Fault and Performance Management

The Cisco MGM Alarm component, which is a customized component of the Cisco EMF platform, handles Cisco MGX 8000 Series CVG alarms and events. Cisco MGM receives alarm and event messages from managed objects and displays them in the MapViewer and Event Browser screens. MapViewer displays alarms on the topology view, and the event browser displays events in tabular form. The tabular data includes severity, date, source, and other information.

Cisco MGM implements alarm features using SNMP trap messages. A configuration file maps SNMP traps to Cisco MGM alarms. For more information, see the *Cisco Element Management Framework User Guide*.

Before Cisco MGM can process alarm information, you need to register the traps you want the Cisco MGX 8000 Series CVG to forward.

Monitoring Alarms and Events

You can monitor alarms and events from two screens:

- Map Viewer—Shows icons that indicate the most severe alarm
- Event Browser—Shows a table of alarms and events

In addition, you can configure notification groups and channels. These notifications provide audible and visual alerts when significant events occur. For usage details, refer to the *Cisco Element Management Framework User Guide*; the following sections are provided only as an orientation.

Using MapViewer to Display Alarms

Each MapViewer object can display the following information about its associated network element:

- Object name
- Object class
- Object state
- Event unacknowledged count
- Event unacknowledged state
- Event outstanding state

Figure 6-1   Information Displayed on an Object

✎

Note   The icon displays the most severe event only.

- The icon for the object shows the following information:
  - An event counter is displayed in the balloon.
  - A number indicates the number of the most severe events in the category.
  - A letter indicates the highest unacknowledged event severity in the category.
  - A plus sign appears if there are other less severe, unacknowledged events in the category.
- The object has a colored outline which shows the event status color.

The colors and codes of severities used in Cisco EMF are shown in Table 6-1.

Table 6-1   Alarm Severity Colors and Codes

Icon Color	Balloon Code	Severity of Event
Red	C	Critical
Orange	M	Major
Yellow	m	Minor
Cyan	W	Warning
Green	(none)	Normal
White	i	Informational

Event Browser Display

The event status of objects contained in a map can affect the event status of the parent icon. If the event status changes on a map object, the change is propagated to the parent icon. The event status for a parent icon is changed to reflect the most severe event of its children.

In Cisco EMF, when a condition (fault) occurs on a managed object, the system is notified immediately. This notification is shown as an event and can be viewed with the Cisco EMF Event Browser. The Event Browser is opened from the Cisco EMF launchpad. A window similar to the one shown in Figure 6-2 is displayed.

Figure 6-2   Cisco EMF Event Browser

The Event Browser enables you to manage the network efficiently; you can list, query, and sort all or some events according to how you want to manage the network.

Note   You can view events on Cisco EMF maps; however, only the most severe fault on a managed object is shown on the map icon for that object.

The main panel in the Event Browser window displays a list of events including:

- Object name (the managed resource name associated with the event).
- Time the event was raised.
- Severity of the event (color-coded). Refer to the Table 6-1 for more information.
- Description of the event.

Two indicators, color coded to match the severity of the event, are available to the left of the object name:

- Clear (shows whether an event is active or cleared)
- Ack (shows whether an event is acknowledged or unacknowledged)

Click the **Ack** button to indicate to other users that the fault is being worked on. The button changes to the color of the severity. If for any reason you cannot clear the problem, you can deselect this button so that the event can be reassigned. The **Clear** button is highlighted when the fault has been rectified. Highlighting indicates that the event requires no further attention.

Launching the Event Browser

You launch the Event Browser application using an icon on the Cisco EMF Launchpad. This icon opens the Query Editor window, from which you can specify the type of events to view.

Alternatively, you can right-click on one or more objects in the Map Viewer and then click **Tools > Event Browser**. The Event Browser displays only the events associated with the selected objects.

Viewing Cisco MGM Logs

You can check the log files for significant Cisco MGM and Cisco EMF events. Table 6-2 describes the important logs:

Table 6-2   Log Files

File	Description
<CEMFROOT>/logs/cmgmvCtlr.log	Controller event log
<CEMFROOT>/logs/LoggercmgmvCtlr.log	Cisco MGM-specific log

For more information about Cisco MGM log files, refer to the "Cisco MGM Log Files" section on page A-2.

Trap Management

Cisco MGM recognizes all traps sent from Cisco MGX 8000 Series CVGs. All traps are reported in the Cisco MGM Event Browser. Chassis, card, and line traps are reported in MapViewer.

Registering Traps

Before Cisco MGM can process alarm information, you need to register the traps you want the Cisco MGX 8000 Series CVG or media gateway controller (MGC) to forward to Cisco MGM.

✎ **Note**   Before registering traps, verify that the proper read/write community string is listed for the selected chassis you want to register.

To register traps, perform the following steps:

Step 1   Log on to Cisco EMF. The Cisco Element Manager Framework Launchpad screen opens.

Step 2   Click the **Viewer** button. The MapViewer screen opens.

Step 3   Click the tree of objects to display the list of sites and nodes.

Step 4   Right-click the desired site or node and click **Trap Registration**. The Trap Registration window opens. (See Figure 6-3.)

Figure 6-3   Trap Registration

Step 5   Select your desired chassis objects from the chassis list.

Step 6   Select **Register** from the Operation pull-down menu.

✎
Note   The default pull-down menu is blank. You must click on the pull-down menu to reveal the available options.

Step 7   Click **Start** to execute the operation. A pop-up dialog box indicates the success or failure of the request.

✎
Note   For PXM1-based chassis, trap manager aging is set to ENABLE by default. This parameter (set during trap registration) will eventually timeout and MGX will cease to send traps to Cisco MGM. However, Cisco MGM reregisters for traps periodically. Use the CLI command **agetrapmgr** to disable trap manager aging.

Deregistering Traps

To deregister traps using Cisco MGM MapViewer, perform the following steps:

Step 1   Log on to Cisco EMF. The Cisco Element Manager Framework Launchpad screen opens.

Step 2   Click the **Viewer** button. The MapViewer screen opens.

Step 3   Click the tree of objects to display the list of sites and nodes.

Step 4   Right-click the desired site or node and click **Trap Registration**. The Trap Registration window opens. (See Figure 6-3.)

Step 5   Select your desired chassis objects from the chassis list.

Step 6   Click **Deregister** from the Operation pull-down menu.

> **Note**   The default pull-down menu is blank. You must click on the pull-down menu to reveal the available options.

Step 7   Click **Start** to execute the operation. A pop-up dialog box indicates the success or failure of the request.

Updating Trap Forwarding

To update forwarding from Cisco MGM to other hosts, follow these steps:

Step 1   Log in as the root user.

Step 2   Change to the directory for scripts.

```
cd <CEMFROOT>/config/scripts/cmgmv
```

Step 3   Run the configuration script.

```
./updCmgmTrapForward
```

> **Tip**   To get help, enter **updCmgmTrapForward -h**

The script automatically restarts the trap manager, and the system begins forwarding traps.

Performance Management

Cisco MGX 8000 Series CVGs report performance information for DS1, E1, DS3, and SONET lines. In addition, you can set performance thresholds and assign alarm severities for the reporting gateways.

In addition to Cisco MGM performance management, CiscoView also provides device-specific performance management, including the following information:

- LAPD statistics
- Session set counters
- Session group counters
- RUDP statistics and counters
- SVC statistics counters
- Bearer statistical counters
- HDLC counters
- DSX1 line real time counters

All statistics data is collected in real-time, no historical data is stored.

For detailed information on CiscoView installation and operation, refer to *Using CiscoView 5.4*.