



Managing Faults

This chapter describes the process of fault management, and details the options available in Cisco MGM to locate, diagnose and correct network problems. This chapter includes the following information:

- [9.1 What Is Fault Management?](#)
- [9.2 Where Can I Get Information on Affected Services and Customers?](#)
- [9.3 What Fault Information Can I See?](#)
- [9.4 Is the Service Working?](#)
- [9.5 Where Is the Fault?](#)
- [9.6 How Can I Use Advanced Debugging to Find the Cause of the Fault?](#)
- [9.7 What Is the Fault Priority?](#)
- [9.8 Who Is Responsible for Managing the Fault?](#)
- [9.9 How Did You Manage the Fault?](#)

9.1 What Is Fault Management?

Fault management (FM) is the process of locating, diagnosing, and correcting network problems. This is important for increasing network reliability and effectiveness, and for increasing the productivity of network users. Fault management is more than just handling emergencies. It is the detection, isolation, and correction of abnormal conditions in the network and its environment. It provides functions for managing problems with services and handling customer-facing service problems.

Efficient fault management can:

- Reduce repair costs through efficient fault detection, location, and correction.
- Improve customer care through efficient trouble administration.
- Improve service availability and equipment reliability through proactive maintenance and through measurement, review, and corrective action.

One responsibility of fault management is to detect faults. A piece of equipment, a transmission medium, a software module, or a database is said to be in a fault state if it cannot perform its intended function and meet all of the requirements placed on that function. The onset of a fault is called a *failure event* and is usually signaled by one or more alarm reports. The termination of a fault state is called a *clear event*.

Fault management is responsible for determining, from a variety of information sources, the root cause of a fault, and for its repair. In certain cases, the root cause of a fault may be in a connecting network. In such cases, fault management is responsible for reporting the problem through appropriate channels.

Service assurance is the overall process of ensuring that the purchased level of service is delivered. The Element Management System (EMS) plays a key role in maintaining the health of both network elements and transmission facilities. This is done in conjunction with other systems, typically at the network management layer and service management layer. The EMS can be the primary repository of detailed history of NE-specific faults and events, technician action, and performance data.

The steps for successful fault management are:

1. Identify a problem by gathering data about the state of the network (polling and trap generation).
2. Restore any services that have been lost.
3. Isolate the cause, and decide if the fault should be managed.
4. Correct the fault if possible.

9.1.1 What the NE Provides

NEs can provide the following information that is required for effective fault management:

Currently deployed, intelligent NEs provide the management system with the following, which are required for effective fault management:

- Detection of the four main types of failure:
 - Equipment failure—Detected through failure detection mechanisms built into the hardware, and through routine exercises and diagnostics.
 - Software failure—Detected through failure of software checks, and through routine audits.
 - Communications failure—Detected through defects in the incoming signal or communicated from the distant end of a trail in an embedded operations channel by the signal processing chip sets, and through continuous or periodic measurements of incoming and outgoing signal characteristics. Defects include line coding errors, framing bit errors, parity errors, cyclic redundancy check errors, and addressing errors. Signal characteristics include, optical or electrical power, analog signal to noise ratio, and deviation from required voltage or wavelength.
 - Environmental failure—Defects could include power faults such as overheating.
- Notification of failure—NEs notify Cisco MGM when a failure occurs by generating an alarm report. The NE can also report a summary of current fault states, or replay its log of historical failures and clears.
- Notification of changes in the operational state of the NE's components—If a component of the NE is in the fault state, then Cisco MGM should not receive (or expect to receive) further alarms, alerts, or scheduled performance data from that component if the alarm is not cleared.

Cisco MGM forwards information northbound and integrates with other third party management systems to give options not directly available in Cisco MGM.

9.1.2 Fault Notification and Maintenance

Fault notification and maintenance can be proactive or reactive:

- Proactive notification—Where X notifies Y of a problem regarding a service delivered from X to Y.
- Reactive maintenance—Where Y contacts X to query X on potential problems in X's domain.

9.1.2.1 Proactive Maintenance

Automated detection tests and surveillance software enable rapid initiation of the repair process, sometimes even before customers have noticed a problem. This is called proactive maintenance and promotes customer satisfaction.

Proactive maintenance consists of functions and processes associated with the detection, analysis, isolation, and resolution of problems by means that are independent of customer trouble reports. The problems may be faults or degradations in equipment or transmission media.

The goals of proactive maintenance are to:

- Detect and fix service quality problems before the customer calls to establish a trouble report (ideally), or at least to start the repair process before the customer calls, thereby minimizing the time, as perceived by the customer, before service is restored.
- Maintain the transport network at a high level of quality by identifying the facilities that perform relatively poorly and rehabilitating them.

9.1.2.2 Reactive Maintenance

Reactive maintenance is required when a failure occurs. This type of problem can be time-consuming and costly. It requires accurate administration of trouble reports, rapid analysis and repair of service affecting faults, and notifications to customers of restoration of service, all of which also promote customer satisfaction.

9.1.3 Root Cause Analysis

The *root cause* is the most basic reason for an undesirable condition or problem that, if eliminated or corrected, would have prevented the problem from existing or occurring. The outcome of the root cause analysis is not a restatement of the most obvious symptom, but is the result of a methodical analysis of the problem situation, leading to the most basic cause.

Root cause analysis captures additional information about defects for the purpose of identifying preventive actions.

Cisco MGM includes advanced debugging features which capture additional information about defects.

9.2 Where Can I Get Information on Affected Services and Customers?

The first thing to do in fault management is to identify what services and which customers are affected by the fault. Cisco MGM provides a number of options for viewing this information, including:

- [9.2.1 Dashboard](#)
- [9.2.2 Tooltips](#)
- [9.2.3 Domain Explorer](#)
- [9.2.4 Alarm Browser](#)
- [9.2.5 Network Map](#)
- [9.2.6 Diagnostic Center](#)

Then you need to identify the alarms:

- [9.3.1 How Are Alarms Displayed?](#)

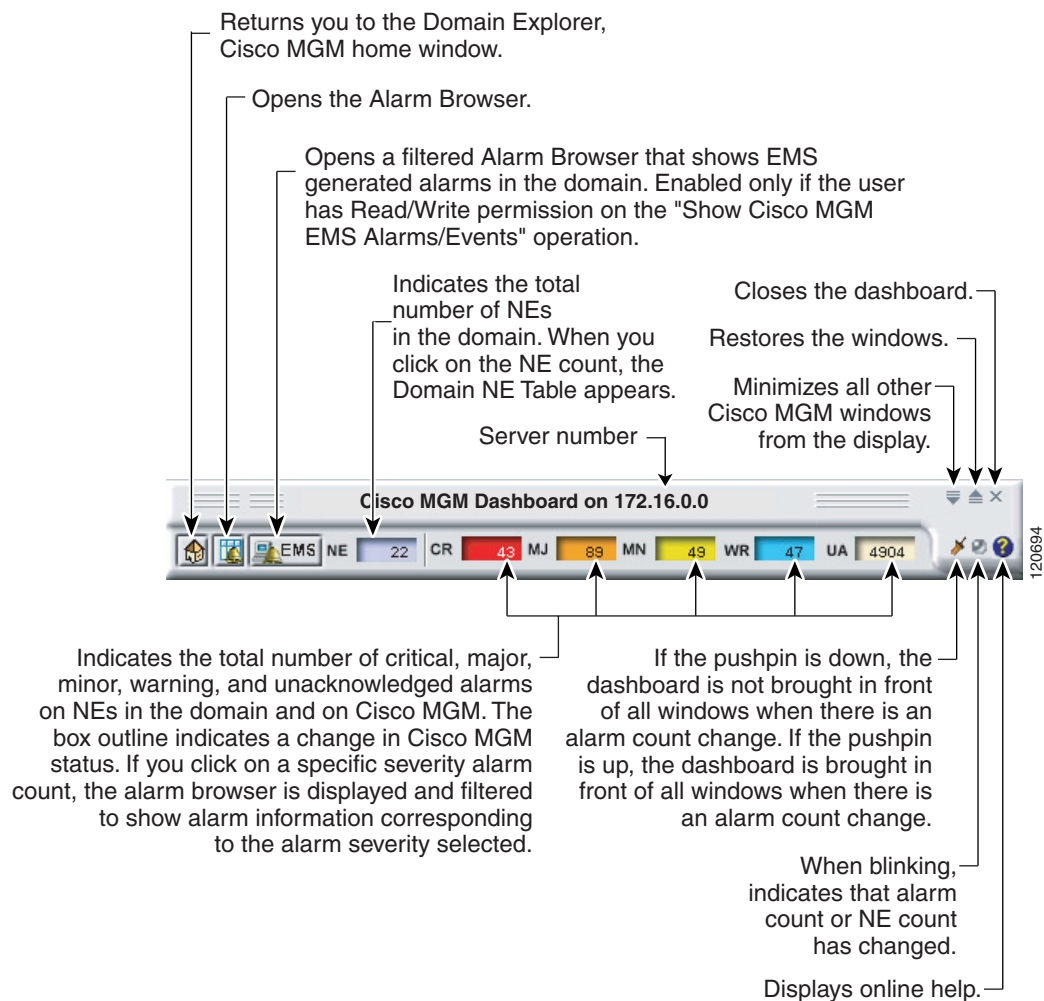
When a module is under maintenance, you can suppress the alarms so that they are not displayed on the Cisco MGX Alarm or History tab or on any other client:

- [9.3.2 Suppressing Alarms](#)

9.2.1 Dashboard

The Dashboard shows useful alarm and NE information in one easily accessible location. See [Figure 9-1](#).

Figure 9-1 Dashboard



**Note**

If you click an alarm count box in the Dashboard, the Alarm Browser appears (see [Figure 9-3](#)), prefiltered for the selected alarm severity.

If there is a change in the alarm count, and the pushpin is up, the Dashboard is moved to the front of the other windows.

9.2.2 Tooltips

A tooltip appears with the actual alarm counters when the cursor is positioned over a managed object (domain, group, NE, or board). The tooltip displays a count for each of the following severities:

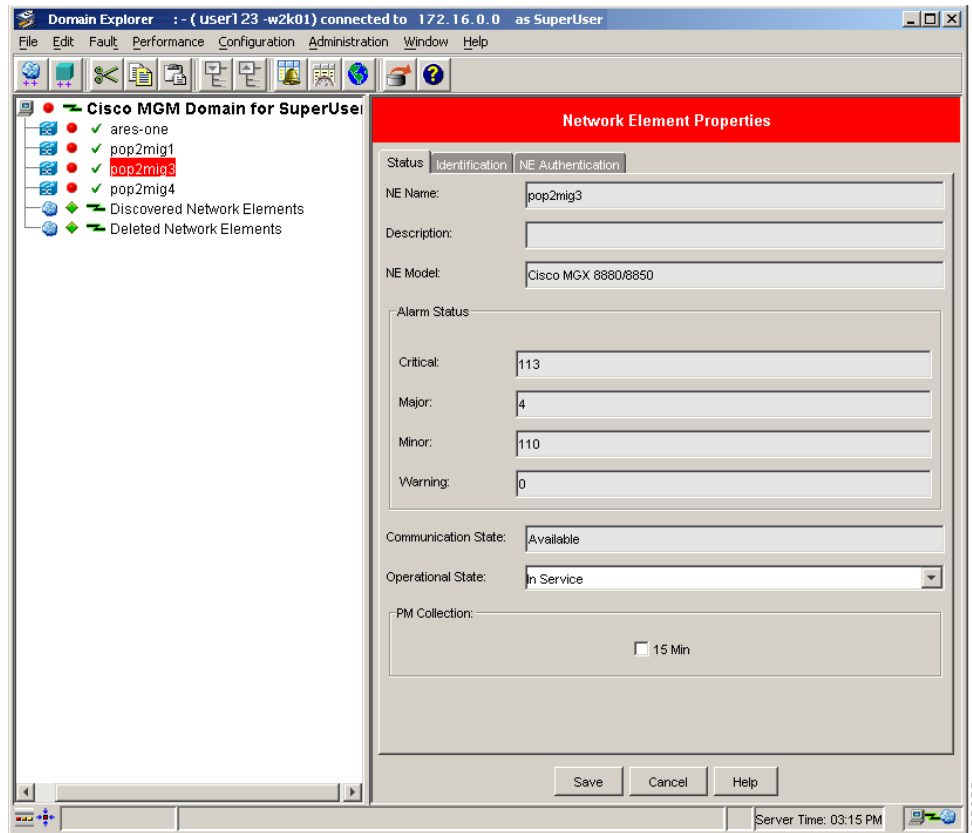
- CR—Critical
- MJ—Major
- MN—Minor
- WR—Warning
- UA—Total number of alarms unacknowledged

9.2.3 Domain Explorer

The Domain Explorer is the home window and provides a logical view of the network plus alarm, connectivity, and operational status. (See [Figure 9-2](#).) It is divided into two sections:

- Hierarchy pane—Consists of the different components, which appear in a hierarchical format. The top level of the hierarchy is the management domain, followed by groups, and then NEs. Groups and NEs may be repositioned in the hierarchy using either cut/paste or drag and drop operation. Groups and NEs can exist in multiple locations in the tree.
- Property sheet—Displays information about the component selected in the Hierarchy pane. There are three property sheets: Management Domain Properties, Group Properties, and Network Element Properties.

Figure 9-2 Domain Explorer



SuperUsers or Network Administrators use the Domain Explorer to create groups of NEs and to organize the domain in a hierarchy. By default, the Domain Explorer contains the following groups that are visible to SuperUsers and Network Administrators only:

- Discovered NEs—Contains NEs that have been automatically discovered by the server. Discovered NEs are added to the Discovered NEs group by default and then managed automatically. Refer to the “4.2.4 Network Element Discovery” section on page 4-7 for more information on discovery service.
- Deleted NEs—Contains NEs that have been deleted. An NE appears in this group only when the last instance of that NE has been deleted.
- Lost and Found—The client performs a minimal check at initialization to verify that the tree representation for the administrator’s domain is valid. If there are any mismatches between the groups and NEs in the domain and those in the administrator’s domain, the mismatched NEs or groups are shown in the Lost and Found group in the Domain Explorer Hierarchy pane. If the administrator moves the NEs or groups in the Lost and Found group to another group and then clicks **Refresh Data** or restarts the client, the Lost and Found group disappears.

**Note**

The Discovered NEs, Deleted NEs, or Lost and Found groups may not be deleted or renamed.

**Note**

The server time is displayed on the lower right side of the Domain Explorer.



Note

Clicking **Refresh Data** in the Domain Explorer window refreshes all data for the entire client and closes all open windows (except the Domain Explorer window). Depending on the number of NEs in the network, there might be some delay while the data refreshes. The status bar shows the status after the Domain Explorer refreshes. It will show “Refresh Data Complete.”

The Fault menu and associated toolbar tools are listed next to their corresponding menu options in [A.3.3 Fault Menu](#).

9.2.4 Alarm Browser

The Alarm Browser displays standing alarms and conditions in the managed domain that are assigned a severity level of critical, major, minor, or warning. It also shows cleared alarms that are not acknowledged. See [Figure 9-3](#). The Alarm Browser and Alarm Log views provide a robust listing of all current and historical alarms and events. See the “[9.9.1 Archiving Alarm Log](#)” section on page 9-50 for more information about the Alarm Log.

To display the Alarm Browser, select an NE, group, or domain node from the Domain Explorer, or Network Map; then, choose **Fault > Alarm Browser** (or click the Open Alarm Browser tool from the Dashboard). Use the toolbar buttons to manage the alarm display. These buttons are described in “[A.3.1 File Menu](#)” section on page A-7.

Figure 9-3 Alarm Browser

Id	PS	Ack	Note	Source ID	Probable Cause	Affected Object	Module Name	Physical Location	MGT
29913	CR			ares-one	Critical shelf aggregate alarm		MGX-MG NE	N/A	100%
29880	CR			ares-one	Secondary Card not present		MGX-MG Slot	Slot=31	100%
29879	CR			ares-one	Secondary Card not present		MGX-MG Slot	Slot=15	100%
29851	CR			MGM	Server Monitor Threshold Crossed	Memory Usage RAM	N/A	N/A	100%
29845	CR			pop2mig1	SVC Port, failed		MGX-MG Port	Slot=2:Bay=1:Line=1:P...	100%
29844	CR			pop2mig1	SVC Port, failed		MGX-MG Port	Slot=9:Bay=2:Line=2:P...	100%
29843	CR			pop2mig1	SVC Port, failed		MGX-MG Port	Slot=9:Bay=1:Line=5:P...	100%
29842	CR			pop2mig1	SVC Port, failed		MGX-MG Port	Slot=9:Bay=1:Line=4:P...	100%
29772	CR			pop2mig4	SVC Port, failed		MGX-MG Port	Slot=1:Bay=1:Line=1:P...	100%
29763	CR			pop2mig4	Receiving OOF		MGX-MG PATH	Slot=14:Bay=1:Line=1	100%
29762	CR			pop2mig4	Receiving AIS		MGX-MG PATH	Slot=14:Bay=1:Line=1	100%
29637	CR			pop2mig4	Path Signal Label mismatch		MGX-MG PATH	Slot=14:Bay=1:Line=1	100%
29635	CR			pop2mig4	Path Receiving STS AIS		MGX-MG PATH	Slot=14:Bay=1:Line=1	100%
29631	CR			pop2mig4	Receiving OOF		MGX-MG PATH	Slot=2:Bay=1:Line=2	100%
29630	CR			pop2mig4	Receiving AIS		MGX-MG PATH	Slot=2:Bay=1:Line=2	100%

Column Name	Value
Alarm ID	29913
Perceived Severity	Critical
Acknowledged	No
Note	
Source ID	ares-one
Probable Cause	Critical shelf aggregate alarm
Affected Object	

[Table 9-1](#) provides descriptions of the fields in the Alarm Browser.

Table 9-1 *Field Descriptions for the Alarm Browser Window*

Column Name	Description
Alarm ID	Indicates the unique number that the system uses to identify a particular alarm.
Perceived Severity	Displays the perceived severity of the selected alarm (critical, major, minor, or warning). The background color also indicates the severity, where: <ul style="list-style-type: none"> • Red = Critical • Orange = Major • Yellow = Minor • Cyan (blue-green) = Warning • Green = Cleared
Acknowledged	Indicates whether the selected alarm has been acknowledged by the user. Values are Yes and No.
Note	Displays any notes that were entered for the selected alarm. This field also shows the login name of the user who entered the note and the time when the note was entered.
Source ID	Displays the name of the network element where the selected alarm occurred.
Probable Cause	Displays the probable cause of the selected alarm. Displays Not Applicable/Unknown if no additional information is available.
Affected Object	Displays the name of the object where the selected alarm occurred.
Module Name	Displays the name of the module where the selected alarm occurred.
Physical Location	Displays the physical location of the equipment where the selected alarm occurred, such as slot, and port numbers.
Alarm Time Stamp	Displays the date and time when the alarm occurred on the server.
NE Alarm Time Stamp	Displays the date and time when the alarm occurred on the NE.
Service Affecting	Indicates whether the alarm condition is service affecting (SA); values are Yes and No.
Clear Time Stamp	Displays the date and time when the alarm was cleared on the server.
NE Clear Time Stamp	Displays the date and time when the alarm was cleared on the NE.
Acknowledged Time Stamp	Displays the date and time when the user acknowledged the selected alarm.
Acknowledged Username	Displays the login name of the user who acknowledged the selected alarm.
Alarm Status	Displays the status of the selected alarm (active or cleared).
Description	Displays additional information about the selected alarm. If there is no additional information, this field is blank.

9.2.5 Network Map

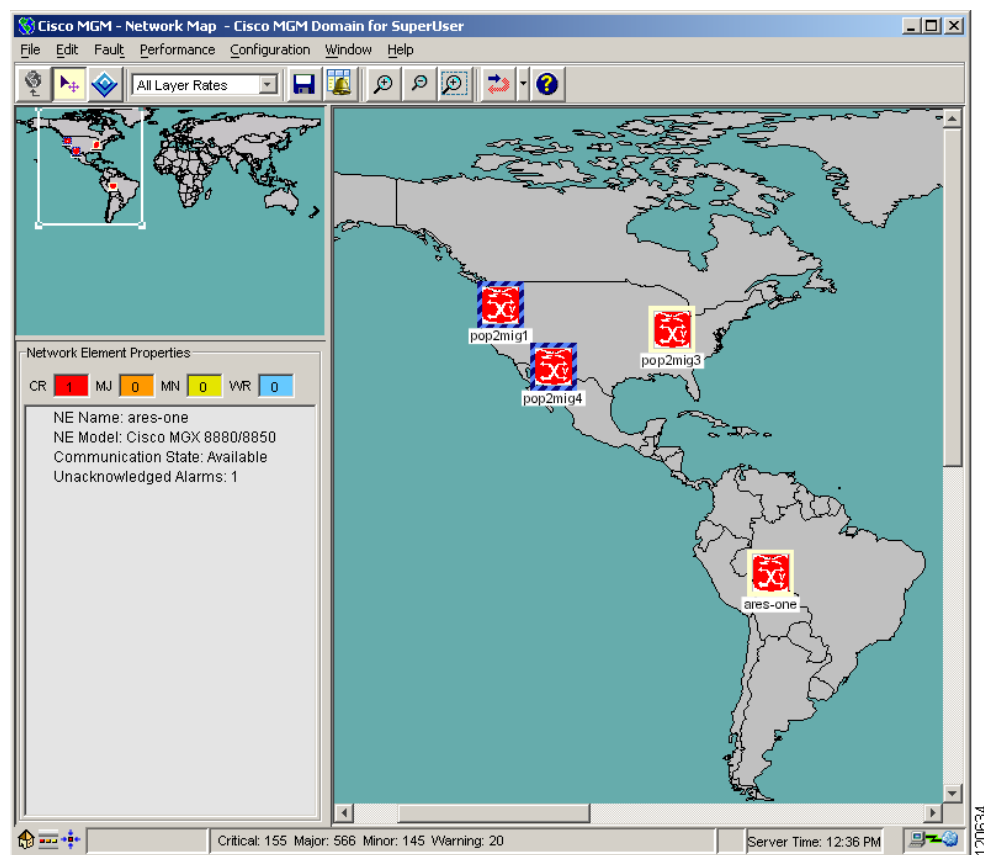
The Network Map window displays a geographical layout of the network. (See [Figure 9-4](#).) It consists of three areas:

- The right side displays a map with the individual groups and NEs icons.
- The upper left side displays the position of the map on the right side with respect to a larger world map.
- The lower left side displays the NE, or group properties, including the number of alarms and ID.

A Network Map window can be opened for an NE, group, or the domain. Select a node in the Domain Explorer Hierarchy pane and choose **File > Network Map** (or click the **Open Network Map** tool).

The Network Map is organized into a multilevel hierarchy that corresponds to the structure of the Domain Explorer when launched from the respective window. The Network Map hierarchy consists of management domains, groups, and NEs, that are represented by icons plotted automatically in a map. Zooming capabilities are provided and the node positions, node icons, and background map images can be customized.

Figure 9-4 Network Map



9.2.6 Diagnostic Center

The Diagnostic Center provides a hierarchical representation of network elements, which include networks, nodes, cards, lines and ports displayed in tree format in the Hierarchy pane of the Diagnostic Center's main window. Associated information about a selected network element is displayed in table format in the right panel of the Diagnostic Center window (See [Figure 9-5](#)).

Each network element managed by Cisco MGM has its own attributes and fits into the network's physical or logical hierarchy. The Diagnostic Center presents the network elements that are discovered, managed, and controlled in a hierarchical view for all networks populated in the tables by Cisco MGM processes.

The Diagnostic Center displays the network elements in a hierarchical format based on either a physical or logical relationship among the various network elements. Networks are displayed at the root level of the component tree; nodes are displayed beneath the networks in a parent/child relationship.

The Diagnostic Center also displays informational messages in a multiline text display; other types of messages can be displayed in response to user actions.

The Diagnostic Center can be opened for an NE, group, or the domain. Select a node in the Domain Explorer Hierarchy pane and choose **Fault > MGX8880/8850 MG > Diagnostic Center**.

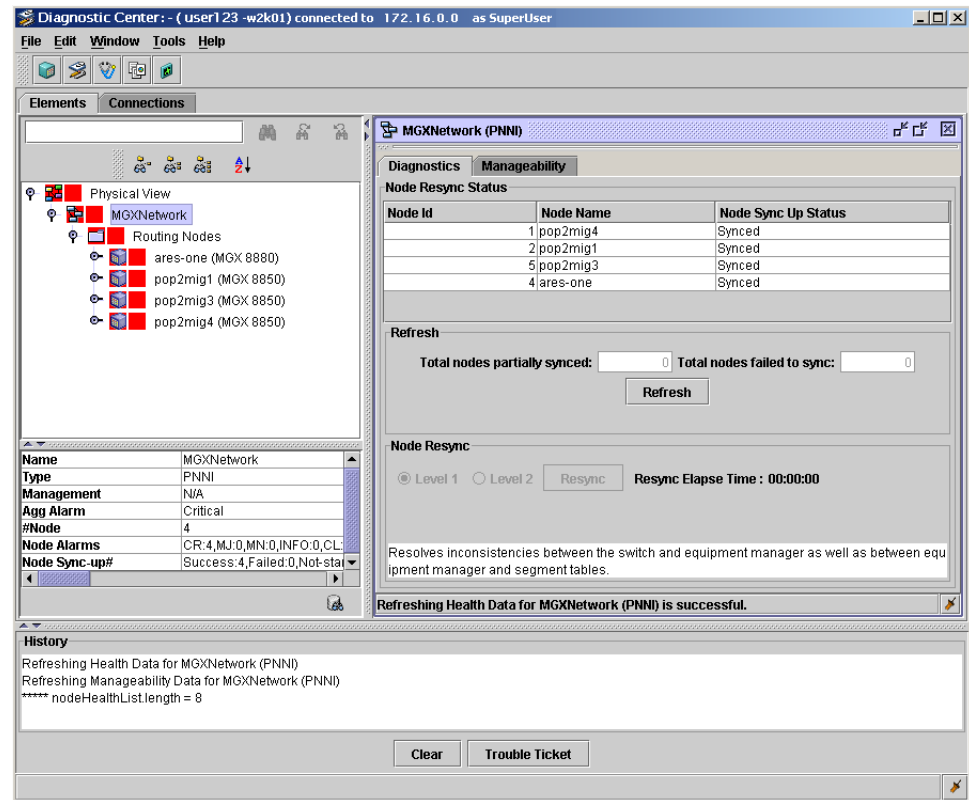
The Diagnostic Center has two access tabs:

- Diagnostic—Displays the diagnostic status and test results for the network elements.
- Manageability—Monitors the statistics events for network manageability

The Diagnostic Center allows users to:

- Diagnose network elements, for example, networks, nodes, cards, lines, ports, or paths. 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.
- 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.
- Diagnose connections to:
 - 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.

Figure 9-5 Diagnostic Center



9.3 What Fault Information Can I See?

An alarm is represented by a notification from a managed NE that a certain condition has just occurred. These alarms usually represent error conditions on NEs. Each alarm is associated with the NE for which it provides notification, and an NE can have a number of alarms related to itself at any time.

Each NE shown in the Domain Explorer Hierarchy pane has a corresponding alarm icon that indicates the highest severity alarm that affects the NE. Management domain nodes and group nodes have alarm icons that reflect the highest alarm condition of the NEs contained in the domain or group.

The user-defined Domain Explorer Network views have “bubble-up” alarm severity propagation and drill-down capabilities to isolate fault conditions and to identify service-delivery impact.

In Cisco MGM you can see:

- [9.3.1 How Are Alarms Displayed?](#)

There are occasions when it is useful to control the alarm display:

- [9.3.2 Suppressing Alarms](#)

9.3.1 How Are Alarms Displayed?

Each node displays an icon, which uses an industry-standard color scheme that indicates the current alarm status. The multicolor displays are updated in real-time in response to events occurring in the network. Icons representing network nodes change color dynamically to reflect the status of the node, which allows rapid recognition of network faults as they occur.

In the Diagnostic Center, Configuration Center, Chassis View, and Statistics Report, you can display the color legend for alarms, choose **Help > Color Legend**.

Table 9-2 lists the color legend for alarms.

Table 9-2 *Color Legend for Alarms for Diagnostic Center, Configuration Center, Chassis View, and Statistics Report*

Color	Alarm State
Green	Clear
Yellow	Minor
Orange	Major
Red	Critical
Grey	Unmanaged
Blue	Unknown
Purple	LineHasLoopback

You can set the Alarm Browser or Alarm Log to display full background color for the entire selected row. The color corresponds to the alarm status and severity. In the Domain Explorer window, choose **Edit > User Preferences**. The User Preferences dialog box appears. On the FM Preferences tab, check the **Color Entire Row in Table View** check box.

In the Dashboard, Map Viewer, Alarm Browser, and the Domain Explorer, the color of the border surrounding a component, or the background color, indicates the operational status of the component. When status changes, the border or the background color changes as indicated in Table 9-3.

Table 9-3 *Dashboard, Map Viewer, Alarm Browser, and Domain Explorer Alarm Severity Color Descriptions*

Color	Severity	Meaning	Description
Green	Cleared	Component is active.	The component is operating normally.
Yellow	Minor	Minor failure.	The component is down; both administrative and operational values are down. This does not necessarily indicate a fault condition; the component might be disabled.
Orange	Major	Component is down.	Administrative status is up and operational value is down.
Red	Critical	Component failed.	Physical hardware failure.
Cyan (blue-green)	Warning	Interface is dormant.	The interface cannot pass packets, but is in a pending state waiting for some external event to place it in the up state. The interface might have packets to transmit before establishing a connection to a remote system, or a remote system might be establishing a connection to the interface. When the pending event occurs, the interface changes to the up state.

9.3.2 Suppressing Alarms

Suppressing alarms prevents alarms from appearing on the Cisco MGX Alarm or History tab or on any other clients. Alarms are suppressed when the NE is under maintenance. See [5.3.1 Changing the Operational State of an NE](#).

9.4 Is the Service Working?

Network devices will report symptoms of problems by generating events. An event in this context is a message indicating that a device or application in your network has discovered something of note. The network devices will generate many types of events automatically.

In addition, you can use thresholds to define or modify the conditions under which events are generated. A *threshold* is a trigger, set up on a continuous data stream, that is a point of interest that generates events when that point is satisfied.

The events generated need to be analyzed to determine whether they represent a fault condition or problem in your network.

It is important to generate events when there is a problem in the EMS. It is also important to limit the number of events generated to prevent an excessive load on the network. The EMS performs a number of self-monitoring tasks where threshold limits can be set. The threshold limits are set in the Self Monitor Table. If one of these thresholds is crossed, then an EMS alarm will be generated.

The user can obtain information regarding how the system is performing and how long certain tasks are taking to complete by selecting **Administration > Control Panel** then **Alarm Configuration > Threshold EMS Alarms** or **Alarm Configuration > Non-Threshold EMS Alarms**. (See [9.4.3 Setting Up and Viewing Alarm Configuration Parameters](#).) By monitoring this data, you can identify potential system problems before they become critical in the operation of the EMS. Associated with each parameter that is monitored are three alarm thresholds. The administrator can set a minor, major, and critical threshold value for each parameter. If any of these thresholds are crossed, then an alarm will be raised to provide notification of the situation.

Threshold alarms are raised when their limit exceeds the value set for Critical, Major, Minor, or Warning thresholds. For example, you can set threshold alarms for disk usage for 90%, 80%, 70%, and 60%, meaning a warning alarm is raised when the disk becomes 61% full and a critical alarm is raised when the disk becomes 91% full. The server checks these parameters at every polling interval that is set in the Poll Frequency field.

Non-threshold alarms do not have an alarm threshold. Instead, non-threshold alarms occur when a condition occurs, such as loss of connectivity to an NE. Use the Non-Threshold EMS Alarms tab to set the severity level (critical, major, minor, or warning) for which a non-threshold alarm should be raised when that condition occurs.

**Caution**

Changing the EMS alarm severities can affect the alarm status seen by listeners on the EMS's OSS interfaces.

The following sections provide information on network elements:

- [9.4.1 Viewing Service Status](#)
- [9.4.2 Viewing Alarms](#)
- [9.4.3 Setting Up and Viewing Alarm Configuration Parameters](#)

These tasks are used to diagnose network elements with the Diagnostic Center:

- [9.4.4 Displaying the Status of all Nodes in the Network](#)
- [9.4.5 Displaying the Status of a Node](#)
- [9.4.6 Displaying the Status of a Card](#)
- [9.4.7 Displaying the Status for Lines or Ports](#)
- [9.4.8 Displaying the Status for Paths in a Loopback for the VXSM-OC3 Card](#)
- [9.4.9 Displaying the Status for Lines in a Loopback](#)

These tasks are used to diagnose the voice cards for both Voice Service Module (VXSM) and Voice Interworking Service Module (VISM-PR):

- [9.4.10 Displaying the Paths in Loopback for the VXSM-OC3 Card](#)
- [9.4.11 Displaying the Status for a Bit Error Rate Test for the Voice Cards](#)
- [9.4.12 Displaying the Lines in Loopback for the Voice Cards](#)
- [9.4.13 Managing the Status for the VXSM Features](#)
- [9.4.14 Managing the Status for the VISM-PR Features](#)

This task is used to diagnose connections:

- [9.4.15 Diagnosing Connections](#)

These tasks describe the Bit Error Rate Test (BERT) used to verify the integrity of a network element:

- [9.4.16 Bit Error Rate Test](#)
- [9.4.17 Configuring Bit Error Rate Test](#)
- [9.4.18 Displaying Bit Error Rate Test](#)

9.4.1 Viewing Service Status

You can monitor the different services that run on the server. To view service status, choose **Administration > Service Monitor** in the Domain Explorer window. The Service Monitor Table appears and displays the status of the services that are currently running on the server. The table displays the following information:

- Service Name—Name of the service
- Logged In At—Time that the user last logged in
- IP Address—IP address of the service
- Session ID—Unique session ID



Note

The **showmgm** command from the CLI is an alternate way of viewing processes or services that are currently running on the server.

9.4.2 Viewing Alarms

The Alarm Browser has a specific selection context, which means that it displays alarm information that corresponds to the view where it was launched. If you launch the Alarm Browser from the management domain node, the browser shows all NE alarms, and all 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 for that group, or NE node. If you launch the Alarm Browser from the Dashboard, the browser shows all NE alarms for the domain.

The Alarm Log window shows alarms that have transitioned from the Alarm Browser. Cleared alarms are transitioned when you acknowledge them or when automatic acknowledgment has been enabled. 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).

You can locate the equipment for an existing alarm in the Domain Explorer, choose **Fault > Alarm Browser** or **Fault > Alarm Log** (or click the Open Alarm Browser or Open Alarm Log tool).

9.4.3 Setting Up and Viewing Alarm Configuration Parameters

The Alarm Configuration property sheet allows you to configure alarm severities for system parameters. The Self Monitor Table displays information about threshold parameters. These parameters are collected and evaluated based on the NE model types. To set up and view alarm configuration parameters:

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
Click **Alarm Configuration** to open the Alarm Configuration property sheet. The Threshold EMS Alarms tab displays the information detailed in [Table 9-4](#):

Table 9-4 Alarm Configuration—Threshold EMS Alarms Tab

Field	Description
Poll Frequency	Displays the polling interval, in minutes, at which the Cisco MGM server checks parameters.
Parameter Name	<p>This column displays the name of the parameter as follows:</p> <ul style="list-style-type: none"> • CPU Usage (%): Percentage of CPU time utilized for executing user, system, and I/O tasks. • Config Resynch Time (seconds): Time it takes for Cisco MGM to collect alarm and inventory information from the NE. • Disk Usage (%): Percentage of disk space used in a particular partition. Cisco MGM database and partitions are monitored separately. • Memory Usage RAM (%): Percentage of RAM memory used for all processes of the system. • Memory Usage SWAP (%): Percentage of SWAP memory used for all processes of the system. • NE Synch Time (seconds): Time it takes to synchronize Cisco MGM server with the NEs. • PM Collection Time (seconds): Time it takes to collect PM data for an NE. It is the sum of the time it takes to read the PM data and the time it takes to update the database. • Prune Time Audit Log (seconds): Time it takes to prune audit log data. • Prune Time Audit Trail Log (seconds): Time it takes to prune audit trail log data. • Prune Time Error Log (seconds): Time it takes to prune Error Log data. • Prune Time FM (seconds): Time it takes to prune FM data. • Prune Time Job Monitor (seconds): Time it takes to prune job monitor data. • Prune Time PM (seconds): Time it takes to prune PM data. • Prune Time Purge NE (seconds): Time it takes to prune NE purge data. • Prune Time Server Monitor (seconds): Time it takes to prune server monitor data.
Enable	This column displays whether or not the corresponding parameter in the Parameter Name column is enabled (checked) or disabled (unchecked). When checked, it enables monitoring for the selected parameter. If an EMS threshold alarm is outstanding when you disable monitoring, the EMS clears the alarm.
Critical	This column displays the amount of time, in minutes, that must elapse before triggering a critical alarm.
Major	This column displays the amount of time, in minutes, that must elapse before triggering a major alarm.
Minor	This column displays the amount of time, in minutes, that must elapse before triggering a minor alarm.



Note If an alarm is outstanding when you disable it, the system clears the alarm.

Step 2 In the **Non-Threshold EMS Alarms** tab, you can select the severity level that will be assigned to the non-threshold alarm parameter. See [Table 9-5](#) for details.

Table 9-5 Alarm Configuration—Non-Threshold EMS Alarm Tab

Field	Description
Parameter Name	<p>The Parameter Name column displays the following parameters:</p> <ul style="list-style-type: none"> • Loss of Communication • Memory Auto or Manual Backup Failure • Maximum Login Attempts Exceeded • Alarm Resync Unsuccessful • Cisco MGM failed authentication by NE • A critical process is hanging, Cisco MGM will shut down in 5 minutes • Communication through Secondary IP Address • Sync-Up has not Started yet • Currently in Sync-Up • Partial Sync-Up • Sync-Up Failed • Server in Partial Sync-Up • Server Sync-Up Failed • FTP Transfer failure • FTP file size mismatch • FTP transfer failed • Upload File Error • Minus 2 Trap • Card Lost Trap • SNMP Retry exceeded • FTP Retry exceeded

Table 9-5 Alarm Configuration—Non-Threshold EMS Alarm Tab (continued)

Field	Description
Parameter Name (continued)	<ul style="list-style-type: none"> • Sync-up Failed • Stats File Error • Stats File Transfer Error • SNMP Throttle Error • Backoff failed • SNMP timeout • FTP Session timeout • FTP Transfer timeout • Unknown Error • Initialization Error • Configuration Error • Communication Error in ILOG • Communication Error in shared memory • Communication Error in CORBA • NTS Registration failed • NTS Trap loss • DataBroker Sync-Up Complete • Process Restarted • PM Fail EMS Alarm • PM Lost EMS Alarm
Severity	Allows you to click in the appropriate cell and select the alarm severity level from the available options (Critical, Major, Minor, or Warning) for each of the corresponding parameters listed in the Parameter Name column. If an EMS alarm is outstanding when you change its severity, the outstanding EMS alarm's severity remains the same. The next time the alarm is raised, the severity changes to the new setting.

Step 3 Click **Save**.

9.4.4 Displaying the Status of all Nodes in the Network

To display the status of all nodes in the network:

Step 1 In the Diagnostic Center, click the Elements tab, and double-click or drag the network to the right hand pane to display the diagnostics at the network level. By default, the **Diagnostics** tab is selected in the right hand pane.

- Step 2** The status of the following attributes at the network level are displayed:
- Node ID
 - Node Name
 - Current sync status of all the nodes of the network
 - All out-of-sync nodes in the network
 - A total of partially synced and failed synced nodes
-

9.4.5 Displaying the Status of a Node

To display the status of a node:

- Step 1** In Diagnostic Center, click the Elements tab, and double-click or drag the node to the right hand pane to display the diagnostics at the node level. By default, **Diagnostics** tab is selected in the right hand pane.
- Step 2** Verify the status of the following attributes at the node level:
- Current sync status of the node
 - All out-of-sync cards in the node
 - Node level statistics if applicable
-

9.4.6 Displaying the Status of a Card

Depending on the type of card, you can perform one or all of the functions from the following tabs:

- Paths in Loopback—Displays the paths in the loopback. (See [9.4.10 Displaying the Paths in Loopback for the VXSM-OC3 Card.](#))
- Lines in Loopback—Displays all lines that currently have loopback running. (See [9.4.12 Displaying the Lines in Loopback for the Voice Cards.](#))
- VXSM Features—Displays details of the Media Gateway Links, CIDs, RUDP Sessions, and XGCP MGC. (See [9.4.13 Managing the Status for the VXSM Features.](#))
- VISM-PR Features—Displays details of the XGCP Peers, SRCP Peers, and RUDP Sessions. (See [9.4.14 Managing the Status for the VISM-PR Features.](#))
- Running Berts—Display all lines that currently have a Bit Error Rate Test (BERT) running. (See [9.4.11 Displaying the Status for a Bit Error Rate Test for the Voice Cards.](#))

To display the status of a card:

- Step 1** In the Diagnostic Center, click the Elements tab, and double-click or drag the card from the Hierarchy pane to the right hand pane to display the diagnostics at the card level.
- Step 2** Verify the status of the attributes at the card level.
- Step 3** Click **Refresh** to update the Card Diagnostics window.
-

9.4.7 Displaying the Status for Lines or Ports

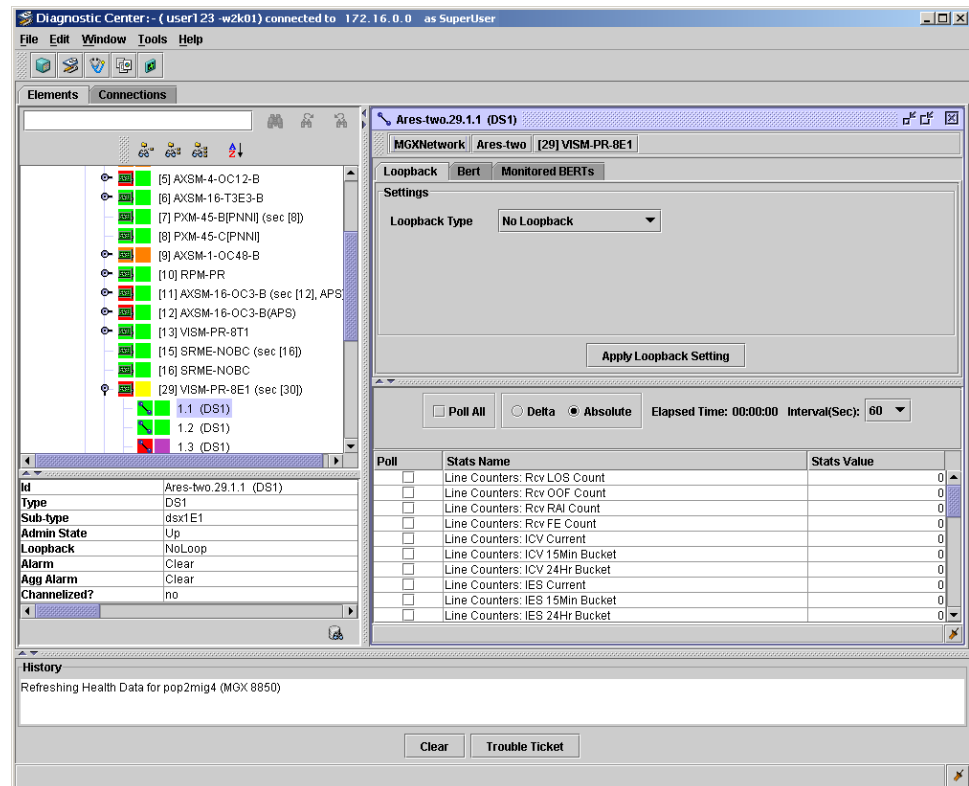
To display the status for lines or ports:

-
- Step 1** In the Diagnostic Center, click the Elements tab, and double-click or drag the line or port from the Hierarchy pane to the right hand pane to display the diagnostics at the line or port level. See [Figure 9-6](#). Depending upon the card type, you can also configure Bit Error Rate Test (BERT). For more information, see [9.4.17 Configuring Bit Error Rate Test](#). You can also see if a line is in loopback. See [9.4.9 Displaying the Status for Lines in a Loopback](#).
- Step 2** Click the **Delta Mode** radio button or **Absolute Mode** radio button. See [Table 9-6](#).
- Step 3** Choose the polling interval time from the **Poll Interval (Sec)** drop-down arrow.
- Step 4** Verify the statistics name and statistics value. [Appendix E, “Real-Time Counters”](#) gives details of the real-time counters displayed in the Diagnostic Center. [Appendix D, “Statistics Summary”](#) gives details of the statistics that are collected from the Cisco MGX 8880 and Cisco MGX 8850.
- Step 5** Check the **Poll All** check box to initiate polling for the statistics. To select individual counters for polling, check the counter check box.
-

Table 9-6 Diagnostic Center—Delta Mode and Absolute Mode Radio Buttons

Radio Button	Description
Delta Mode	Resets the counters and displays only the delta differences. Delta mode restarts the timer and takes the current values of the counters as base values, which are subtracted from the polled values for all the subsequent polls. The delta report is always the base values and the timer, which indicates the time lapsed since entering the delta mode. If you switch between delta to absolute mode, the timer is reset again.
Absolute Mode	(default) Provides the raw data shelved at the current counter state for the switch.

Figure 9-6 Diagnostic Center—Line Status



9.4.8 Displaying the Status for Paths in a Loopback for the VXSM-OC3 Card

To display the paths for a loopback for the VXSM-OC3 card:

- Step 1** In the Diagnostic Center, click the Elements tab, and double-click or drag the card from the Hierarchy pane to the right hand pane to display the diagnostics at the path level.
- Step 2** Click the **Paths In Loopback** tab.
- Step 3** Verify the following parameters for the path:
 - Path Id
 - Path Type
 - Loopback Type
- Step 4** Click **Refresh** to update the settings for the Path Diagnostics window.

9.4.9 Displaying the Status for Lines in a Loopback

To display the lines for a loopback:

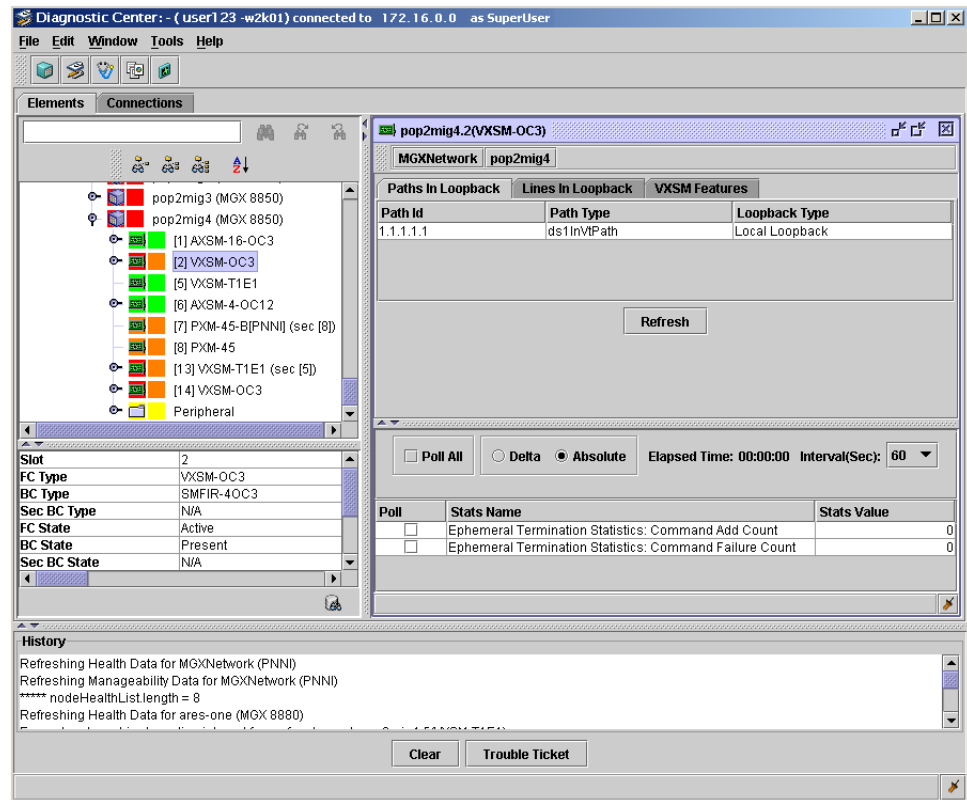
-
- Step 1** In the Diagnostic Center, click the Elements tab, and double-click or drag the card from the Hierarchy pane to the right hand pane to display the line in the loopback.
- Step 2** Click the **Lines In Loopback** tab.
- Step 3** Verify the following parameters for the line:
- Line Number
 - Loopback Type
- Step 4** Click **Refresh** to update the settings for the Line Diagnostics window.
-

9.4.10 Displaying the Paths in Loopback for the VXSM-OC3 Card

To display the paths in loopback for the VXSM-OC3 card for both SONET and SDH lines:

-
- Step 1** In the Diagnostic Center, click the Elements tab, and double-click or drag the VXSM-OC3 card from the Hierarchy pane to the right hand pane to display the diagnostics at the card level. See [Figure 9-7](#).
- Step 2** Click the **Paths In Loopback** tab.
- Step 3** Verify the following parameters for the path:
- Path Id
 - Path Type
 - Loopback Type
- Step 4** Click the **Delta Mode** radio button or **Absolute Mode** radio button. See [Table 9-6](#).
- Step 5** Choose the polling interval time from the **Poll Interval (Sec)** drop-down arrow.
- Step 6** Verify the statistics name and statistics value for the real-time counters.
- Step 7** Check the **Poll All** check box to initiate polling for the statistics. To select individual counters for polling, check the counter check box.
- Step 8** Click **Refresh** to update the settings for the paths in loopback for the VXSM-OC3 card for both SONET and SDH lines.
-

Figure 9-7 Diagnostic Center—Paths in Loopback



9.4.11 Displaying the Status for a Bit Error Rate Test for the Voice Cards

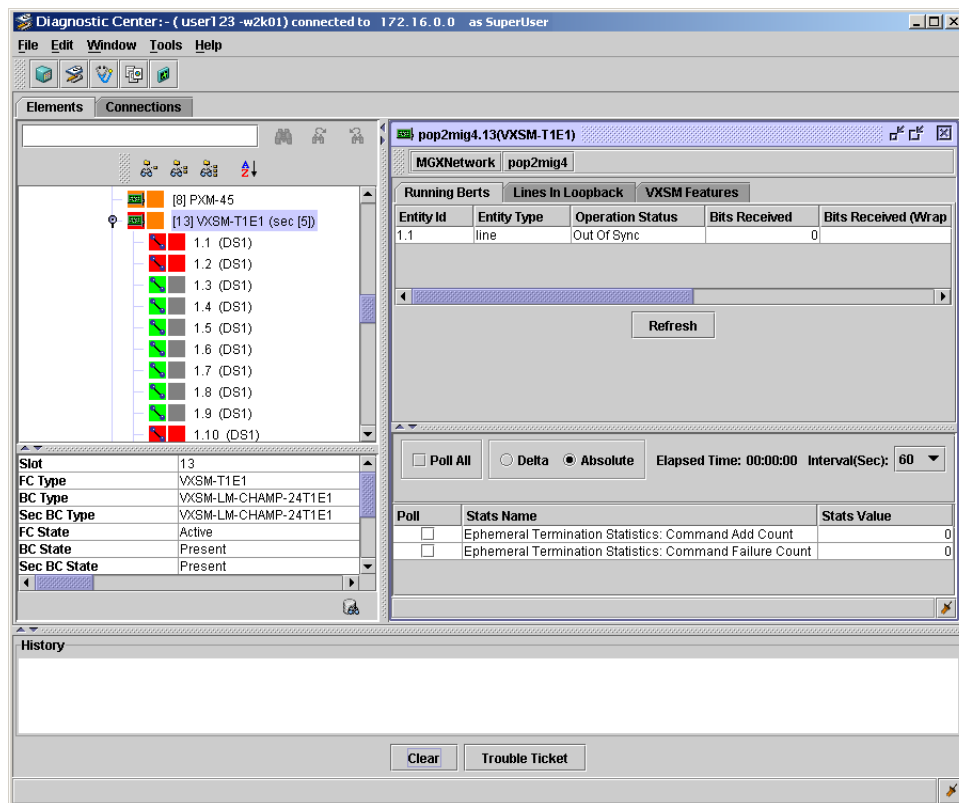
You can setup BERT options on the looped back connection and use the available test patterns displayed in the BERT Configuration window. See [9.4.17 Configuring Bit Error Rate Test](#)

To display the status for a BERT for the VXSM card for a T1E1 line and VISM-PR cards:

- Step 1** In the Diagnostic Center, click the Elements tab, and double-click or drag the VXSM-48T1E1 card or VISM-PR card from the Hierarchy pane to the right hand pane to display the diagnostics at the card level. See [Figure 9-8](#).
- Step 2** Click the **Running Berts** tab.
- Step 3** Verify the following parameters for the BERT test:
 - Entity Id
 - Entity Type
 - Operation Status
 - Bits Received
 - Bits Received (Wrap Count)
 - Bits Received In Error
 - Bits Received In Error (Wrap Count)

- Step 4** Click the **Delta Mode** radio button or **Absolute Mode** radio button. See [Table 9-6](#).
- Step 5** Choose the polling interval time from the **Poll Interval (Sec)** drop-down arrow.
- Step 6** Verify the statistics name and statistics value for the real-time counters.
- Step 7** Check the **Poll All** check box to initiate polling for the statistics. To select individual counters for polling, check the counter check box.
- Step 8** Click **Refresh** to update the settings for the lines in loopback for VXSM.

Figure 9-8 Diagnostic Center—Bit Error Rate Test



9.4.12 Displaying the Lines in Loopback for the Voice Cards

To display the lines in loopback for the VXSM card for both SONET and T1E1 lines and the VISM-PR cards:

- Step 1** In the Diagnostic Center, click the Elements tab, and double-click or drag the VXSM or VISM-PR card from the Hierarchy pane to the right hand pane to display the diagnostics at the card level. See [Figure 9-7](#).
- Step 2** Click the **Lines In Loopback** tab.

- Step 3** Verify the following parameters for the path:
- Line Number
 - Loopback Type
- Step 4** Click the **Delta Mode** radio button or **Absolute Mode** radio button. See [Table 9-6](#).
- Step 5** Choose the polling interval time from the **Poll Interval (Sec)** drop-down arrow.
- Step 6** Verify the statistics name and statistics value for the real-time counters.
- Step 7** Check the **Poll All** check box to initiate polling for the statistics. To select individual counters for polling, check the counter check box.
- Step 8** Click **Refresh** to update the settings for the lines in loopback for VXSM.
-

9.4.13 Managing the Status for the VXSM Features

These tasks are used to manage the status for the VXSM features:

- [9.4.13.1 Displaying the Status for Media Gateway Links for the Voice Cards](#)
- [9.4.13.2 Displaying the Status for Reliable User Datagram Protocol for the Voice Cards](#)
- [9.4.13.3 Displaying the Status for Xternal Gateway Control Protocol for the Voice Cards](#)

9.4.13.1 Displaying the Status for Media Gateway Links for the Voice Cards



Note

A session of the type of object must be available before it can be polled.

To display the Media Gateway Links (MGL) for voice cards for both SONET and T1E1 lines:

- Step 1** In the Diagnostic Center, click the Elements tab, and double-click or drag the VXSM card from the Hierarchy pane to the right hand pane to display the diagnostics at the card level.
- Step 2** Click the **VXSM Features** tab and choose **Media Gateway Links** from the drop-down box.
- Step 3** Verify the following parameters for the path:
- Gateway Link ID
 - Gateway IP Address
 - Gateway Port
 - Control Protocol
 - Gateway Link Operational State
- Step 4** Click the **Delta Mode** radio button or **Absolute Mode** radio button. See [Table 9-6](#).
- Step 5** Choose the polling interval time from the **Poll Interval (Sec)** drop-down arrow.

- Step 6** Verify the statistics name and statistics value for the real-time counters.
 - Step 7** Check the **Poll All** check box to initiate polling for the statistics. To select individual counters for polling, check the counter check box.
 - Step 8** Click **Refresh** to update the settings for the Media Gateway Links for VXSM.
-

9.4.13.2 Displaying the Status for Reliable User Datagram Protocol for the Voice Cards



Note

A session of the type of object must be available before it can be polled.

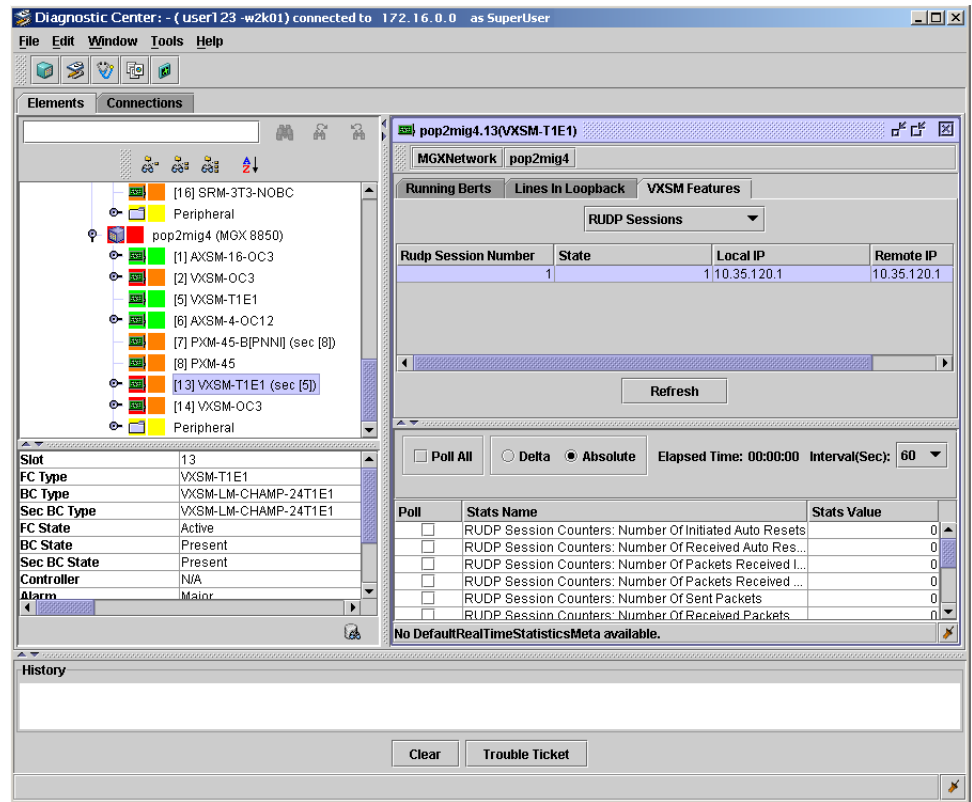
To display the Reliable User Datagram Protocol (RUDP) for VXSM card for both SONET and T1E1 lines:

- Step 1** In the Diagnostic Center, click the Elements tab, and double-click or drag the VXSM card from the Hierarchy pane to the right hand pane to display the diagnostics at the card level. See [Figure 9-9](#).
 - Step 2** Click the **VXSM Features** tab and choose the **RUDP Sessions** option from the drop-down arrow.
 - Step 3** Verify the following RUDP session parameters:
 - **RUDP Session Number**—Specifies the session group where the group belongs. One group has a maximum of four sessions. The range is from 1-64.
 - **State**—Specifies the following RUDP session states:
 - **oos**—Out of Service. When an RUDP session is created, the session state is **oos**.
 - **Is**—In Service. The state is changes to **Is** after the VXSM sent a start message to the MGC. The message is sent after a channel is created between the VXSM and the MGC.
 - **unknown**
 - **Local IP**—Specifies the IP address of the local VXSM.
 - **Remote IP**—Specifies the IP address of the remote VXSM.
 - Step 4** Click the **Delta Mode** radio button or **Absolute Mode** radio button. See [Table 9-6](#).
 - Step 5** Choose the polling interval time from the **Poll Interval (Sec)** drop-down arrow.
 - Step 6** Verify the statistics name and statistics value for the real-time counters.
 - Step 7** Check the **Poll All** check box to initiate polling for the statistics. To select individual counters for polling, check the counter check box.

[Appendix E, “Real-Time Counters”](#) gives details of the real-time counters displayed in the Diagnostic Center.

[Appendix D, “Statistics Summary”](#) gives details of the statistics that are collected from the Cisco MGX 8880 and Cisco MGX 8850.
 - Step 8** Click **Refresh** to update the settings for the RUDP sessions for VXSM.
-

Figure 9-9 Diagnostic Center—Reliable User Datagram Protocol for Voice Card



9.4.13.3 Displaying the Status for Xternal Gateway Control Protocol for the Voice Cards



Note A session of the type of object must be available before it can be polled.

To display the Xternal Gateway Control Protocol (XGCP) for VXSM card for both SONET and T1E1 lines:

- Step 1** In the Diagnostic Center, click the Elements tab, and double-click or drag the VXSM card from the Hierarchy pane to the right hand pane to display the diagnostics at the card level. See [Figure 9-9](#).
- Step 2** Click the **VXSM Features** tab.
- Step 3** Choose the **XGCP MGC** option from the drop-down arrow.
- Step 4** Verify the following XGCP peer group parameters:
 - **MGC Group Number**—Specifies the media gateway controller number. The range is from 1-8.
 - **Gateway IP Address**—The Gateway IP Address Index parameter defines the media gateway address that relates to the PVC control type. The range is from 1-16.
 - **Protocol Index**—Specifies the media gateway protocol number. The range is from 1-3.
 - **Gateway UDP Port**—Specifies the Gateway User Datagram Protocol (UDP) port.
- Step 5** Click the **Delta Mode** radio button or **Absolute Mode** radio button. See [Table 9-6](#).

- Step 6** Choose the polling interval time from the **Poll Interval (Sec)** drop-down arrow.
- Step 7** Verify the statistics name and statistics value for the real-time counters.
- Step 8** Check the **Poll All** check box to initiate polling for the statistics. To select individual counters for polling, check the counter check box.
- [Appendix E, “Real-Time Counters”](#) gives details of the real-time counters displayed in the Diagnostic Center.
- [Appendix D, “Statistics Summary”](#) gives details of the statistics that are collected from the Cisco MGX 8880 and Cisco MGX 8850.
- Step 9** Click **Refresh** to update the settings for the XGCP peer group for VISM-PR.
-

9.4.14 Managing the Status for the VISM-PR Features

This task is used to manage the status for the VISM-PR features:

- [9.4.14.1 Displaying the Status for the Simple Resource Coordination Protocol Peers](#)

9.4.14.1 Displaying the Status for the Simple Resource Coordination Protocol Peers

To display the status for the Simple Resource Coordination Protocol (SRCP) peer group for both VISM-PR cards:

-
- Step 1** In the Diagnostic Center, click the Elements tab, and double-click or drag the VISM-PR card from the Hierarchy pane to the right hand pane to display the diagnostics at the card level.
- Step 2** Click the **VISM Features** tab.
- Step 3** Choose the **SRCP Peers** option from the drop-down arrow.
- Step 4** Verify the following SRCP peer group parameters:
- **SRCP Peer Number**—Specifies the media gateway controller number. The range is from 1-8.
 - **SRCP Peer Name**—Specifies the name of the SRCP peer. The range is from 1-64 characters.
- Step 5** Click the **Delta Mode** radio button or **Absolute Mode** radio button. See [Table 9-6](#).
- Step 6** Choose the polling interval time from the **Poll Interval (Sec)** drop-down arrow.
- Step 7** Verify the statistics name and statistics value for the real-time counters.
- Step 8** Check the **Poll All** check box to initiate polling for the statistics. To select individual counters for polling, check the counter check box.
- Step 9** Click **Refresh** to update the settings for the SRCP peer group for VISM-PR.
-

9.4.15 Diagnosing Connections

The Diagnostic Center is used to diagnose connections. The key functions are the ability to test status, delay and integrity of SPVC connections.

This task is used to test SPVC connection:

- [9.4.15.1 Polling a Connection for an SPVC](#)

You can test the integrity of any existing connection that is nondisruptive to user traffic. The operation is similar to the **tstcon** command. For more information on the **tstcon** command, refer to the *Cisco WAN Switching Command Reference, Release 9.3.30*.

9.4.15.1 Polling a Connection for an SPVC

To poll a connection:

-
- Step 1** In the Domain Explorer, select the node and choose **Configuration > MGX8880/8850 MG > Configuration Center**.
 - Step 2** Click the **Connections** tab to display the Connection Browser window.
 - Step 3** Drag the node from the Hierarchy pane to the right hand pane to display the connection details. Click the **Connection List** tab. See [Figure 7-1](#).
 - Step 4** Click **More Filters** to display the Filter Settings window. See [Figure 7-2](#).
 - Step 5** Choose the filter settings from the Filter Settings window. For example, check both the **Status** check box and the **OK** check box if you want to retrieve only active connections.
 - Step 6** Click **OK** to apply the filter settings.
 - Step 7** Enter the number of connections that you want to retrieve in the **Connection Count to be retrieved** field. To retrieve all the connections, enter *.
 - Step 8** Click **Get** to retrieve the connections. For example, you can retrieve both local and remote endpoints. The Connection Browser window appears with the number of connections matching the filtering criteria. A list of connections that have either local or remote endpoints are displayed in the connection list.
 - Step 9** You now test the connection. Right-click the SPVC connection from the list of connections and choose **Diagnostic Center**.
 - Step 10** In the Diagnostic Center, click the **Test Connection** tab.
 - Step 11** There are three radio button options:
 - Click the **Test Conn** radio button to initiate an end-to-end integrity test of the selected connection.
 - Click the **Test Delay** radio button to initiate an end-to-end measurement of round-trip delay.
 - Step 12** Check the **Poll Local** or **Poll Remote Endpoint** check box to initiate polling for the statistics. To select individual counters for polling, check the counter check box.
 - Step 13** Click the **Delta Mode** radio button or **Absolute Mode** radio button. See [Table 9-6](#).
 - Step 14** Choose the polling interval time from the **Poll Interval (Sec)** drop-down arrow.

- Step 15** Verify the statistics name and statistics value for the real-time counters.
- Step 16** Click **Start Test Connection** to proceed with testing.
- Step 17** Click **Abort Test Connection** to stop the test.

9.4.16 Bit Error Rate Test

Bit Error Rate Test (BERT) verifies the integrity of a network element by measuring error statistics that result from sending known bit patterns, analyzing a remote interface, and analyzing the pattern that is returned. BERT is used on DS3, DS1, and DS0/DS0 bundle interfaces.

BERT generates a known data sequence into a transmission device, and examines the received sequence at the same device or a remote device for errors. Tests are run on a full T1E1 line or a fractional T1E1, for example, single DS0 or a group of DS0s. BERT tests the quality of links by directly comparing a pseudo-random or repetitive test pattern with an identical, local-generated test pattern.



Note

SRME, SRME/B, VXSM, VISM-PR, and AXSME card types support BERT.

BERT includes the following functions:

- Configures a local loopback on a line or port, or specifies a remote loopback be used instead.
- Defines the bit pattern.
- Specifies a duration for the BERT session after the session automatically terminates.
- Specifies BERT can start on a designated line or port.
- Lists BERT tests that are initiated from Cisco MGM.
- Refreshes the display to update the output for the current BERT.
- Stops a BERT started from Cisco MGM.

9.4.17 Configuring Bit Error Rate Test

You can setup BERT options on the looped back connection and use the available test patterns displayed in the BERT Configuration window. Before you configure the BERT options in the BERT Configuration window, make sure a line or port is selected from a BERT-supported service module.

In Cisco MGM, BERTs are only applicable on:

- AXSME 32 T1E1 (on DS1 Line)
- VXSM 48 T1E1 (on DS1 Line)
- VXSM OC3 (on DS1 Paths)
- VISM PR 8T1E1 (accompanied by an SRM Card, on DS1 Line)

This section also includes the following details:

- [9.4.17.1 Stopping Bit Error Rate Test](#)
- [9.4.17.2 Modifying Bit Error Rate Test](#)

To configure a BERT session:

Step 1 In the Diagnostic Center, double-click or drag the line or port that is supported by BERT from the Hierarchy pane to the right hand pane to display the Line and Port Configuration window.

Step 2 Click the **Bert** tab to display the BERT Configuration window. See [Figure 9-10](#).



Note Not all the BERT configuration parameters are applicable for all card types.

Step 3 Choose the test pattern options from the **Test Pattern** drop-down arrow.

The default option is **allZeros**.

Step 4 Choose one of the following Invert Rx Test options from the **Invert Rx Test Pattern** drop-down arrow:

- **Not Inverted**
- **Inverted**

Step 5 Choose one of the following Invert Tx Test options from the **Invert Tx Test Pattern** drop-down arrow:

- **Not Inverted**
- **Inverted**

Step 6 Ensure that the type of end device and loopback device option is correct from the **Device To Loop** drop-down arrow.

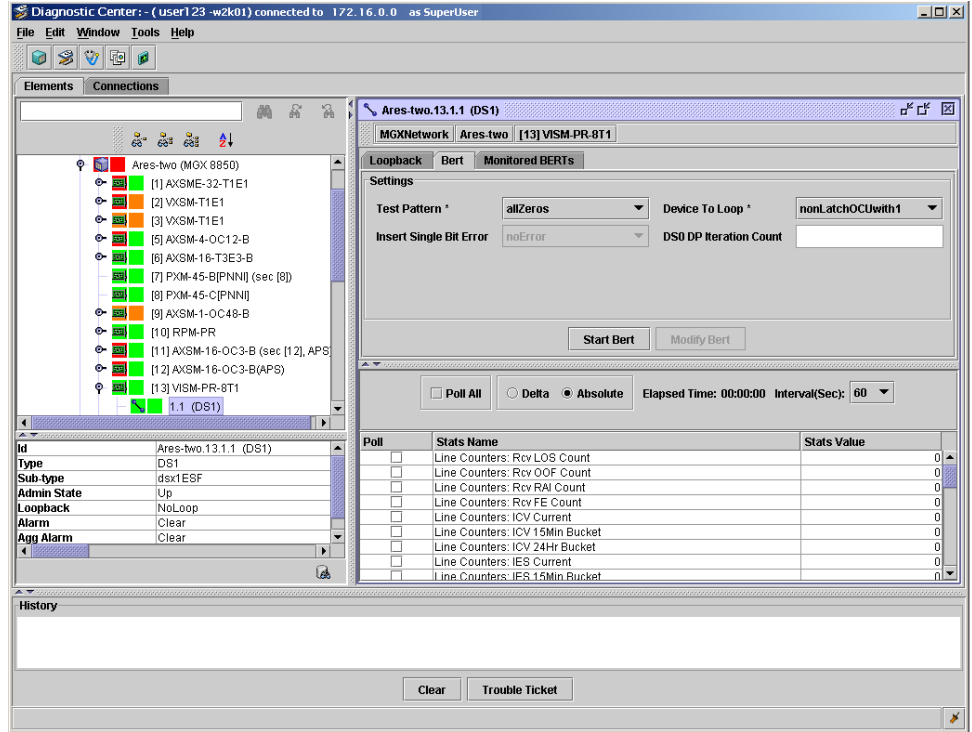
Step 7 Choose the error insertion option from the **Error Insertion** drop-down arrow.

The insert constant-rate error option verifies that the transmitted pattern is being properly received and errors are properly detected. Once set to send continuous errors, errors are inserted at the configured rate until set to **no Error** option.

If you set the value to insert errors while the test is not running, the test is not affected. However, when the test is started again, errors are inserted at the configured rate.

Step 8 Click **Start Bert** to initiate the BERT session. Note that once BERT is started, you can restart it with the modified options.

Figure 9-10 Diagnostic Center—BERT Options



9.4.17.1 Stopping Bit Error Rate Test

While the BERT session is running, you can stop the session from the BERT Configuration window that is applicable to your selected line or port. From the BERT Configuration window, click **Stop Bert** to stop the session.

9.4.17.2 Modifying Bit Error Rate Test

After you stop a BERT session, you can modify the session.

To modify a BERT:

-
- Step 1** Choose one of the following single-bit error options from the **Insert Single Bit Error** drop-down arrow:
- No Error
 - Insert Error
- Step 2** Click **Modify Bert** to modify the BERT line by inserting a single-bit error in the transmitted BERT pattern.
-

9.4.18 Displaying Bit Error Rate Test

After initiating a BERT session, you can view the status of all initiated BERT sessions at once. To display BERT status:

Step 1 In the Diagnostic Center, double-click or drag the line or port that is supported by BERT from the Hierarchy pane to the right hand pane to display the Line and Port Configuration window.

Step 2 Click the **Monitored BERTs** tab to display the Monitored BERTs window. See [Figure 9-10](#).

[Table 9-7](#) describes the parameters for the BERT statistics. Select the BERT entry to update the statistics, and click **Refresh**.

Table 9-7 Bit Error Rate Test Statistics Parameters

Name	Definition
Start Date and Time	Specifies the start date and time.
Operation Status	Specifies the current operation status of BERT.
Failed Reason	Defines the reason for the BERT failure. If the Operation Status parameter is set to BERT Failed, more information is available.
Bits Transmitted	Specifies the total number of bits.
Bits Received In Error	Receives the total number of bit errors.
Error Inject Count	Specifies the total number of injected bit errors.

9.5 Where Is the Fault?

You need to be able to quickly troubleshoot problems on the network, identify when network capacity is being reached, and provide information to management on the number and types of devices being used on the network. If the network goes down, one of the first things you will need to know is what devices are running on the network. You will want to know the types of devices you are dealing with as well as the names, addresses, and interfaces associated with each device in order to begin troubleshooting the problem. The more information you have about all your devices in one central place, the easier it is to locate necessary information, resolve problems quickly, and provide detailed information to interested parties.

[9.5.1 Sources of Information](#)

[9.5.2 Identifying and Monitoring Alarms](#)

[9.5.3 Using Visual and Audible Alarm Notifications](#)

[9.5.4 Sources of EMS Raised Alarms](#)

[9.5.5 Viewing Fault Management Data for a Set of NEs](#)

9.5.1 Sources of Information

Fault management receives and processes information from the following sources:

- Autonomous reports of failures from NEs
- Trouble reports from customers and peer systems
- Results of diagnostics, exercises and audits from NEs
- Impairment indications from performance management
- Network configuration data from configuration management.

Cisco MGM constantly updates the alarm status of the network based on the alarm and event notifications sent by the monitored NEs and generated by the EMS itself. It performs alarm synchronization with the NE each time the connection to the NE is established or re-established and the NE is in service.

9.5.2 Identifying and Monitoring Alarms

There are a number of options available to identify and monitor alarms on the entire domain or in a group of NEs:

- In the Domain Explorer Hierarchy pane, select the management domain node or a group node. If it shows a critical, major, minor, or warning alarm icon, it means that one or more NEs within the management domain or group are experiencing an alarm.
- Select the management domain node or group node and choose **Fault > Alarm Browser** (or right-click the node and choose **Alarm Browser** in the popup menu). This opens the Alarm Browser window, which shows all the NEs in the management domain or group that are experiencing a critical, major, minor, or warning alarm. See [Figure 9-3](#).
- Click an alarm count box in the Dashboard, the Alarm Browser appears, prefiltered for the selected alarm severity.
- Click the **Open Alarm Browser** tool from the Dashboard to show Cisco MGM specific EMS alarms in the Alarm Browser.
- Click the **Open Cisco MGM EMS Alarm Browser** tool from the Dashboard to show alarms on Cisco MGM in the Alarm Browser.

To identify and monitor alarms on specific NEs:

-
- Step 1** Select an in-service NE in the Domain Explorer Hierarchy pane that shows an alarm icon.
- Step 2** Choose **Fault > Alarm Browser**, or right-click and choose **Alarm Browser** in the popup menu.
-



Note Alarms relating to PM collection indicate that the load on the system is high. Reduce the load on the system before proceeding.

**Note**

No alarms or events will be generated in the Alarm Browser if Oracle shuts down.

9.5.3 Using Visual and Audible Alarm Notifications

To use visual and audible alarm notifications:

- Step 1** In the Domain Explorer window, choose **Edit > User Preferences**.
- Step 2** The User Preferences dialog box appears. On the Event Notification tab, in the Show Notification Dialog area, select whether or not an alert popup opens when a specific alarm or informational event occurs on NEs in the management domain or in the application.

The Event Notification dialog box opens whenever a new alarm or event occurs. According to your User Preferences selection, you will receive popup notification about alarms by severity and information on events from the network element (NE) or from Cisco MGM. The Event Notification popup remains open until one of the following occurs:

- You click OK to close the dialog box.
- It is replaced by an Event Notification dialog box with a higher severity.
- You click Disable to disable all event notifications.

The Event Notification displays the information shown in [Table 9-8](#).

- Step 3** In the Play Audible Notification area, select whether or not an audible alert is sounded when a specific alarm or informational event occurs on the NE or in the application. You can also select whether or not a continuous audible alert is sounded when there is an update in the Dashboard. Check the **Continuous Alarm for Dashboard notifications** check box.

**Note**

To stop the continuous audible alert, choose **Fault > Stop Continuous Beep** in the Domain Explorer.

- Step 4** Check the **Save current settings** check box and click **OK**.

**Tip**

Click **Disable** on the popup window itself to disable additional popups.

Table 9-8 *Event Notification Dialog Box Descriptions*

Field	Description
Source	Displays the name of the source where the alarm or event originated.
Time	Displays the date and time that you received the Event Notification popup.
Category	Indicates the category of alarm or event; alarm categories include Critical, Major, Minor, or Cleared. Event categories include NE Event (if the event occurred on a NE) or EMS Event (if the event occurred on Cisco MGM).
Probable Cause	Identifies the probable cause of the alarm or event.
Affected Object	Identifies the object that is affected by the alarm or event.

Table 9-8 Event Notification Dialog Box Descriptions (continued)

Field	Description
Description	Displays a brief description of the alarm or event.
Service Affecting	Indicates whether the alarm or event affects service.

9.5.4 Sources of EMS Raised Alarms

In addition to reporting NE-generated alarms, the EMS monitors and reports alarms on the EMS itself; for example, loss of connectivity to NE, and so forth.

The EMS monitors and reports the NE-specific alarms (see [Table 9-9](#)) and non-NE-specific alarms (see [Table 9-10](#)).

See [Appendix F, “Cisco MGM CORBA Gateway Events”](#) for details of the Cisco MGM CORBA Gateway events.

**Note**

NE-specific alarms can be viewed and accessed by users who are assigned to the particular NE.

Table 9-9 EMS-NE-Specific Alarms


NE-Specific Alarms	Description
Loss of communication to an NE	When the system detects loss of connectivity to an NE, an EMS alarm is generated in the Alarm Browser. This EMS alarm is cleared when the system reestablishes connectivity to the NE or when the NE is marked Out of Service.
Automatic or manual memory backup failure	If an automatic or manual memory backup job fails, an EMS alarm is generated in the Alarm Browser. An individual EMS alarm is generated for each memory backup failure that occurs. All instances of the backup-related EMS alarms are cleared (for that particular NE) when the memory backup succeeds or when the NE is marked Out of Service.
Switching IP addresses	When an active IP address switches from the primary to the secondary IP address, an alarm will be generated. It is only cleared when the address is switched back to the primary IP address or when communication to the NE is lost.
Failed PM data retrieval	An alarm will be generated for every PM data retrieval failure. PM 15-min Retrieval Fail Alarms are generated if the system has not retrieved 15-min PM data after the number of times to retrieve PM data has been reached. These alarms can be cleared manually or cleared automatically if a Lost PM alarm is generated or if PM data is retrieved.
Lost PM data	An alarm will be generated for all lost PM data. PM lost alarm 15-minute is generated when: <ul style="list-style-type: none"> The EMS is not able to collect PM data for 15 minutes and the NE’s PM collection is set to 15 Min. The EMS is not able to collect 15-minute PM data after 8 hours. If there are outstanding PM 15-min Retrieval Fail Alarms, these alarms will be cleared and the PM 15-min Lost PM Bucket Alarm is generated. <p>These alarms can be cleared manually. Lost PM data alarms are generated only if the PM collection is set to 15-Min.</p>

Table 9-10 Non-NE-Specific Alarms

Non-NE-Specific Alarms	Description
Maximum number of login attempts exceeded	By default, users have a maximum of five login attempts. The user account is locked after the fifth unsuccessful login attempt and an EMS alarm is generated in the Alarm Browser. The alarm is cleared once the user account is unlocked or the account is deleted.
System self-monitor alarm	<p>Threshold parameters such as CPU usage, memory usage, disk usage, circuit creation time, PM collection time, and resynch time are collected and evaluated to monitor the server performance.</p> <p>An alarm is generated if any of these parameters cross their threshold values with their corresponding severity level. The alarms are cleared only after the corresponding parameter value falls below the minor threshold. Subsequent threshold crossings for the same parameter will not generate further alarms. Only the severity level is changed to indicate the current severity level for the specific parameter.</p> <p>Note Alarms associated with circuit creation, configuration resynchronization, NE synchronization, and PM collection indicate that the load on the system is high. Reduce the load on the system before proceeding.</p> <p>Alarms associated with pruning times also indicate that the load on the system is high. Reschedule pruning at a time when the system has less activity.</p>

9.5.5 Viewing Fault Management Data for a Set of NEs

To view fault management data for an NE:

-
- Step 1** In the Domain Explorer Hierarchy pane, select the management domain, group, or NE node for which to view the data.
- Step 2** Open an Alarm Browser, choose **Fault > Alarm Browser**.
-  **Note** A preliminary filter is always applied based on the object selected in the tree view or map.
-
- Step 3** In the table, click the **Filter Data** tool (or choose **File > Filter**). The Filter dialog box appears.
- Step 4** Most fault management tables (for example, the Alarm Browser and Alarm Log tables) have a filter tool for filtering data for a set of NEs. In the Filter dialog box, select the NEs that will be included in the filter. Specify other filter parameters, as needed. See [9.7.2 Filtering the Alarm Log](#).
- Step 5** Click **OK** to show the results in a table.
-

9.6 How Can I Use Advanced Debugging to Find the Cause of the Fault?

Advanced debugging captures additional information about defects.

The EMS should correlate events and determine the faults that exist in the network. To correlate events means to look for relationships between them.

Advanced debugging can be carried out using information from the following sources:

- [9.6.1 Setting an EMS Process as Critical](#)
- [9.6.2 Setting Up and Viewing Error Logs](#)
- [9.6.3 Setting Debug Options](#)

9.6.1 Setting an EMS Process as Critical

You can mark an EMS service as critical for process monitoring purposes. To set a process as critical:

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
- Step 2** Click **Recovery Properties** to open the Recovery Properties sheet.
- Step 3** Click the Process Monitoring tab. [Table 9-11](#) describes the fields within the Process Monitoring tab. The system services listed are:
- Service Manager
 - Oracle Service
 - OS Agent
 - GateWay/CORBA Service
 - MGX8880/8850 NE Service
 - MGX8880/8850 PM Service
- Step 4** Check the Critical check box beside each service to indicate that the service is critical.



Note The Service Manager, Oracle Service, and OS Agent are permanently critical. You cannot uncheck the Critical check boxes for these services.



Note If a critical process stops running or it fails to poll monitoring services for a long time, the server will be shut down and the client will generate an alarm.

Table 9-11 Recovery Properties—Process Monitoring Tab

Field	Description
Service Name	Displays the process monitoring service name.
Critical	If checked, the selected service is designated as critical for process monitoring. Service Manager, Oracle Service, and OS Agent cannot be unchecked.

9.6.2 Setting Up and Viewing Error Logs

The Error Log tables display server error information that is useful for debugging Cisco MGM processes. In most cases, the Error Log is requested by service personnel for debugging a problem on the Cisco MGM server. The Error Log captures abnormal and significant events based on severity level. Critical, major, minor, and informational errors are saved in the database.

There are two types of Error Log available in Cisco MGM:

- Error logs for the Diagnostic Center, Configuration Center, Statistics Report and Chassis View. These Error Logs are accessed directly from the log directory on the server at `/opt/root/log`.
- Error logs for the other applications in Cisco MGM. Choose **Administration > Error Log** to view these Error Logs.




As the default, the Error Log displays information about significant events that occurred during the last four hours. You can change the default time period in the User Preferences dialog box.

The Error Log Configuration property sheet allows the user to control the volume of messages that are created by the server. All changes take effect immediately and do not require restart of the server. To reduce the amount of information logged to the database, turn off entire components. To set up and view Error Logs:

Step 1 In the Domain Explorer window, choose **Administration > Control Panel**.

Click **Error Log Properties** to open the Error Log Configuration property sheet. The Error Log property sheet displays the information in [Table 9-12](#):

Table 9-12 Field Descriptions for the Error Log Properties

Field	Description
Cisco MGM Server and GateWay/SNMP	<p>Allows you to choose the error level to include in the Error Log for services related to the Cisco MGM server and GateWay/SNMP. Critical, major, minor, and informational errors are logged to the database; trace and debug information is logged to a log file.</p> <p> Caution Cisco MGM performance will degrade significantly if the trace or debug option is left on. All operations will slow down and you may lose alarm and event notifications. Use trace or debug only when troubleshooting with a customer support engineer.</p> <p>Note Trace and debug information does not appear in the Error Log table.</p>
SM Service	<p>Allows you to choose the error level to include in the Error Log for the SM service. Critical, major, minor, and informational errors are logged to the database; trace and debug information is logged to a log file.</p> <p> Caution Cisco MGM performance will degrade significantly if the trace or debug option is left on. All operations will slow down and you may lose alarm and event notifications. Use trace or debug only when troubleshooting with a customer support engineer.</p> <p>Note Trace and debug information does not appear in the Error Log table.</p>
SNMP Trap Service	<p>Allows you to choose the error level to include in the Error Log for the SNMP Trap service. Critical, major, minor, and informational errors are logged to the database; trace and debug information is logged to a log file.</p> <p> Caution Cisco MGM performance will degrade significantly if the trace or debug option is left on. All operations will slow down and you may lose alarm and event notifications. Use trace or debug only when troubleshooting with a customer support engineer.</p> <p>Note Trace and debug information does not appear in the Error Log table.</p>

Step 2 In the Error Level field, choose the error level that will be included in the Error Log (Critical, Major, Minor, Informational, Debug, or Trace). Critical, major, minor, and informational errors are logged to the database; trace and debug information are logged to a log file.



Caution When the trace or debug option is left on, it can lead to an insufficient disk space situation. Use these options only when troubleshooting with a customer support engineer.

Step 3 Click **Save**.

To open the Error Log, choose **Administration > Error Log** in the Control Panel window menu bar. The Error Log displays the information shown in [Table 9-13](#).

Table 9-13 Error Log Descriptions

Column Name	Description
Cisco MGM Time Stamp	Displays the date and time when the error occurred on the Cisco MGM server.
Module	Displays the name of the module where the error occurred.
Severity	Displays the severity level of the error (see Table 9-15 for a description of the severity levels).
Submodule	Displays the name of the submodule where the error occurred.
Filename	Displays the name of the file where the error occurred. Cisco technical support engineers use this information for troubleshooting.
Line	Describes the exact line where the error occurred. Cisco technical support engineers use this information for troubleshooting.
Message	Displays the text of the error message.



Note Each NE service and PM service has an error level selection. For example, choose **Control Panel > NE Service** or **PM Service > MGX8850** or **MGX8880**. In the **Error Level** drop-down list, choose the error level to include in the Error Log for the selected NE service or PM service. Click **Save**.

Step 4 You can filter the Error Log data according to criteria that you select and to display the results in the Error Log table. [Table 9-14](#) details the options available:

Table 9-14 Error Log Filter Dialog Box Descriptions

Tab	Description
Time Stamp (time zone)	Allows you to filter Error Log data for a specified time period, ranging from the past hour to the past 6 months. You can click the User Specified radio button to specify an exact filter starting and ending time by month, day, year, and hour. The time zone can be Greenwich mean time (GMT), a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. If you want to filter Error Log data and the time period is not important, click No Time Specified .
Modules	Allows you to filter Error Log data by Cisco MGM module.
Submodules	Allows you to select Cisco MGM server submodules to filter Error Log data.
Severity	Allows you to filter Error Log data based on severity level: Critical, Major, Minor, and Informational.

The Error Log window shows Cisco MGM server error information that is useful for debugging purposes. The Error Log captures abnormal and significant events based on severity. [Table 9-15](#) shows the severity levels.

Table 9-15 Severity Levels and Error Log

Severity Level	Description
critical major minor informational	When set to any of these severity levels, all messages corresponding to critical, major, and minor severity levels are logged to the database and all informational messages are stored in the log file.
debug trace	When set to debug or trace, all informational and higher messages are logged to the database. All debug and trace messages are logged to the log files.

All messages are logged to the following files in the `/opt/CiscoMGMServer/log` directory:

- `MGMTL1FWDerror.log`
- `MGX8880NEService-number.log`
- `MGX8880NEService-numberError.log`
- `MGX8880PMService-number.log`
- `MGX8880PMService-numberError.log`
- `UnmanagedNEService-number.log`
- `UnmanagedNEService-numberError.log`
- `SnmpTrapService.log`
- `SnmpTrapServiceError.log`
- `CORBAGWService.log`
- `CORBAGWServiceError.log`



Note

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

After resetting the Error Log level to critical, major, minor, or informational, remove the log files to free disk space. Each time a new log file is started, a backup of the previous file is kept in the `log-file.bak` file. Remove the backup file at any time.

9.6.3 Setting Debug Options

In Cisco MGM, the debug option gives you information to investigate, diagnose and fix a problem.



Note

If required, set the debug levels for specific Cisco MGX NE backend processes by updating the debug parameter in the configuration file for that process in the `/opt/svplus/config` directory. See [Table 9-16](#). When the changes are made, stop, then restart the Cisco MGM server.

Table 9-16 Cisco MGM Processes and Configuration Files

Process	ConfigFile	Parameter	Range	Default
AuditLogger	AuditLogger.conf	DB_LEVEL	[1..5]	5
cmgrd	-none-	-none-		
cmsvr	cmsvr.conf	LOG_LEVEL	[1..7]	7
configserver	configserver.conf	LOG_LEVEL	[1..7]	7
cwmftpd	cwmftpd.conf	LOG_LEVEL	[1..7]	7
cwmsmap	-none-	-none-		
DCServer	DCServer.conf	LOG_LEVEL	[1..7]	7
dmd	dmd.conf	LOG_LEVEL	[1..7]	7
		SYNCUP_LOG_LEVEL	[1..7]	4
eventd	-none-	-none-		
ILMITopoc	ILMITopoc.conf	Debug Level	[1..5]	2
NMServer	NMServer.conf	LOG_LEVEL	[1..7]	7
		STARTUP_LOG_LEVEL	[1..7]	7
nts	nts.conf	DEBUG_LEVEL	[1..5]	5
oemc	emd.conf	OODebug Level	[1..7]	6
pmcollector	pmcollector.conf	LOG_LEVEL	[1..7]	7
RtmProxy	SNMPProxy.conf	-none-		
sdbroker	sdbroker.conf	LOG_LEVEL	[1..7]	7
		SYNCUP_LOG_LEVEL	[1..7]	4
snmpcomm	snmpcomm.conf	DEBUG_LEVEL	[1..5]	4
srtserver	srtserver.conf	LOG_LEVEL	[1..7]	7
statsparser	statsparser.conf	LOG_LEVEL	[1..7]	7
topod	Topod.conf	Debug Level	[1..5]	2

Specifying the debug options allows you to choose the parameters that will be displayed in the debug log.

To set the debug options:

-
- Step 1** In the Domain Explorer, choose **File > Debug Options**.
- Step 2** Specify the debug options. The options available in the Debug Options dialog box are described in [Table 9-17](#).
- Step 3** Click **Apply**.
-

Table 9-17 Field Descriptions for the Debug Options Dialog Box



Field	Subfield	Description
Modules	—	Select modules that will display debug messages. Use the Add and Remove buttons to move modules to the Selected list or remove modules from the list.
Debug Level	Fatal	Instructs the Debug Log to display messages with a severity level of at least Fatal.
	Warning	Instructs the Debug Log to display messages with a severity level of at least Warning.
	Info	Instructs the Debug Log to display messages with a severity level of at least Info.
	Debug	Instructs the Debug Log to display messages with a severity level of at least Debug.  Caution Cisco MGM performance will degrade significantly if the Debug option is left on. All operations will slow down and you may lose alarm and event notifications. Use Debug only when troubleshooting with a Cisco customer support engineer.
Trace		Instructs the Debug Log to display messages with a severity level of at least Trace.
		 Caution Cisco MGM performance will degrade significantly if the Trace option is left on. All operations will slow down and you may lose alarm and event notifications. Use Trace only when troubleshooting with a Cisco customer support engineer.

Table 9-17 Field Descriptions for the Debug Options Dialog Box (continued)

Field	Subfield	Description
Display Options	File	<p>Check the File check box to write the Debug Log to a specific file. You can click Browse to browse for a local client directory for the Debug Log. After you specify the filename, the log is stored at <code><filename>0.log</code> and <code><filename>1.log</code> when <code><filename>0.log</code> is filled to its maximum size.</p> <p>By default, the Debug Log is saved at <code>C:\Cisco\MediaGatewayManagerClient<version_number>\debug\MGMC-debug0.log</code> or <code>/opt/CiscoMGMClient<version_number>/debug/MGMC-debug0.log</code>. The dialog box shows the filename without the number 0 or 1, which is appended by default by the Java debugging APIs.</p> <p>Note <code><version_number></code> is replaced by the version number of the installed Cisco MGM client.</p>
	Max File Size	Enter the maximum file size for the Debug Log, in bytes.
	Telnet	<p>Check the Telnet check box to write the Debug Log to a Telnet port.</p> <p>Note Telnet to the IP address of the Cisco MGM client workstation, not the Cisco MGM server.</p>
	Console	Check the Console check box to write the Debug Log to the console.

9.7 What Is the Fault Priority?

After you have gathered information about the faults, it is then important to prioritize that information. There are several ways to determine the priority of a fault. You can simply assign a priority to an NE or group, or you can try to derive this information from a knowledge of the network.

The priority of a fault can vary depending on a variety of factors, such as:

- Influences outside of the network (for example, the time of day an outage occurs)
- Amount and type of traffic that will be affected
- Who specifically is affected by the fault
- Potential financial consequences

You can decide to filter events. Filtering means to identify events that do not need to be processed immediately, or might never need to be processed. Because the volume of events to be processed can be high, it is important to filter unwanted events as soon as possible.

You can get information for prioritizing faults in the following sections:

- [9.7.1 Alarm Severity Levels](#)
- [9.7.2 Filtering the Alarm Log](#)
- [9.7.3 Filtering Data by Time](#)

9.7.1 Alarm Severity Levels

Cisco MGM supports the following alarm severities in the Alarm Browser:

- Critical (CR)—Red
- Major (MJ)—Orange
- Minor (MN)—Yellow
- Warning (WR)—Cyan (blue-green)

9.7.2 Filtering the Alarm Log

By default, the Alarm Log shows alarm and event information that occurred during the last 4 hours. Use the drop-down menu to the right of the time-based filter tool to filter event data for the past 4 hours, past 8 hours, past 12 hours, past day, or past week.

-
- Step 1** In the Domain Explorer Hierarchy pane, select a domain, group, or NE and choose **Fault > Alarm Log**.
- Step 2** To set the filter time to start immediately, choose **Fault > Reset All Events**.
To filter the data in the log, click the **Filter Data** tool (or choose **File > Filter**). The Alarm Log Filter dialog box contains the information detailed in [Table 9-18](#).
- Step 3** When all filter criteria have been specified, click **OK** to run the filter.
-

Table 9-18 Field Descriptions for the Alarm Log Filter Dialog Box

Tab	Description
Cisco MGM Time Stamp (time zone)	Allows you to filter alarm and event data for a specified time period, ranging from the past hour to the past 6 months. Additionally, you can click the User Specified radio button to specify an exact filter starting and ending time by month, day, year, and hour. The time zone can be Greenwich mean time (GMT), a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. If you want to filter alarms and events and the time period is not important, click No Time Specified . Click From Now Onward to set the filter time to start immediately and continue until you change filter parameters.
Source ID	Allows you to move network elements (NEs) back and forth between the list of Available Source IDs and Selected Source IDs and then run the Alarm Log Filter. If you have the appropriate user permission, you can filter Cisco MGM EMS alarms and events by selecting MGM and adding it to the Selected Source ID list. If more than 100 NEs are selected, the Source ID tab becomes gray and all devices are included in the filter criteria you specify.
Module Name	Allows you to specify which module types you want to include in the filter. The modules displayed depend on the NE selection in the Domain Explorer Hierarchy pane when the Alarm Log is opened. Use the Add and Remove buttons to filter the display to specific modules. The Alarm Log displays events for modules listed under Selected Module Name.

Table 9-18 Field Descriptions for the Alarm Log Filter Dialog Box (continued)

Tab	Description
Affected Object	Allows you to specify which objects you want to include in the filter. The objects displayed depend on the NE selection in the Domain Explorer Hierarchy pane when the Alarm Log is opened. Use the Add and Remove buttons to filter the display to specific objects. The Alarm Log displays events for entities listed under Selected Affected Object. To filter NE-specific EMS alarms, select MGM and add it to the Selected Affected Object list.
PS	Allows you to filter data based on the perceived severity (PS) of the alarm or event. Additionally, you can filter service affecting alarms and events, non-service affecting alarms and events, and/or not-available alarms and events (alarms and events where the service affecting status is not known).
Physical Location	Allows you to filter data based on the physical location of an NE or its components. To view the tab, an NE must be selected in the Domain Explorer Hierarchy pane. The filters that are available depend on the NE selected.
ID	Allows you to filter data based on alarm or event ID. Enter a starting ID and an ending ID; then, run the filter to see only the alarms or events that occurred within the specified range of IDs. Check the Disregard All The Other Filter Criteria check box to ignore all other filter specifications. In addition, you can filter the view to only alarms, only events, or both alarms and events.
NE Alarm Time (time zone)	Allows you to filter alarm data for a specified time period, ranging from the past hour to the past 6 months. Additionally, you can click the User Specified radio button to specify an exact filter starting and ending time by month, day, year, and hour. The time zone can be Greenwich mean time (GMT), a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. If you want to filter alarms and the time period is not important, click No Time Specified . Click From Now Onward to set the filter time to start immediately and continue until you change filter parameters.

9.7.3 Filtering Data by Time

Most fault management tables (for example, the Alarm Browser and Alarm Log tables) have a filter tool for filtering data for a set of NEs. A preliminary filter is always applied based on the object selected in the tree view or map.

To filter data by time:

-
- Step 1** In the Domain Explorer Hierarchy pane, select the node for which to filter time-based fault management data. Choose **Fault > Alarm Browser**.
 - Step 2** In the Alarm Browser, click the **Filter Data** tool (or choose **File > Filter**). The Filter dialog box appears.

- Step 3** In the Filter dialog box, click the **NE Alarm Time** tab. Click one of the following radio buttons:
- **Past Hour to Past Month**—Filters data for a specified time period, ranging from the past hour to the past month.
 - **From Now Onward**—Sets the filter time to start immediately and continue until filter parameters are changed.
 - **No Time Specified**—Filters data without specifying a time period.
 - **User Specified**—Allows you to specify an exact filter starting and ending time by month, day, year, and hour. The time zone can be local time, GMT, or an offset from GMT, depending on what is specified in the User Preferences dialog box.
- Step 4** Click **OK** to show the results in the table.

**Note**

Clicking Refresh Data resets the time-based filter. The filter retrieves data for the specified interval, beginning when the Refresh Data tool is clicked. For example, if the specified interval is Past Hour and Refresh Data is clicked at 3:02 P.M., the filter retrieves data that occurred between 2:02 P.M. and 3:02 P.M. If the specified interval is From Now Onward at 8:00 P.M., data is retrieved beginning at 8:00 P.M. and the time is reset only after From Now Onward is clicked again.

9.8 Who Is Responsible for Managing the Fault?

To manage faults effectively, you must know who is taking responsibility for managing each case. Cisco MGM offers the following options:

- [9.8.1 Configuring Alarm Acknowledgement and Alarm Notes](#)
- [9.8.2 Acknowledging and Unacknowledging Alarms](#)

9.8.1 Configuring Alarm Acknowledgement and Alarm Notes

To configure alarm acknowledgment, and enable or disable the alarm note feature:

- Step 1** In the Domain Explorer window, choose **Administration > Control Panel** and click **UI Properties**.
- Step 2** Under fault management, select either Manual or Automatic Alarm Acknowledgement.
- If you choose **Manual Alarm Acknowledgment**, alarms must be acknowledged manually. Cleared alarms move from the Alarm Browser to the Alarm Log once they are acknowledged.
 - If you choose **Automatic Alarm Acknowledgment**, the server automatically acknowledges alarms when they are cleared and moves them from the Alarm Browser to the Alarm Log.



Note Active alarms are not automatically acknowledged.

If the alarms are initially set to Manual Alarm Acknowledgement, and then you switch to Automatic Alarm Acknowledgement, all the alarms in the Alarm Browser will be cleared and acknowledged automatically. This might take a while, depending on the number of alarms in the database that have not been acknowledged manually.

You can still acknowledge alarms manually even if Automatic Alarm Acknowledgment is set.

- Step 3** Use the Overwrite Alarm Notes option to enable or disable the ability to overwrite alarm notes created by another user.
- Step 4** Select either Enable or Disable Alarm Un-Acknowledgement.
- If you choose **Enable Alarm Un-Acknowledgement**, you can unacknowledge alarms in the Alarm Browser.
 - If you choose **Disable Alarm Un-Acknowledgment**, alarms can only be acknowledged in the Alarm Browser.
- Step 5** Click **Save**.

9.8.2 Acknowledging and Unacknowledging Alarms

If you enable automatic alarm acknowledgment in the Control Panel > User Interface Properties sheet, the server automatically acknowledges alarms when they are cleared and transitions the alarms to the Alarm Log. If you enable manual alarm acknowledgment, you manually acknowledge a cleared alarm; then, the alarm transitions to the Alarm Log.

The alarm acknowledgement feature acknowledges selected alarms or all alarms with a single click. See [Appendix A, “Icons and Menus”](#) for more information about alarm acknowledgment tools.

To acknowledge or unacknowledge alarms:

- Step 1** In the Domain Explorer window, select an NE and choose **Fault > Alarm Browser**. This opens the Alarm Browser window for the selected NE.
- The Alarm Browser window lists critical, major, minor, and warning alarms that have not been cleared or cleared alarms that have not been acknowledged.
- Step 2** Select the alarms to be acknowledged and choose **Fault > Acknowledge Alarms** (or click the **Acknowledge Selected Alarm(s)** tool). Click **Yes** in the confirmation dialog box. Click the **Refresh Data** tool to see the changes. A check mark icon provides a visual indication of acknowledged alarms.
- When cleared alarms are acknowledged, they transition from the Alarm Browser to the Alarm Log. For more information about the Alarm Log, see the [“9.9.1 Archiving Alarm Log”](#) section on page 9-50.

Step 3 Click the **Acknowledge Selected Alarm(s)** tool again to unacknowledge the selected alarms. Click **Yes** in the confirmation dialog box. Click **Refresh Data** to see the changes. The check mark will be removed, indicating that the alarm has been unacknowledged.



Note Alarm unacknowledgement is disabled by default. Make sure to enable the alarm unacknowledgement feature in the Control Panel before unacknowledging an alarm. See the “[9.8.1 Configuring Alarm Acknowledgement and Alarm Notes](#)” section on page 9-48 for more information.

Step 4 To acknowledge all alarms in the view, choose **Fault > Acknowledge All Alarms** (or click the **Acknowledge All Alarms** tool). Click **Yes** in the confirmation dialog box.

Choose **Fault > Show Alarm Note** (or click the **Show Alarm Note** tool) to read any comments that have been entered for the selected alarm and to enter additional comments. You can add comments to the previous comments, click the **Append** radio button. To overwrite the previous comments, click **Replace**. To delete the comments, click **Delete**.



Note You can enable and disable the Replace and Delete functions in the **Control Panel > User Interface Properties** sheet.

9.9 How Did You Manage the Fault?

Alarm information can be useful to evaluate the actions taken, for a number of reasons:

- How sure are you that the problem cannot recur?
- What other devices need the same fix?
- Do you know the root cause of the problem?
- What can you do to prevent this problem from reoccurring?
- What new problems could occur when you apply this fix?

In Cisco MGM, you can get information to make this assessment by doing the following:

- [9.9.1 Archiving Alarm Log](#)
- [9.9.2 Exporting Alarms and Events to a Text File](#)

9.9.1 Archiving Alarm Log

The Alarm Log window contains alarms that have transitioned from the Alarm Browser. In order for an alarm to transition from the Alarm Browser to the Alarm Log, it must be cleared and acknowledged. In addition, the Alarm Log shows all transient conditions (also known as events). Events have a single possible severity of Indeterminate and do not have associated clear messages. Events are placed directly into the Alarm Log. They do not appear in the Alarm Browser.

By default, the Alarm Log shows alarm and event information that occurred during the last 4 hours. To view the Alarm Log:

- Step 1** In the Domain Explorer Hierarchy pane, select a domain, group, or NE.
- Step 2** Choose **Fault > Alarm Log**. The Alarm Log appears and displays the information detailed in [Table 9-19](#).

Table 9-19 *Field Descriptions for the Alarm Log Window*

Field	Description
ID	Unique number that the system uses to identify a particular alarm or event.
Source ID	NE or EMS where the selected alarm or event occurred.
Affected Object	Object where the selected alarm or event occurred. For NE-specific alarms, the affected object fields will display “MGM”. For the non-NE specific alarms: <ul style="list-style-type: none"> • Maximum number of login attempts exceeded alarm—The affected object field displays the user ID associated with the alarm. • Cisco MGM self monitor alarm—The affected object field displays the threshold parameter associated with the alarm.
Module Name	Name of the module where the selected alarm or event occurred.
Physical Location	Physical location of the equipment where the selected alarm or event occurred.
Probable Cause	Probable cause of the selected alarm or event.
PS	Perceived severity of the alarm before it was cleared. Severity can be Critical, Major, Minor, Warning, or Indeterminate. The background color of the column indicates the alarm status. A green background indicates that the alarm is cleared.
SA	Indicates whether the alarm or event is service affecting. Values are: <ul style="list-style-type: none"> • Yes if its service affecting • No if its not service affecting • N/A if no information is provided by the NE
MGM Time Stamp (GMT)	Date and time when the alarm or event occurred on the server.
MGM Clear Time	Date and time when the alarm was cleared on the server.
MGM Duration	Amount of time required to clear an alarm (MGM Clear Time Stamp – MGM Time Stamp) in dddd:hh:mm:ss format.
NE Time Stamp	Date and time when the alarm or event occurred on the NE.
NE Clear Time	Date and time when the alarm or event was cleared on the NE.
Description	Brief description of the selected alarm or event. If no description is entered, this field is blank.

Table 9-19 Field Descriptions for the Alarm Log Window (continued)

Field	Description
Acknowledged Username	Login name of the user who acknowledged the alarm or event. Note MGM is the username registered for alarms that are automatically acknowledged. Automatic acknowledgement does not overwrite the username of manually acknowledged alarms.
Acknowledged Time	Date and time when the alarm or event was acknowledged. Note If the alarm acknowledgement is set to Automatic and you can manually acknowledge an alarm, the Acknowledged Time is not overwritten when the alarm clears.
Note	Any notes that were entered for the selected alarm or event. This field also shows the login name of the user who entered the note and the time stamp when the note was entered.

9.9.2 Exporting Alarms and Events to a Text File

Use the Event Export Manager to export alarms and events to a text file as they occur. In addition, you can use the Event Export Manager to set various export parameters to refine the export.

-
- Step 1** In the Domain Explorer window, choose **Fault > Event Export Manager**.
 - Step 2** The Event Export Manager appears. In the Available Network Elements list, select the NEs that you want to export and click **Add**. In the Selected Network Elements list, select the NEs that you do not want to export and click **Remove**.
 - Step 3** To export Cisco MGM-specific alarms and events, check the **Export Cisco MGM EMS Alarms/Events** check box.
 - Step 4** In the Severity area, check the **Critical, Major, Minor, Warning, Indeterminate**, and/or **Cleared** check boxes. Alarms and events with a corresponding severity level will be exported.
 - Step 5** Specify a destination for the file in the Export To area. Click **Browse** to browse for a particular destination. The files can also be overwritten or appended.
 - Step 6** Select a field separator type in the Export Options area. In addition, check the **Stop Export when** check box, and enter a number of records. The Event Export Manager will stop exporting after the user-specified number of records are exported.
 - Step 7** Click the **Start Export** tool. The Event Export Manager exports alarms and events to the specified file until **Stop Export** is selected, or until the current Cisco MGM session ends.
-