behavior of NEs, network, and services, including quality assurance, monitoring, management control, and analysis. Performance management can be performed in the Configuration Center or in the Statistics Report.	Chapter 10, "Managing Performance"
Security management	Prevents and detects any improper use of network resources and services as well as recovery from security violations. Aspects of security management include prevention, detection, containment, and recovery.	Chapter 8, "Managing Security"

2.3.2 Understanding Fault Management

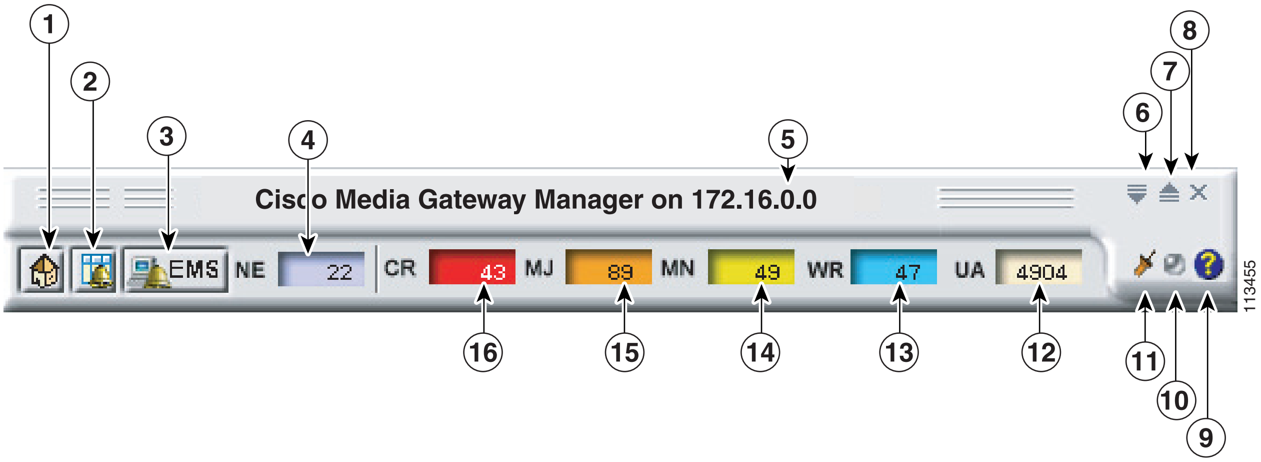
Fault management enables the network administrator to avoid catastrophic conditions through alarms and early warnings. The primary basis for fault management is provided by real-time messages (traps) generated by network elements when a change in status occurs.

The fault management tools for Cisco MGM are described in Table 2-11.

Table 2-11 Fault Management Tools

Name	Description
Alarm Management	Identifies network problems and failures by using alarm management. For more information, see Chapter 9, "Managing Faults."
Device Management with Chassis View	Provides a graphical view of equipment status for the operational and alarm status of each card, port, line, or trunk, which is represented with a predefined color. For more information, see 2.3.3.2 Managing Devices with Chassis View, page 2-18.
Diagnostic Center	Generates real-time displays of element performance and utilization using system counters repeatedly polled with SNMP, and facilitates the monitoring of activity and error rates of individual ports, lines, and trunks. By periodically polling each network element through SNMP, real-time counters detect and display hardware failures at the card, interface, port, line, and trunk level. Monitors statistics events to identify problems with Cisco MGM to effectively manage the network. For more information, see section 2.3.6 Using the Diagnostic Center, page 2-25.
Alarm Browser	Displays standing alarms and conditions in the managed domain. The Alarm Browser window lists the conditions that are assigned a severity level of critical, major, minor, or warning. It also shows cleared alarms that are not acknowledged. For more information, see Chapter 9, "Managing Faults."
Alarm Log	The Alarm Log window contains alarms that have transitioned from the Alarm Browser. Cleared alarms are transitioned when you acknowledge them or when automatic acknowledgment has been enabled (in the Control Panel > User Interface Properties pane). In addition, the Alarm Log shows a history of cleared and acknowledged alarms and all transient conditions (also known as events or autonomous nonalarmed messages). For more information, see Chapter 9, "Managing Faults."
Dashboard	The Cisco MGM Dashboard shows useful alarm and NE information in one easily accessible location. See Figure 2-1.

Figure 2-2 *Dashboard*



1	Layers the Domain Explorer window as the top active window. The Domain Explorer is the Cisco MGM home window[1].	**9**	Displays online help for the Dashboard.
2	Opens the Alarm Browser window; this highlights NE-specific critical, major, minor, and warning alarms.	**10**	Indicates a change in Cisco MGM status, including: • New alarms have occurred on NEs in the domain • New NEs have been added to the domain • Connectivity status has changed When a change in Cisco MGM status occurs, a blue outline appears around the affected EMS alarms icon, NE count box, or alarm count box(es). Click the Cisco MGM Status has Changed tool to acknowledge the status change. The tooltip toggles to No Change in Cisco MGM Status and the blue outline disappears, which indicates that you acknowledged the status change.
3	Opens the Alarm Browser window, filtered to show all EMS alarms in the domain. This tool is enabled only if you have read/write permission for the Show Cisco MGM EMS Alarms/Events operation.	**11**	If you click the pin tool, the Dashboard window is *pinned down*, meaning that it is not brought to the foreground by default. If you click the pin tool again, the Dashboard window is *pinned up*, meaning that it is brought to the foreground each time an update occurs (alarm counts change, NE count changes, and so on).
4	Lists the total number of NEs in the domain. Click the counter to open the Domain NE table, which provides an inventory of NEs within the selected management domain.	**12**	Lists the number of unacknowledged alarms in the domain. The alarm count includes unacknowledged alarms on NEs and on the EMS. Click the counter to open the Alarm Browser window, filtered to show all unacknowledged alarms.
5	Displays the server IP address.	**13**	Lists the number of warning alarms in the domain. The alarm count includes warning alarms on NEs and on the EMS. Click the counter to open the Alarm Browser window, filtered to show all warning alarms.

6	Minimizes all Cisco MGM windows, except for the Dashboard window itself.	**14**	Lists the number of minor alarms in the domain. The alarm count includes minor alarms on NEs and on the EMS. Click the counter to open the Alarm Browser window, filtered to show all minor alarms.
7	Restores all minimized Cisco MGM windows.	**15**	Lists the number of major alarms in the domain. The alarm count includes major alarms on NEs and on the EMS. Click the counter to open the Alarm Browser window, filtered to show all major alarms.
8	Closes the Dashboard.	**16**	Lists the number of critical alarms in the domain. The alarm count includes critical alarms on NEs and on the EMS. Click the counter to open the Alarm Browser window, filtered to show all critical alarms.

[1] For a legend of Domain Explorer icons, see Appendix A, "Icons and Menus."

2.3.2.1 Defining Events and Alarms

Events and alarms are different with the following requirements:

- Events are network-generated entities that do not have any state or duration.
- Alarms are Cisco MGM generated entities that do have state and duration.
- Alarms and states are changed based on Cisco MGM receiving certain events.
- Only a subset of all events results in alarm state changes.

2.3.3 Understanding Configuration Management

Note For detailed information on configuration management, see Chapter 6, "Configuring Hardware."

Configuration management in Cisco MGM includes both the configuration of individual network elements at the port and line level, and the provisioning of user services, for example, network elements and connections.

These topics describe configuration management for Cisco MGM:

- 2.3.3.1 Configuration Center Overview, page 2-17
- 2.3.3.2 Managing Devices with Chassis View, page 2-18
- 2.3.3.3 Understanding Inventory Management, page 2-18
- 2.3.3.4 NE Release Management, page 2-19

2.3.3.1 Configuration Center Overview

The Configuration Center enables internal chassis connection configurations into one application.

The Configuration Center window has three main areas:

- Hierarchy Pane—Displays the network hierarchy as a tree of objects with real-time alarms. The tree is used to navigate the networks from the network level down to the port level.
- Configuration Pane—Displays the elements of the selected object. If an object is not selected, the configuration window is empty.

- Inspector View—Provides a list of detailed information for the selected network element from the hierarchy view. Click the **Show static data** button to update the information in the Inspector View.

2.3.3.1.1 Network Elements Overview

By performing network element configuration tasks, you can:

- Communicate with individual network elements, for example, a switch or a concentrator, using Simple Network Management Protocol (SNMP).
- Obtain a list of inventory data, for example, ports under a line or cards in a node.
- Create templates for all network elements.

2.3.3.1.2 Connections Overview

Configuration Center creates new connections, displays, modifies, and deletes existing connections. You select the desired connection end-points and configure the connection type and class of service. The end-to-end connection is automatically established between two cards in the switch. In addition, the status for each connection is viewed from one endpoint to the other.

By performing connection configuration tasks, you can:

- Provision SPVC connections for VISM, ATM and RPM.
- Configure the traffic parameters and other parameters for each end of the connection.
- Configure the connection parameters for the end-to-end connection.
- Add Descriptors to the connections.

2.3.3.2 Managing Devices with Chassis View

The front and rear panel displayed within the Chassis View provide a real-time indication of the status of individual cards, lines, and ports for the network device. Both card and line alarms (LEDs) are provided for all platforms and service modules.

By managing the graphical representations of the network nodes and device objects with Chassis View, you can:

- Provide status updates for nodes, cards, and lines.
- Display the front or rear view of the node.
- Perform provisioning tasks, such as, shelf, card, and line levels by quickly navigating to the Configuration Center.
- Display the LED status for each card reflecting both standby and active states.

2.3.3.3 Understanding Inventory Management

Inventory information is another component of configuration management. Cisco MGM provides two levels of inventory reports:

- Domain NE table—A complete list of all the NEs that belong to a specific group or to the entire domain.
- Equipment Inventory table—A detailed list of cards and modules installed on a specific NE. For detailed information about inventory reports, see Chapter 11, “Managing Inventory.”

2.3.3.3.1 Adding New NEs to the Cisco MGM Domain

The Add New NE wizard allows you to add a new NE, or to add several new NEs at once. The wizard allows you to enter multiple NE IP addresses one at a time, or enter a beginning and ending IP address and automatically add a range of NEs.

2.3.3.3.2 NE Connectivity and Operational States

The operational state of an NE can have the following values:

- Under Maintenance—The NE is temporarily under maintenance but requires monitoring. This state is the same as In Service except that Cisco MGM does not report alarms or events for under-maintenance NEs.
- In Service—The NE is currently deployed and requires monitoring. Cisco MGM collects polling, FM, configuration management, and PM data from in-service NEs and stores the data in the database.
- Out of Service—The NE has been marked Out of Service by a network administrator and does not require monitoring. The Cisco MGM database records the last known state of the NE when it was in service.
- In Service–Initializing—The NE is marked as In Service–Initializing when Cisco MGM connects to the NE (Communication State is marked as Available) and the discovery process starts. The initialization process is completed when fault and inventory have been synchronized. The operational state changes from In Service–Initializing to In Service–Synch Configuration.
- In Service–Sync Configuration—The NE is marked as In Service–Sync Configuration when Cisco MGM uploads a configuration for that NE. You can change the operational state of an NE from In Service–Sync Configuration to Out of Service.

The communication state of an NE can have the following values:

- Not Applicable—The NE is Out of Service. The connection to the NE has not been established or has been dropped.
- Available—The NE is In Service or Under Maintenance and Cisco MGM is connected to the NE. The NE is declared Available when the NE is reachable and supported by Cisco MGM (as defined in the Administration > Supported NE table).
- Unavailable—The NE is In Service or Under Maintenance but Cisco MGM cannot establish a connection to the NE. When Cisco MGM loses the connection to the NE, an EMS alarm with a probable cause of “Connection loss” is generated.

2.3.3.4 NE Release Management

An NE added to the Cisco MGM domain is discovered and managed by Cisco MGM only if the NE software version is defined in the Supported NE table.

Note See *Cisco Media Gateway Manager 5.0 Release Notes* for the NE software versions that are supported in Cisco MGM 5.0. The Cisco MGM release notes are available on the product CD and online at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/optnet/mgm/mgmreln/index.htm.

Caution Before updating the software image on an NE, check the Cisco MGM release notes to verify whether the NE software version is supported in this Cisco MGM release.

The following NE administration features are available for the Cisco MGX 8880 and Cisco MGX 8850:

- Software download
- Memory backup and restore
- Job monitoring
- NE Software table (used to commit or revert software images)

2.3.3.4.1 Software Download Dialog Box

Use the Software Download dialog box to download software to NEs. After the download is complete you can use the NE Software table to activate the software. The downloaded software becomes the active version, and the active version becomes the standby version. Cisco MGM stores two software versions, active and standby.

2.3.3.4.2 Memory Backup Dialog Box

Use the Memory Backup dialog box to back up configuration and provisioning information that resides in the flash memory of an NE. By default, the local Cisco MGM server automatically backs up the memory of NEs once a day for seven days and stores the backup files on the Cisco MGM server. After seven days, the oldest backup file is replaced by the current backup.

2.3.3.4.3 Memory Restore Dialog Box

Use the Memory Restore dialog box to restore provisioning and configuration information stored in the flash memory of an NE.

2.3.3.4.4 Job Monitor Table

The Job Monitor table provides information about scheduled administrative tasks such as task type, task owner, task status, task start and end time, and so on.

2.3.3.4.5 NE Software Table

The NE Software table displays the active and standby software versions for the NE. From this table, you can activate new software or revert software on NEs.

2.3.4 Understanding Performance Management

The performance management function in Cisco MGM involves the system's ability to collect and store massive amounts of statistical data for network activity.

Note For detailed information on performance management and the Statistics Report, see Chapter 10, "Managing Performance."

2.3.4.1 Statistics Report

You can use the Statistics Report to view reports of statistics data that are collected from the switch.

You can launch the Statistics Report from various Cisco MGM applications, such as the Diagnostic Center, Configuration Center, or Chassis View. The Statistics Report appears in the toolbar.

To launch Statistics Report, choose **Performance > MGX 8880/8850MG > Statistics Report**.

Depending upon the report selected, you can identify certain criteria, such as network object, type of statistics, granularity, report interval, and graphical format.

Note VISM cards are supported for the Statistics Report.

Table 2-12 lists the report types that are supported for each network element from the Hierarchical Tree.

Table 2-12 Report Types for Each Network Element

Network Element	Report Types
Network	Supports the following report types: • Raw Data Report for cards, lines, ports, and trunks in the network. • Utilization Data Report for ports and trunks in the network.
Node	Supports the following report types: • Raw Data Report for all cards, lines, ports, PNNI, trunks, and paths on the node. • Utilization Data Report for ports and trunks on the node.
Card	Supports the following report types: • Raw Data Report for all cards[1], lines, ports, PNNI, trunks, and paths on the card. • Utilization Data Report for connections, ports, and trunks on the card.
Port	Supports the following report types: • Raw Data Report for ports and connections on the selected port. • Performance Data Report for ports and connections on the selected port. • Utilization Data Report for ports and connections on the selected port.
Line	Supports the following report types: • Raw Data Report for the line. If applicable, additional statistics are shown for physical lines.
Paths	Supports the Raw Data Report for paths and other elements.

[1] Card support is used only for AXSM cards.

2.3.5 Understanding Security Management

Security management protects the revenue-generating assets in the network. Examples of security management include:

- Controlling access to element management functions
- Controlling access to network logical resources

Security for the Cisco MGM system can be divided into the following areas:

- Cisco MGM security domain: To log into the Cisco MGM client, a username and password are required. A user profile defines the access privileges. Cisco MGM passwords are stored using MD5 one-way encryption.

- OSS security domain: OSS-to-Cisco MGM sessions are configured by the Cisco MGM GateWay EMS-to-NMS interface architectural component.
- NE security domain: At the NE level, a username and password are configured to enable the user to connect directly through the console port (EIA/TIA-232), through the management port (10BASE-T), or remotely through an SSH or Telnet session. NE passwords are stored using base-64 two-way encryption.
- Cisco MGM server login: You must have root user privileges to log into the Cisco MGM server workstation for debugging or changing the Cisco MGM server program. A username and password are required.
- Oracle database access: Access to the Oracle database requires Oracle root user authentication, as well as Cisco MGM database access authentication. The Oracle username and password are encrypted in the server configuration file.

Cisco MGM supports the following security features:

- 2.3.5.1 Logging into the Client, page 2-22
- 2.3.5.2 Login Advisory Message, page 2-22
- 2.3.5.4 User Management and Profiles, page 2-23
- 2.3.5.5 NE Access Control, page 2-24
- 2.3.5.6 Audit Log, page 2-24

2.3.5.1 Logging into the Client

See *Cisco Media Gateway Manager 5.0 Installation Guide* for the procedure to log into the Cisco MGM client on a Windows or Solaris workstation.

2.3.5.1.1 Locking and Unlocking the Client

A Cisco MGM client is locked automatically after a defined period of inactivity.

- To manually lock the Cisco MGM client, select **File > Lock Cisco MGM Client** in the Domain Explorer. The Cisco MGM Locked window opens, indicating that the Cisco MGM client is locked.
- To unlock the Cisco MGM client, enter your password in the MGM Locked window; then, click **Unlock**.

2.3.5.2 Login Advisory Message

The following is the default advisory message after logging into the Cisco MGM client:

```
NOTICE: This is a private computer system. Unauthorized access or use may lead to
prosecution.
```

You can customize the default advisory message, or disable it altogether. For more details, see Chapter 8, "Managing Security."

2.3.5.3 Understanding Network Partitioning

You can configure for network partitioning by dividing the network into logical areas. You can then access only the areas that are specified under your security profile. The nodes and elements must fall under the area or areas that fit your security profile for each Cisco MGM application.

You can:

- Define the network partitions from the associated list of nodes.
- Define, modify, and view the areas within your network.
- Manage only the areas under your security profile.
- Manage connections that originate and terminate within the assigned area(s). The domain can include multiple areas.

2.3.5.4 User Management and Profiles

Cisco MGM user management includes the ability to:

- Manage predefined default user profiles with different access privileges, also known as network partitioning, which allows you to define user types and levels of access to the network. The default user types are:
  - SuperUser—Users who have access to all operations associated with the Cisco MGM server and client.
  - SysAdmin—System administrators who manage Cisco MGM access. They can perform limited tasks associated with the Cisco MGM server and client. This privilege is primarily used as the main profile when Cisco MGM has been initially installed.
  - NetworkAdmin—Typically, network operations center (NOC) supervisors who perform daily network surveillance, provisioning, and PM activities on any group or NE.
  - Provisioner—Users who perform daily network surveillance, provisioning, and PM activities on specific NEs. Each Provisioner can have only one active session. Provisioners cannot access administrative information.
  - Operator—Users who perform daily network surveillance and PM activities on specific NEs. Each Operator can have only one active session. Operators cannot access administrative information.
- Create, delete, modify, and duplicate custom user profiles with certain privileges. Custom user profiles are grouped into categories and each category has a set of operations.
- Create, delete, or modify Cisco MGM users; lock or unlock user accounts; view logged-in users; and end active user sessions.
- Regulate user logins, including password aging, number of failed login attempts before an account lockout, login disable period, lockout time, and logout time.
- Configure the username and password used by the Cisco MGM server and Cisco MGM GateWay/CORBA to access NEs.
- View, add, modify, and delete NE user accounts on one or more NEs.

Note For detailed information about user management, see Chapter 8, "Managing Security."

2.3.5.4.1 Configuring Cisco MGM User Access

You can configure user access by using the Administration menu, which provides controlled access (network partitioning) to multiple users of Cisco MGM, based on the user's UNIX user-ID and password. The Administration menu is launched from the Domain Explorer window.

By configuring user access, you can:

- Provide user-access profiles that can be customized for each user. The user-access profile is a list of operations or actions a user can perform coupled with assigned access privileges for each action.
- Assign access privileges to read, create (write), modify, and delete profiles.

  By default, only the *root* user can start and stop the Cisco MGM core processes. The *root* user has sufficient access privileges to launch all Cisco MGM applications and administer security.

Other users are assigned access privileges that enable them to perform operations within security-controlled applications. Depending on the setting of access privileges by those who administer security management, the operations are limited. Without the proper access privileges, users cannot launch security-controlled applications.

Note For detailed information about user access, see Chapter 8, "Managing Security."

2.3.5.5 NE Access Control

NE access control includes the ability to:

- Configure the username and password used by the Cisco MGM server and Cisco MGM GateWay/CORBA to access NEs and retrieve alarms, configuration, and inventory information.

  Note Each username and password specified must exist on the selected NE in order for Cisco MGM to manage it. A new or modified password takes effect at the next reconnection.

- Configure the username and password on multiple NEs by using the bulk NE authentication feature. With a single operation, you can specify the same username and password for NEs that belong to the same group or are assigned to the same user.
- Manage NE user accounts by using the NE User Access Administration table. This feature supports the ability to view, add, modify, and delete NE user accounts on one or more NEs.
- Monitor active NE users and log out selected users.
- Add predefined users on a selected NE.

2.3.5.6 Audit Log

The Audit Log contains information about significant events (user-initiated changes and activities) that occurred on the Cisco MGM server during a specific time period for the purposes of establishing accountability. It also helps in identifying remedial actions to correct an improper activity. The Audit Log is implemented in the Cisco MGM database, where each record has a time stamp, record type, and message string.

Tip See Chapter 8, "Managing Security" for a list of runtime-affecting operations that the Audit Log records for monitoring purposes.

2.3.6 Using the Diagnostic Center

Note For detailed information about using the Diagnostic Center, see Chapter 9, “Managing Faults.”

You can launch the Diagnostic Center from various Cisco MGM applications, such as the Statistics Report, Configuration Center, or Chassis View. The Diagnostic Center tool appears in the toolbar.

To launch the Diagnostic Center, you can:

- Choose **Fault > MGX 8880/8850MG > Diagnostic Center**.

The Diagnostic Center consolidates all the following diagnostic operations:

- 2.3.6.1 Diagnostic Operations for Network Elements, page 2-25
- 2.3.6.2 Diagnostic Operations for Network Manageability, page 2-25
- 2.3.6.3 Diagnostic Operations for Connections, page 2-25

2.3.6.1 Diagnostic Operations for Network Elements

You can diagnose network elements, for example, networks, nodes, cards, lines, ports, paths, or trunks.

By diagnosing network elements, you can:

- Monitor real-time counters.
- Extend support for the Node Resync process to allow for two different levels.
- Configure bit error rate test (BERT) to verify the integrity of a network element by measuring error statistics.

2.3.6.2 Diagnostic Operations for Network Manageability

You can monitor statistic events for network manageability to collect element management health-related statistics. In addition, you can:

- Verify that all the nodes in the network are managed correctly by Cisco MGM.
- Identify general network problems.
- Provide success rates, failure rates, and throughput of Cisco MGM to protocols such as FTP and SNMP.
- Create a trouble ticket that extracts all the information from the History Panel.

2.3.6.3 Diagnostic Operations for Connections

By diagnosing connections, you can:

- Access fault management capabilities in the form of diagnostic tests for connections, which include continuity (integrity) facility for PNNI soft permanent virtual connection (SPVC).
- Perform general test operations such as up and down connections, and connection loopback.

2.3.7 Managing Cisco MGM CORBA Interfaces

Chapter 12, "Managing CORBA Interfaces." describes the management of Cisco MGM GateWay/CORBA, which allows another program or application to communicate with the Cisco MGM server, and also about CORBA management, which allows communication between the Cisco MGM client and server.