APPENDIX A

BAMS, Cisco MGC, and CMNM Messages

This appendix provides two kinds of information about event messages displayed in the CMNM Event Browser:

- For BAMS and Cisco MGC-related messages, it provides references from which you can navigate to the relevant document to look up the message you are interested in. A short description of each document is included.
- For CMNM internal messages, it provides a short explanation of each message along with any recommended action.

For information on alarm messages for the other devices managed by CMNM, see the following sections of Chapter 8:

- For the Cisco SLT, see Chapter 8, “Cisco SLT Alarms”.
- For Catalyst LAN switches, see Chapter 8, “Catalyst LAN Switch Alarms”.
- For the Cisco MGX 8260, see Chapter 8, “Cisco MGX 8260 Alarms”.

For information on application-related alarm messages for the Cisco MGC Host and the BAMS, see Chapter 8, “MGC Host and BAMS Resource Alarms”.

Looking Up BAMS and Cisco MGC Messages

Use this procedure to locate information for a specific message.

Step 1 In the Event Browser, check the Object Name to determine the network object that generated the event. Note the event description.

Step 2 In this document, go to the section that applies to that object.

Step 3 Click on the name of the document or section (displayed in blue to indicate a link) that contains the information you want. The linked document opens.

Step 4 Press Ctrl+F for your browser’s Find dialog box. In the dialog box, enter some of the initial text of the event description and click OK.

Note If your search text is not found, it means that the Event Browser description does not exactly match the generated message. You can search on a different part of the description string, or scroll through the document to find the message.

Cisco MGC Host Messages

The Cisco MGC Software Reference Guide (MGC Version 7.0 http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/sw_ref/index.htm) is a reference to Cisco MGC MML commands, system messages, XECfgParm, and billing interface. The System Messages chapter documents alarms and informational events in a chart (Table 2-2, Version 7 http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/sw_ref/elsysmsg.htm#83882) that includes the following information on each event:

- Alarm category—Alarm/event message, corresponding to the event description in the CMNM Event Browser.
- Description—Brief description of alarm/event.
- Severity level—The severity of the alarm/event.
- Event reporting—Whether the event is reported to the management interface and can be obtained using SNMP. (In the Event Browser, you will see only those events that are reported.)
- Alarm/event cause—The condition causing the alarm/event.
- SNMP trap type—Which SNMP trap type pertains to the event, displayed with a numeric code for the trap type:
  - 0 = No error
  - 1 = Communication alarm
  - 2 = Quality of service
  - 3 = Processing error alarm
  - 4 = Equipment error alarm
  - 5 = Environment error alarm
- Suggested Action—Recommendations for resolving the problem.

BAMS Messages

The BAMS traps alarms and minor, major, or critical events and forwards them to network management systems such as CMNM. The severity level for message forwarding defaults to minor and above, but may be changed by the BAMS system administrator.

The Billing and Measurements Server (Version 2.x) User Guide http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/bams2/ includes an appendix (Appendix A. Troubleshooting http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/bams2/app_a.htm) that provides a discussion of these messages and their use in troubleshooting. Messages are related to the tasks the BAMS performs, and the appendix also includes an explanation of BAMS tasks. The message documentation is organized by task.

The following categories of information are provided for each system message:

- Message ID—a six-character label that uniquely identifies each message. The first three characters are the application task ID, which identifies the application task that generated the message. (For example, MGR denotes the Manager task and MSC denotes the Mass Storage Control task.) The second three characters are the message number; for example, 013 or 122.
- Text—The verbal part of the message that appears in the system log file, generally corresponding to the event description in the CMNM Event Browser.

- Arguments—Variable parts of the message, enclosed in angle brackets.
- Description—An explanation of the event that generated the message.
- Action—what you should do as a result of the event described in the message. In some cases (for example, informational messages), no action may be required. Actions for error messages (manual, warning, minor, major, and critical) may include steps that should be followed to identify and correct problems. Error actions may also describe how BAMS responds to the specified error condition.

CMNM Internal Messages

The following messages may be generated by CMNM itself and reflect errors in deployment, discovery, or configuration. See the next section, “Solving Deployment and Discovery Errors”, for how to correct deployment and discovery errors.

Table A-1 CMNM Internal Events

Message	Explanation	Action
Subrack discovery failed. Check logs	CMNM failed to discover components on the device. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent does not run on the device, (3) the device is not reachable.	(1) Check the SNMP community strings and correct if needed. (2) If MGC or BAMS, check that the snmpdm and mib2agt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. For more information, refer to the log file <CEMF_INSTALLED_DIR>/logs/ mgcController.log
BAMS is not configured to receive Call Data Records from any MGC Host	Since the BAMS server is not configured to collect data from any MGC Host, CMNM cannot deploy the device to the right MGC node. Thus, its alarm status will not be propagated in the MGC-Node-View.	Check your BAMS configuration and check the VSC status.

Table A-1 CMNM Internal Events

Message	Explanation	Action
Could not get BAMS Poll table	CMNM failed to retrieve BAMS configuration via SNMP. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent does not run on the device, (3) the device is not reachable. As a result, CMNM cannot deploy the device to the correct MGC node. Thus, its alarm status will not be propagated in the MGC-Node-View.	(1) Check the SNMP community strings and correct if needed. (2) Check that the snmpdm and sagt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. For more information, refer to the log file <CEMF_INSTALLED_DIR>/logs/mgcController.log.
No IP addresses defined on this device. All traps from it will be ignored.	CMNM failed to find any address on this device via SNMP. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent does not run on the device, (3) the device is not reachable.	(1) Check the SNMP community strings and correct if needed. (2) Check that the snmpdm and mib2agt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.
Could not get password for host <IP Address>	Password is not specified for the deployed VSC host. As a result, CMNM cannot fully discover the device.	Correct the password information, then rediscover the device.
<Host name>: Could not collect inventory: Password not specified	Password is not specified for the deployed device. As a result, CMNM cannot fully discover the device.	Correct the password information, then rediscover the device.
<Host name>: Could not get Host Device table. Check IP address and read-community string.	CMNM failed to retrieve the device table from the device. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent or the hostagt process does not run on the device, (3) the device is not reachable.	(1) Check the SNMP read-community string and correct if needed. (2) Check that the snmpdm and hostagt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.

Table A-1 CMNM Internal Events

Message	Explanation	Action
<Host name>: Could not get Host Files System. Check IP address and read-community string.	CMNM failed to retrieve the device table from the device. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent or the fsagt process does not run on the device, (3) the device is not reachable.	(1) Check the SNMP read-community string and correct if needed. (2) Check that the snmpdm and fsagt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.
<Host name>: Could not get Host Storage table. Check IP address and read-community string.	CMNM failed to retrieve the device table from the device. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent or the hostagt process does not run on the device, (3) the device is not reachable.	(1) Check the SNMP read-community string and correct if needed. (2) Check that the snmpdm and hostagt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.
Could not get IP Address table from <device name>. Check IP address and read-community string.	CMNM failed to retrieve the interface table from the device. The problem may be (1) wrong SNMP community strings, (2) Invalid IP Address, (3) the device is not reachable.	(1) Check the SNMP read-community string and correct if needed. (2) Check the IP address. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.
Failed to launch action <Action name>. Perhaps hostController is not running.	The most probable cause is that the CMNM process *hostController* is down while CMNM is trying to discover a VSC.	Verify that the hostController is running. For example, enter: `ps -ef | grep hostController` If the hostController is running, rediscover the device. If not, contact the TAC.
The IP Address <IP Address> is not reachable.	CMNM failed to do SNMP ping with this address.	Check the network connection.
This device is not reachable.	CMNM cannot reach the device using SNMP. If the device has multiple IP addresses, then all of them are unreachable.	(1) Check the SNMP community strings and correct if needed. (2) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection.

Solving Deployment and Discovery Errors

If you receive a message about a problem in device deployment or discovery, use these procedures to change the deployment information or rediscover network elements

Changing Password or Community Strings

To change the password or community strings for a device:

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

Step 2 From the pull-down menu, choose Accounts. You see the Accounts dialog box.

Step 3 On the Accounts tab, check and if needed change the password.

Step 4 On the SNMP tab, check and if needed change the SNMP community strings.

Step 5 Click the Save button on the toolbar. Close the dialog box.

Step 6 If you made a change in community strings to any device, or in password to the MGC host, rediscover the device as described in "Rediscovering a Device After a Problem" below.

Changing IP Address

If the wrong IP address was entered, the device must be redeployed. To redeploy a device:

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

Step 2 From the pull-down menu, select Deployment and then Delete Objects. You see the Deployment Wizard dialog box with the message, "Ready to delete 1 object".

Step 3 Click the Finish button. You get a message that the object has been deleted. Click OK.

Step 4 Redeploy the device following the instructions in Chapter 6, "Manually Deploying a Site, Object, or Network".

Step 5 After deployment, rediscover the device as described in "Rediscovering a Device After a Problem" below.

Rediscovering a Device After a Problem

Follow these steps to rediscover a device after correcting a problem that interfered with discovery.

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

Step 2 Choose States. You see the States dialog box.

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

Step 4 Click Yes. CMNM rediscovers the device. During discovery, Current State is discovering. When the discovery is complete, Current State changes to active.

Step 5 Close the dialog box.