Troubleshooting

This appendix offers troubleshooting steps to help solve high-level problems while operating Cisco MGM or Cisco MGM GateWay. This chapter includes the following troubleshooting information:

For a list of error messages, see Appendix B, “Error Messages”.

Follow the troubleshooting procedures described in this section before contacting Cisco technical support.

1. Identify the source of the problem—Which devices, interfaces, hosts, applications have the problem?
2. Locate the problem on the network—On what VLAN, subnet, or segment is the problem occurring?
3. Compare current network performance against an established baseline—Is the performance better or worse?
4. Find out when the problem started—When did you first see the problem? Is it recurring?
5. Determine the extent of the problem—How widespread is the problem? Is it getting worse?

Note This chapter assumes that the server is installed under the default /opt/CiscoMGMServer directory and the client is installed under the default /opt/CiscoMGMClient or C:\Cisco\MediaGatewayManagerClient directory. If a directory other than the default installation directory is specified, replace the default path with the installed path during setup.

C.1 Server Problems

This section describes troubleshooting procedures for the following Cisco MGM server-related problems:

Note Log in as the root user on the Sun Solaris workstation where the Cisco MGM server is installed to perform any operations on the Solaris workstation.

C.1.1 Cisco MGM Server Does Not Respond

If the server does not respond, complete the following steps:

Step 1 Log in as the root user on the Solaris workstation where the Cisco MGM server is installed.

Step 2 Enter the following command to view the status of the Cisco MGM server processes:

```
showmgm
```

If you do not have root user privileges but you belong to the UNIX group that can use sudo functionality to run commands as non-root, enter the following command:

```
sudo showmgm
```

If there is a line containing /MGMServer, the Cisco MGM server is running.

If there is no line containing /MGMServer, the Cisco MGM server is not running. Proceed to Step 3.

Note You can also check the mgmop.log file found in /opt/CiscoMGMServer/log to check whether the server was stopped by another user or it stopped abnormally. If it stopped abnormally, proceed to Step 3.

Step 3 Run the **getinfo.sh** Cisco MGM server tool and send the data to Cisco technical support for analysis.

If you do not have root user privileges but you belong to the UNIX group that can use sudo functionality to run commands as non-root, enter the following command:

```
sudo getinfo.sh
```

Step 4 Start the Cisco MGM server by using the mgms-start script located in the /opt/CiscoMGMServer/bin directory.

a. Log in as the root user.

b. Change the directory to /opt/CiscoMGMServer/bin and enter the following command:

```
mgms-start
```

If you do not have root user privileges but you belong to the UNIX group that can use sudo functionality to run commands as non-root, enter the following command:

```
sudo mgms-start
```

If the preceding procedure does not solve the problem, complete the following steps:

Step 1 Verify that the /opt/CiscoMGMServer/cfg/MGMServer.cfg file is not corrupted. The file should contain the db-config-mode = auto parameter in the [database] section. If the entry is missing, the Cisco MGM server configuration file is corrupt. Reinstall the Cisco MGM server.

Step 2 Verify that the first entry in the /var/opt/oracle/oratab file looks similar to MGM5_0:/oraclesw/product/8.1.7:Y. If this entry is missing, the Oracle database might not be installed. The Oracle database is a prerequisite for installing the Cisco MGM server.

C.1.2 Cannot Connect to the Cisco MGM Server

If you cannot connect to the server, complete the following:

Step 1 Ping the server's IP address from the client PC/workstation.

Step 2 If the ping fails, resolve the IP connectivity problem and try again.

Step 3 SSH or Telnet to the server and log in as the root user.

Step 4 Enter the following command to verify if Cisco MGM is running:

```
showmgm
```

If you do not have root user privileges but you belong to the UNIX group that can use sudo functionality to run commands as non-root, enter the following command:

```
sudo showmgm
```

Step 5 The server should have at least the following four processes running:

```
root 3778 0.1 0.1567 9592 ? S 16:57:36 0:00 /opt/CiscoMGMServer/bin/CTMServer
root 3771 0.1 0.4 6208 pts/1 S 16:57:34 0:00 /opt/CiscoMGMServer/bin/CTMServer
root 3876 0.5 0.6129464 8648 ? R 16:58:12 SnmpTrapService
root 3798 26.8 4.115732060968 ? S 16:57:37 0:29 SMService
```

Step 6 Manually stop the server if you see fewer than four processes running. Enter the following command:

```
mgm-stop
```

Step 7 If you changed the server IP address, verify that the configuration files shown in Table 5-18 have been updated. See the "5.3.6.1 Updating the Configuration Files after Changing the Cisco MGM Server IP Address" section on page 5-42.

Step 8 Verify if the Oracle database is accepting connections.

a. Log in as the Oracle user. Enter the following command:

```
su-oracle
```

b. Open an SQLplus session:

```
omu-u60-3% sqlplus ctmanager/ctm123!
SQL*Plus: Release 8.1.7.0.0 - Production on Fri Aug 30 00:08:12 2002
(c) Copyright 2000 Oracle Corporation. All rights reserved.
Connected to:
Oracle8i Release 8.1.7.0.0 - Production
JServer Release 8.1.7.0.0 - Production
SQL>
```

Step 9 Reboot the server if you get another error message and the SQL prompt does not appear. Wait enough time for the server to boot up and try to run the client. The SQL prompt indicates that the Oracle database is running and accepting connections

Step 10 Manually restart Cisco MGM.

```
SQL> exit
Disconnected from Oracle8i Release 8.1.7.00 - Production
JServer Release 8.1.7.0.0 - Production
omu-u60-3% exit
omu-u60-3% logout
mgms-start
```

If you do not have root user privileges but you belong to the UNIX group that can use sudo functionality to run commands as non-root, enter the following command:

```
sudo mgms-start
```

Step 11 Wait for 5 minutes and run the client.

C.1.3 NE Connection State Is Listed as Unavailable

If the connection state of an NE is listed as Unavailable in the Domain Explorer window, a connectivity or configuration problem exists. Wait 5 to 10 minutes after adding the NE to the Cisco MGM domain; then, complete the following steps:

Step 1 To see the NE IP address, select the NE in the Domain Explorer window. The Address tab of the Network Element Properties sheet lists the IP address of the selected NE.

Step 2 From the Cisco MGM server, enter the following command to verify connectivity between the Cisco MGM server and the NE:

```
ping IP_address
```

Step 3 If the ping fails, a physical or configuration problem exists in the communication between an NE and Cisco MGM.

Step 4 If the ping succeeds, verify that the NE software version is listed in the Supported NE Table.

Step 5 SNMP read and write community strings must be set up properly on each NE. To view the community string, enter:

```
dspsnmp
```

The community strings configured on the server should match the strings configured on the NE. For information on configuring community strings in Cisco MGM.

C.1.4 Launching Tables Results in Database Errors

If the Oracle database or Oracle listener that Cisco MGM is using is down, launching tables will generate database errors. To troubleshoot table launching errors:

Step 1 Log in as the Oracle user and enter the following command:

```
sqlplus ctmanager/ctm123!
```

If login is successful, an SQL> prompt appears, which indicates that the Oracle database has been installed and the database server is up and running. If login fails, either the Oracle database has not been installed or the database server is not running.

Step 2 To start the Oracle database, log into the Solaris workstation as the Oracle software owner user.

Step 3 Enter the following command at the shell prompt to start the Oracle database:

```
dbstart
```

Step 4 Enter the following command at the shell prompt to start the Oracle listener:

```
lsnrctl start
```

If there are still problems with starting the Oracle database or the Oracle listener, refer to the Oracle documentation or contact Oracle support.

C.1.5 SNMP Traps Are Not Forwarded from NEs

SNMP traps might not be forwarded, either because the trap port is already in use, or because the NE is not properly configured.

C.1.6 Trap Port Is Unavailable

The Cisco MGM server requires exclusive access to the SNMP trap port to receive SNMP traps from the NE.

Step 1 To verify that the standard SNMP trap port (number 162) is not being used by another application running on the same Solaris workstation, enter the following command:

```
netstat -a | grep 162
```

If the following line is seen, the SNMP trap port is being used by another application:

```
*.162 Idle
```

Step 2 If the trap port is being used by another application, you must stop the other application.

C.1.7 NE Is Not Discovered

If Cisco MGM cannot discover an NE, complete the following steps:

Step 1 Verify that the NE is up and running.

Step 2 Verify that the NE IP address and default route are configured correctly.

C.1.8 NE Is Not Reachable

If Cisco MGM cannot reach an NR, complete the following steps:

Step 1 Verify that the NE is up and running.

Step 2 Verify that the NE IP address and default route are correctly configured.

Wait for five poll cycles while Cisco MGM reestablishes connectivity with the NE.

Step 3 To test IP connectivity to the NE from the Cisco MGM server, enter the following command from the Solaris workstation running Cisco MGM:

```
ping NE_IP_address
```

Step 4 Verify that the username and password that Cisco MGM uses to reach the NE exist on the NE.

C.1.9 NE Model Type Appears as Unknown

If an in-service NE is added to the Domain Explorer, but the model type appears as unknown, the software version of the NE might not be prepopulated in the database. In other words, Cisco MGM cannot match the NE with a recognizable version.

C.1.10 Memory Backup, Memory Restore, or Software Download Fails

Complete the following steps if memory backup, memory restore, or software download fails:

Step 1 Log into the Cisco MGM client with the appropriate user profile.

Step 2 In the Domain Explorer window, choose **Administration > Job Monitor**. The Job Monitor Table shows the status of the operation. The reason for the failure is shown in the Additional Information column.

Step 3 Return to the Domain Explorer window and choose **Administration > Error Log**. The Error Log shows information about the backup, memory restore, or download failure.

Step 4 Refer to the "B.2 Cisco MGM Server Error Messages" section on page B-61 for the correct action to take in response to the error.

C.1.11 Memory Autobackup, Software Commit, or Software Revert Fails

If memory autobackup, software commit, or software revert fails, use this procedure to troubleshoot the failure:

Step 1 Log into the Cisco MGM client with the appropriate user profile.

Step 2 In the Domain Explorer window, choose **Administration > Audit Log**. The Audit Log shows the status of the operation.

Step 3 Return to the Domain Explorer window and choose **Administration > Error Log**. The Error Log shows the reason for the failure.

Step 4 Refer to the "B.2 Cisco MGM Server Error Messages" section on page B-61 for the correct action to take in response to the error.

C.2 Client Connectivity Problems

The Cisco MGM client might not be able to connect to the Cisco MGM server for various reasons. Complete the following procedures in the order listed until the problem is resolved:

C.2.1 Database Is Not Available

If the Cisco MGM client cannot connect to the Cisco MGM server, verify that the database is available.

Step 1 Log into the Cisco MGM server as the Oracle user.

Step 2 Enter the following command to connect to the database:

```
sqlplus ctmanager/ctm123!
```

Step 3 If the error message "maximum processes exceeded" is received, the maximum number of database connections have been reached. Close several clients or ask the database administrator to increase the maximum number of processes for the database.

C.2.2 Database Timeout Occurred

If a database timeout occurred, complete the following:

Step 1 Reduce the scope of the query by selecting a group or a network element and not the entire domain before opening tables such as the Alarm Browser, Alarm Log, and Audit Log.

Step 2 Increase the client database query timeout period by editing the ems-client.cfg file located at C:\Cisco\MediaGatewayManagerClient\config, /opt/CiscoMGMClient/config, or other directory where the client was installed.

Step 3 Add hardware resources to the Oracle database server.

Step 4 Ping the Oracle database server from the client to verify the response time. Increase the bandwidth if the round-trip response time is inadequate.

C.2.3 Are the Cisco MGM Client and the Cisco MGM Server Connected?

If the database is available, check connectivity between the client and the server:

Step 1 To see the Cisco MGM server IP address, enter the following command on the Solaris workstation that is running the Cisco MGM server:

```
ifconfig -a
```

The command output looks similar to the following example:

```
hme0:flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST>mtu 1500
inet 192.168.120.93 netmask ffffff00 broadcast 192.168.120.255
```

The IP address is the address following the inet field.

Step 2 To verify that the physical connection between the Cisco MGM client and the Cisco MGM server does not have problems, enter the following command from the Cisco MGM client:

```
ping IP_address
```

where the IP address belongs to the Solaris workstation that runs the Cisco MGM server.

Step 3 If the ping command is not successful, fix the physical connectivity; then, log into the Cisco MGM client.

C.2.4 Cannot Log In as Provisioner or Operator

Complete the following steps if the user cannot log in as a Provisioner or Operator:

Step 1 Use the default username and password to log into the Cisco MGM client:

Username: **SysAdmin**

Password: **MGM123!**

Step 2 If system administrator login is successful, but Provisioner or Operator login was not, verify that the Provisioner or Operator exists and is not disabled. In the Domain Explorer window, choose **Administration > MGM Users** to view a table of all configured Cisco MGM users.

Step 3 If the Provisioner or Operator is not in the Cisco MGM Users table, the user is not configured. Configure the Provisioner or Operator; then, log in as that user.

Step 4 If the Provisioner or Operator is in the Users table, select the row corresponding to that user and click the **Modify User Properties** tool to bring up the Modify Cisco MGM User Properties wizard. Verify that the admin state is enabled. If the admin state is disabled, enable it and log in as the Provisioner or Operator. The user might have been disabled after attempting to log in with an incorrect password.

Step 5 If the password is not correct, set a new password for the user and log in again.

C.2.5 "Cannot Authenticate User" Message Appears

If the "Cannot authenticate user" error message is received when logging into the Cisco MGM client, the Cisco MGM server might be initializing. Wait for five minutes while the Cisco MGM server finishes initializing; then, try to log in again. Alternately, check your username and password and enter them again. The username and password are case sensitive.

C.3 Client Operational Problems

Procedures for troubleshooting client operational problems are provided in the following sections:

C.3.1 Cannot Delete an NE

If an NE cannot be deleted, verify that the user logged in as SuperUser or NetworkAdmin—not as a Provisioner or Operator. Provisioners and Operators cannot delete NEs. If the user logged in as Provisioner or Operator, restart the Cisco MGM client session and log in as SuperUser.

C.3.2 Added a New Software Version to the Wrong NE

If a new software version is added to the wrong NE:

Step 1 In the Supported NE Table, delete the incorrect entry.

Step 2 Select the correct NE row from the Supported NE Table.

Step 3 Add the correct software version.

Step 4 In the Domain Explorer, Network Element Properties, set the operational state of all NEs that are behaving erroneously to **Out of Service**.

Step 5 Click **Save**.

Step 6 In the Network Element Properties, set the operational state of all the NEs back to **In Service**.

C.3.3 Cannot Schedule Jobs

The Cisco MGM client is used to schedule three types of administrative tasks:

- Software download
- Memory backup
- Memory restore

Cisco MGM maintains an Error Log and audit log to track potential problems. To view the Error Log or audit log:

Step 1 In the Domain Explorer window, choose **Administration > Audit Log** or **Administration > Error Log**.

Step 2 Look for errors related to software download, memory backup, or memory restore.

C.3.4 Cannot Customize the Network Map

If an image file is not displayed while changing the Network Map background or while changing a node icon, complete the following steps:

Step 1 Choose another image file. The file might be corrupt.

Step 2 Check the size of the image file. The image file might be larger than 100 KB, which is too big to load. If the file is too big, use a smaller image file.

Step 3 Verify that the image file exists in the \images\mapbkgnds\shapefiles directory or the *MGM_client_install_directory*\images\mapicons directory. If the file is missing, it has been deleted. Reinstall the Cisco MGM client.

Note The client is bundled primarily with shape files (*.shp) and only a few map background GIF files.

C.3.5 Color Settings when the Cisco MGM Client Is Run on a Sun Ultra 5 Workstation?

To run the client on a Sun Ultra 5 workstation, the color map must be changed from 8 bit to 24 bit. If the colors do not look right, change the color map from 8 bit (the default) to 24 bit as follows:

Step 1 To see the current color settings, enter the following command:

```
/usr/sbin/m64config -prconf
```

Command output looks similar to the following example:

```
--- Hardware Configuration for /dev/fbs/m640 ---
ASIC: version 0x7c004750
DAC: version 0x0
PROM: version 104
Card possible resolutions: 720x400x88, 640x480x60, 640x480x72, 640x480x75, 800x600x56,
800x600x60, 800x600x72, 800x600x75, 1024x768x87, 1024x768x60, 1024x768x70, 1024x768x75,
1280x1024x75, 1280x1024x60, 1152x900x66, 1152x900x76, 1280x1024x67, 1280x800x76,
1280x1024x85
1280x1024x76, 1152x864x75, 1024x768x77, 1024x800x84, vga, svga, 1152, 1280, 800x600,
1024x768, 1280x1024, 1152x900
Monitor possible resolutions: 720x400x70, 720x400x88, 640x480x60, 640x480x67, 640x480x72,
640x480x75, 800x600x56, 800x600x60, 800x600x72, 800x600x75, 832x624x75, 1024x768x60,
1024x768x70, 1024x768x75, 1280x1024x75, 1152x870x75, 1152x900x66, 1152x900x76,
1280x1024x67, 1280x1024x76, vga, svga, 1152, 1280, 800x600, 1024x768, 1280x1024, 1152x900
Possible depths: 8, 24
Current resolution setting: 1280x1024x76
Current depth: 8
```

Step 2 To change the color setting to 24 bit, log in as the root user and enter the following commands:

```
su
Password: password
/usr/sbin/m64config -depth 24 -res 1152x900x76
```

Step 3 Reboot the workstation for the new color settings to take effect.

Note The resolution in 24-bit depth is a little lower than is possible with 8-bit depth (1152 x 900 x 76 versus 1280 x 1024 x 76), but the difference is hardly noticeable.

C.3.6 How Do I Collect Thread Dumps?

Thread dumps are helpful references when debugging the Cisco MGM process. To collect thread dumps:

Step 1 Log into the server workstation as the root user.

Step 2 On the command line, enter the following:

```
thread_dumper [\<Group/Service>\]
```

where:

- *Group* is the group name for which to collect thread dumps. It can be:
  - SM
  - SNMPTRAP
  - NE
  - PM
  - GW

- *Service* is the service name for which the thread dump is required. It can be:
  - SMService
  - SNMPTrapService
  - CORBAGWService
  - MGX8880NEService
  - MGX8850NEService
  - UnmanagedNEService

C.3.7 Launching Help on a Solaris Client

To launch help on a Solaris Client, Netscape must be in the PATH environment variable.

To check this:

Step 1 Change to a C-Shell, enter the following command:

```
# csh
```

Step 2 Check to see if Netscape is in the PATH environment, enter:

```
# which netscape
```

If the error message 'Command not found' is received, Netscape is not in the PATH environment.

You can also try to locate the path for Netscape, and check the version. On Solaris 8 machines, the default location is /usr/dt/appconfig/netscape. If Netscape is available, you will see:

```
# /usr/dt/appconfig/netscape/netscape  -version Netscape 4.76/U.S., 06-Oct-00; (c)
1995-2000 Netscape Communications Corp.
```

Step 3 To add Netscape to the PATH environment variable, enter:

```
# setenv PATH /usr/dt/appconfig/netscape:${PATH}
```

To make this change permanent, add the following line to /.cshrc file:

```
# setenv PATH /usr/dt/appconfig/netscape:${PATH} .cshrc
```

Step 4 Launch the Cisco MGM client, enter:

```
# /opt/CiscoMGMClient/mgmc-start
```

C.4 Topology Problems

This section includes the following information:

C.4.1 Discovery Mechanism

Cisco MGM manages the PNNI network. The ILMITopoc process discovers the physical PNNI network using SNMP protocol. All the discovered nodes are displayed in all the MGX NE GUIs such as Configuration Center (CC), Diganostic Center (DC), Statistics Report (SR), Chassis View (CV) GUI. Cisco MGM is notified of all subsequent changes in the network through traps for MGX nodes.

Once the ILMITopoc process discovers all the nodes, it sends all the nodes to topod process. Topod then sends these nodes and trunks to other processes in Cisco MGM such as ooemc, NMServer, nts etc.

C.4.2 Discovery Issues at Startup

This section includes the following information:

C.4.2.1 No Nodes Are Discovered

No nodes are in the Cisco MGM database.

Step 1 Verify that the nodes are ip reachable. Get the primary ip of the node by issuing the CLI commands **dspndparms** and **dspipif**. Then check if the node is ipreachable from Cisco MGM.

This can be done by doing a ping <node ip address>.

Step 2 If the nodes are ip reachable from Cisco MGM, verify that the community strings of the gateway nodes are correct.

This can be done by issuing the command **dspsnmp** on the switch CLI of the node that is not getting discovered. Compare this community string with that in the node_info table. The community string in the node_info table is encrypted. You will need to decrypt this string and verify it.

Step 3 If it is a MGX2 node and If persistent topology is enabled on the switch gateway and some nodes in a peer group are not getting discovered, verify that persistent topology is enabled on the gateway in the peer group using the CLI dsptopogw. If the gateway flag is enabled then verify in the node is part of the list of nodes on the gateway using the CLI command dsptopondlist

Defect Information—Collect the following information for further analysis:

- Save topod.log, ILMITopoc.log
- Collect the data in node_info table.
- Collect the output of dspndparms, dspsnmp, dspipif on the MGX node.

Possible alternative workaround—None

C.4.2.2 Node Name Is Incorrect in Database

The node name of the standalone MGX node is incorrect.

Step 1 If the node table has the name correct

- Dump the cache of topod and ILMITopoc. This can be done by issuing a kill -USR1 to the process. From the dump verify which process has the information incorrectly. If the information is correct in all these processes then open a new GUI and verify if the problem still exists.

Step 2 If the node table does not have the name correctly

- Check the ILMITopoc.log file to see from which node it got the wrong information.
- Do an snmpget -c <community> <ipAddress> 1.3.6.1.2.1.1.5. Verify that the name received as a response is correct. If it is not then verify the name on the switch.

Defect Information—Collect the following information for further analysis:

- Save the ILMITopoc.log and topod.log
- Collect the dump outputs of ILMITopoc, topod. The dump can be captured by issuing a kill -USR1 signal to the process.
- Collect the output of the switch CLI, selnd and dbnds.

Possible alternative workaround—None

C.4.2.3 Node IP Is Incorrect in Database

The ip Address of a node is not shown correctly.

Step 1 If the node table has the ipAddress correct

ßDump the cache of topod and ILMITopoc. This can be done by issuing a kill -USR1 to the process. From the dump verify which process has the information incorrectly. If the information is correct in all these processes then open a new GUI and verify if the problem still exists.

Step 2 If the node table does not have the ipAddress set correctly:

- In Cisco MGM, since the node does not have any PNNI trunks and the persistent topology feature is not enabled on this node, by default this node will be managed using the lan ip address. Verify if this is the case.

Defect Information—Collect the following information for further analysis:

- Save ILMITopoc.log and topod.log
- Save the dump outputs of ILMITopoc, topod. The dump can be captured by issuing a kill -USR1 signal to the process.
- Collect the output of the switch CLI, selnd and dbnds.

Possible alternative workaround—None

C.4.2.4 Node Alarm Shown Incorrectly in Database

The node alarm state of a node is incorrect.

Step 1 Check the cache of topod and ILMITopoc.

Dump the cache of topod, ILMITopoc. This can be done by issuing a kill -USR1 to the process. From the dump verify which process has the information incorrectly.

Step 2 If the node table does not have the node alarm status set correctly:

- Check the ILMITopoc.log file
- do an snmpget -c <community string> <ipAddress>1.3.6.1.4.1.351.110.1.1.14

This will return the alarm state of the node. 1 - Clear, 2- Minor, 3 - Major, 4- Critical

Defect Information—Collect the following information for further analysis:

- Save ILMITopoc.log, topod.log
- Save the dump outputs of ILMITopoc, topod. The dump can be captured by issuing a kill -USR1 signal to the process.
- Collect the output of the switch CLI, selnd and dbnds.

Possible alternative workaround—None

C.4.2.5 Reachable Node Is Shown as Unreachable

Node that is reachable from Cisco MGM is shown as unreachable on the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

Step 1 If the node table has alarm state of this node as minor, major, critical or clear:

- Dump the cache of NMServer,Topod and ILMITopoc. To dump the cache issue a kill -USR1 signal to the process. Check the dumps in the /opt/svplus/log directory and verify if the node alarm status is correct in the cache dumps. If the alarm status is correct in the cache dump then open a new GUI and check if the node shows in the correct alarm status in that GUI.

Step 2 If the node table has alarm state of an MGX node as unreachable:

- Verify that the node is ipreachable from Cisco MGM

Ping the active ip address of the node. The active ip will be the ip address of the node that is populated in the node table.

- Verify that the community string in the node_info table is the same as the community string on the node. The community string of a node can be got using the CLI dspsnmp.
- Check nts logs to see if nts has declared the node as reachable. See C.15.1 NTS. If nts has declared the node as reachable, check the topod.log for "nonRoutingNodeMsg" for this node. Verify that the alarm status in this message is the correct alarm status

Defect Information—Collect the following information for further analysis:

- Save ILMITopoc.log, topod.log, NMServer.*.log, nts.*.log, ooemc*log
- Collect the dump outputs of ILMITopoc, topod and NMServer. The dump can be captured by issuing a kill -USR1 signal to the process.
- Collect the output of the switch CLI, selnd and dbnds.

Possible alternative workaround—None

C.4.2.6 Cisco MGM State Is Incorrect

The management state of the node in the node table (column mgmt_state) shows as DOWN (2) or UNKNOWN (0) even when the node is reachable by IP.

Step 1 Check the trap manager registration of the Cisco MGM station on the node.

Login to the node and do a "dsptrapmgr" to check if the particular Cisco MGM station has registered to the node for traps. This is necessary for the node to be declared as manageable (mgmt_state = UP).

Step 2 Check the community strings of the node in the node-info table.

a. Enter the community strings (SNMP-GET and SNMP-SET) of the node through the Domain Explorer GUIs "NE Authentication" tab. They may have been incorrect in the node-info table. This can be verified if the decrypt tool for the encrypted strings in the database is available.

b. Check in NTS.log to see if trap registration has been successful for the node. See C.15.1 NTS.

Defect Information—Collect the following information for further analysis:

- Save ILMITopoc.log, topod.log and ooemc*.log

Possible alternative workaround—None

C.4.3 Discovery Issues at Runtime

This section includes the following information:

C.4.3.1 Node Added Not Shown in Cisco MGM Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs

Dynamically added Route routing node not shown on Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs

Step 1 If the node table has an entry for the node

- Dump the cache of NMServer, Topod and ILMITopoc. To dump the cache issue a kill -USR1 signal to the process. Check the dumps in the /usr/user/svplus/log directory and verify if the node is present in the cache dumps. If the node is present then open a new GUI and check if the node shows in that GUI.

Step 2 If the node table does not have an entry for the node

- Check ILMItopoc log and verify if it received a 70005 and 70201 (in case persistent topology feature is turned enabled).
- If you see the trap in the log, verify that ILMITopoc's snmp requests issued after receiving the trap are successful. If the snmp is not going through verify if the newly added node is ip and snmp reachable from Cisco MGM.
- If you do not see any of these traps in the ILMITopoc.log, see C.15.1 NTS.

Defect Information—Collect the following information for further analysis:

- Save ILMITopoc.log, topod.log, NMServer.log, nts.*.log
- Collect the dump outputs of ILMITopoc, topod and NMServer. The dump can be captured by issuing a kill -USR1 signal to the process.
- Collect the output of the switch CLI, selnd and dbnds.

Possible alternative workaround—Add the node again to the network by first deleting it and then adding it again.

C.4.3.2 Node Name Change Not Getting Updated in Cisco MGM Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs

Changes in the name of a node not reflected on the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

Step 1 If the node table has an entry for the node with the correct name

- Dump the cache of NMServer, Topod and ILMITopoc. To dump the cache issue a kill -USR1 signal to the process. Check the dumps in the /usr/user/svplus/log directory and verify if the node name is correct in the cache dumps. If the node name is correct in the cache dump then open a new GUI and check if the node shows in that GUI.

Step 2 If the node table does not have an entry for the node with the correct name

- Check ILMItopoc.log and verify if it received a 60006 and 70202
- If you see the trap in the log, verify that ILMITopoc's updates its cache based on this trap. If it fails to update the node name then ILMITopoc.log will contain "%ILMITopoc-3-updateFailed: <Node_c::updateName> Failed to update node name."
- If you do not see any of these traps in the ILMITopoc.log, see C.15.1 NTS.

Defect Information—Collect the following information for further analysis:

- Collect ILMITopoc.log, topod.log, NMServer.*.log, nts.*.log
- Collect the dump outputs of ILMITopoc, topod and NMServer. The dump can be captured by issuing a kill -USR1 signal to the process.
- Collect the output of the switch CLI, selnd and dbnds.

Possible alternative workaround—None

C.4.3.3 Node IP Address Change Not Getting Updated in Cisco MGM Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs

The ip address of the node does not get updated dynamically on the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

Step 1 If the node table has an entry for the node with the correct ip address.

- Dump the cache of NMServer, Topod and ILMITopoc. To dump the cache issue a kill -USR1 signal to the process. Check the dumps in the /opt/svplus/log directory and verify if the node name is correct in the cache dumps. If the node name is correct in the cache dump then open a new GUI and check if the node shows in that GUI.

Step 2 If the node table does not have an entry for the node with the correct ip address

- Check ILMItopoc.log and verify if it received a 60007 and 70202
- If you see the trap in the log, verify that ILMITopoc's updates its cache based on this trap.
- If you do not see any of these traps in the ILMITopoc.log, see C.15.1 NTS.

Defect Information—Collect the following information for further analysis:

- Collect the ILMITopoc.log, topod.log, NMServer.*.log, nts.*.log
- Collect the dump outputs of ILMITopoc, topod and NMServer. The dump can be captured by issuing a kill -USR1 signal to the process.
- Collect the output of the switch CLI, selnd and dbnds.

Possible alternative workaround—None

C.5 Equipment Management Problems

This section includes the following information:

C.5.1 Sync Up Issues

This section includes the following information:

C.5.1.1 EM Declares Successful Node Re-sync When Node Mode Is 3

MGX nodes are managed by OOEMC component in Cisco MGM. Equipment Management (EM) uses coldstart, warm start, and periodic resync to sync up network data. Each of these resync methods will involve configuration file upload, parsing, and DB population. Node mode in node table indicates the state of the sync up process. The possible node modes are 1, 2, 3 and 5. Expected mode for a successful node resync is 3. If the node mode stays in other mode for a long period of time, it indicates some kind of resync problem. Keep in mind that any sync up problem could be caused by switch, SNMP, FTP, and OOEMC itself. User needs to branch out to different areas for identifying the root cause of any sync up problem.

The following is the flow of events which are involved in OOEMC coldstart sync up process:

1. Topo process discovers a node in the network. The process will change the node mode in node DB table to -1. Then it notifies OOEMC component for the discovery. Then OOEMC will change the node mode from -1 to 1 after the component starts managing the node.
2. When NTS component is able to register with the node, it sends link up message to the OOEMC which manages the node. The OOEMC component will change the node mode from 1 to 2 to signify the start of node sync up.
3. The OOEMC component sends SNMP bulk file creation request to the switch. If the request is allowed, the switch will send trap 60901 to the Cisco MGM to signify the start of bulk file creation. When bulk file creation is completed on the switch, the switch will send trap 60902 to the Cisco MGM. After Cisco MGM has received this trap, it will start the FTP of the config upload files.
4. f the upload and parsing of all config files have completed without error, the OOEMC will change the node mode from 2 to 3. If the upload or parsing of config upload for any service module on the switch, the node sync up will complete partially and the OOEMC will change the node mode from 2 to 4 at the end of the node sync up process. If the error occurs on the shelf generic card file (CARD_01_CC.CF) or pnni file (PNNI_01_CC_CF), the OOEMC will change the node mode from 2 to 5 to signify node sync up failure.

C.5.1.2 Network Setup and Configuration Required for OOEMC Sync Up Process

There are network setup and Cisco MGM configuration prerequisite required by EM before it can start sync up process. On the switch, the following is the check list for trap manger and trap IP setup:

Use CLI "dsptrapmgr" to check that the Cisco MGM IP has been added to the trap manager. If you find that your Cisco MGM IP is not registered with the switch, add the Cisco MGM IP to the trap manager by typing the CLI "addtrapmgr cwm_ip 2500" where 2500 in the command is the port number and cwm_ip is the IP address of your Cisco MGM machine. You may need to delete other IP from the trap manager list if the list has been full. If the list is not full, the registration will take place automatically if the Cisco MGM is configured to manage the node.

The trap IP should have been configured on the switch properly. Whenever you configure the switch to use whatever IP (atm0 IP or lnPci0 IP) of the switch as primary IP, the topology component of Cisco MGM should use that IP for node discovery. You can display the primary and secondary IP information of the switch by typing CLI "dspndparms". To configure primary and secondary IP, you can enter "cnfndparms" and the CLI will prompt you for options. After you have set up the primary and secondary IP, you should also configure the primary IP as trap IP on the switch by entering CLI "cnftrapip configured_IP" where configured_IP is the IP that you have chosen to use as primary IP in CLI "cnfndparms".

On the Cisco MGM, the following is a list of configurable parameters in the file /opt/svplus/config/emd.conf of your Cisco MGM machine that you should set up for proper problem logging:

"OODebug" : For debugging purpose, this parameter should be set to level 6 or above, e.g. the log level statement in emd.conf should be "OODebug Level 6".

"OOKeep" : For debugging purpose, this parameter should be set to a value depending on how many log files you want to keep, e.g. the statement in emd.conf should be "OOKeep 100 OOEMC log files per oochild"

Sometimes, a different network environment requires other parameters in the same files to be tuned for correct functioning of Cisco MGM.

C.5.1.3 Node Mode Remains in 1

The node has been discovered by network topology process in Cisco MGM and its node mode has been changed from -1 to 1 in node table entry, but it stays in mode 1 for a long period of time.

Step 1 If the Cisco MGM stays in mode 1 for a long time after Cisco MGM core has been started, you need to check the trap manger on the switch. See C.5.1.2 Network Setup and Configuration Required for OOEMC Sync Up Process for trap manager and trap IP setup.

Step 2 If steps 1 is not an issue, then check for rtm link up message that NTS sends to EMD. OOEMC will start node resync once EMD notifies OOEMC that the node is active. Therefore, the second step for debugging this mode 1 problem is to see whether rtm link up message has been received by EMD and whether it has been forwarded to OOEMC.

For example, to find out the rtm link up messages received by EMD for node with id 9, do the following

grep RTM_LINK_UP emd* | grep "Node id 9"

Once the location of the rtm link up message is found in the log, view the log file for more information on notification to OOEMC

Step 3 If rtm link up message for the node is found and the log indicates that notification to OOEMC has been sent, then collect log files and report the problem.

Step 4 If rtm link up message cannot be found, then search for link down message. Grep "RTM_LINK_DOWN" from emd log files. If rtm link down message is found, then the node is not reachable to the NTS process. Check with the network administrator and see C.15.1 NTS if "RTM_LINK_UP" and "RTM_LINK_DOWN" messages are not found.

Defect Information—Collect ooemc and nts log files under /opt/svplus/log.

Possible alternative workaround—None

C.5.1.4 Node Mode Remains in 2

After rtm link up message has been received by EMD and node active message has been sent to OOEMC, OOEMC will change the node mode from 1 to 2 and trigger node resync. Depending on the switch configuration and network activities, the node resync time varies. If the node mode stays in mode 2 for longer than the node resync normally takes, there can be the problem with node resync process.

Step 1 The debugging process for this problem is mainly focus on log file inspection. Make sure that log level of all related Cisco MGM processes is set at right level. See C.5.1.2 Network Setup and Configuration Required for OOEMC Sync Up Process Cisco MGM configuration.

Step 2 The first thing to check is "cd" to "/opt/svplus/tmp" to check for configuration upload files. For example, if the node's node_id is 9, then do "ls -ltr *.9" to see what files have been uploaded for this node. If you see some files have been uploaded for this node, then the node resync is still proceeding. Make sure that the time stamps for these files refer to current time. Refer to step 6 for list of config upload files.

Step 3 If you don't see any file being uploaded from step 1, it is possible that the trap IP on the switch does not match the IP that is being used for node discovery. Or there is SNMP request failure. First check the trap IP. On the Cisco MGM, find the Managed IP that is used for node discovery by using Cisco MGM CLI "dbnds". Then use switch CLI "dsptrapip" to display the trap IP. If there is mismatch, use switch CLI "cnftrapip" to reconfigure the trap IP to the one that is used by Cisco MGM. See C.5.1.2 Network Setup and Configuration Required for OOEMC Sync Up Process.

Step 4 If the trap IP is not an issue, then check whether there is SNMP request failure. Normally, after node resync is triggered, OOEMC will send SNMP request to the switch to start configuration upload file creation. If the request fails, then OOEMC will retry SNMP request until it exceeds maximum retrials and declares node resync failure with node mode equal to 5. However, it shouldn't take very long to declare node resync failure because of the SNMP request failure. To verify that there is SNMP failure, you can start with ooemc log files and then proceed to check snmpcomm log files.

The child ID is calculated from the following formula remainder (NEDBACCSSID / No. of OOEMC child) + 1

The file name format of OOEMC log file is given as ooemc10.6568.log for example. The "10" in the example is the "child" ID, The "6568" in the examples is the OOEMC process ID which you can obtain by using typing "psg em" at Cisco MGM CLI.

The starting point of log file inspection is to grep "RESYNC" of the log file. The grep result should include node_id and node mode. Once you have locate the starting point in the file, open the file and read the content after this starting point in the file. More or less, the log messages in the file should provide you some information whether SNMP failure has occurred.

Step 5 Very often, the node mode 2 problem is caused by bulk file creation abort on the switch. Referring to the discussion in step 4, if there is no SNMP request failure, the switch should send traps 60901 and 60902 to OOEMC. Trap 60901 indicates that the switch will start bulk file creation, while trap 60902 indicates bulk file creation done. When OOEMC receives trap 60902, it will start FTP the bulk file which is shelf generic configuration file in this case. This is also the first file to be uploaded for every resync mode, whether it is coldstart, warm start or periodic resync. The commonly seen mode 2 problem is that the switch will abort the bulk file creation and send trap 60903 to Cisco MGM. Cisco MGM will reschedule the next SNMP request unless it exceeds maximum retrials. Whenever you find trap 60903 periodically in the log file, you should contact platform team to investigate the bulk file creation failure on the switch.

Step 6 To take CARD_01_CC.CF.10 as an example. This file is shelf generic file and is the first file to be uploaded after Cisco MGM has received 60902 trap from the switch. The "10" in the example is the node_id. If you find 60902 in the log file but no config file has been uploaded after a reasonable amount of time, it is possible that the FTP has failed. By greping "to ftp file" and the config file name, or just "FTP" from the log files, and by tracing the log messages in the log file, you should be able to tell whether or not FTP failure has occurred. For more detail information of SNMP request failure and FTP failure, inspect "snmpcomm" and "cwmftpd" log files Look into cwmftp.log and cwmftp.request_log. Search for the file name at the time the error happened in both files. The cwmftp.request_log gives the summary/final result of the FTP operation and any error is reported. The cwmftp.log shows the step by step details about the FTP operation.

Cisco MGM will upload and parse a set of config files from the switch. The following lists the files uploaded from MGX NE.It includes VISM, AXSM, VXSM, SRM, and RPM/RPM-PR cards:

1. CARD_01_CC.CF
2. SM_1_slot#.CF
3. SM_1_slot#.CS
4. SM_CARD_01_slot#.CF
5. SM_CONN_01_slot#.CF
6. SM_ALARM_01_slot#.CF
7. SM_CON_UPDATE_01_slot#.CF
8. SM_CARD_01_SRM.CF
9. SM_CARD_01_RPM.CF
10. PNNI_01_CC.CF

Files 1 and 2 are uploaded for each NBSM. Files 4 to 7 are uploaded for each AXSM. File 9 is uploaded for all RPM/RPM-PR cards on the switch.

The following list the files uploaded from MGX NE for VISM, AXSM, VXSM, SRM, RPM/RPM-PR, and RPM-XF cards:

1. CARD_01_CC.CF
2. SM_1_slot#.CF
3. SM_1_slot#.CS
4. SM_CARD_01_slot#.CF
5. SM_CONN_01_slot#.CF
6. SM_ALARM_01_slot#.CF
7. SM_CON_UPDATE_01_slot#.CF
8. SM_SC_slot#_transactionID_date.CF
9. SM_IC_slot#_transactionID_date.CF
10. SM_CARD_01_SRM.CF
11. SM_CARD_01_RPM.CF
12. PNNI_01_CC.CF

The different between these two lists is on the files uploaded for AXSM cards and RPM-XF card. For switch running 4.0 or above switch software, static file (SM_SC_slot#_transactionID_date.CF) and incremental file (SM_IC_slot#_transactionID_date.CF) are uploaded, but for switch running 3.0 or lower switch software, conn, alarm and conn update files are uploaded for each AXSM. Files 4 to 7 in the second list are uploaded for each RPM-XF card, and file 11 is uploaded for all RPM/RPM-PR cards on the switch.

Step 7 Another scenario that the node mode stays in 2 for very long time is because the parsing of one particular config upload file has taken very long time and has not completed yet. You can "tail" the ooemc log file by doing "tail -f ooemc_log_file" and get a feeling on what is going on with the parsing.

Defect Information—Collect ooemc log files, nts log files, snmpcomm log files, and cwmftpd log files under /opt/svplus/log.

Possible alternative workaround—None

C.5.1.5 Node Resync Mode is 5

Node syncup failure with mode 5

Step 1 Node mode 5 indicates that node resync fails. This could be caused by the config upload or parsing failure of shelf generic file (CARD_01_CC.CF.13 for example) or pnni file (PNNI_01_CC.CF.13 for example). For the upload issue, in ISS: Node Mode Remains in 2 we have touched on the "mode 5" issue. Refer to that section for more debugging information. In general, mode 5 signifies that problem has happened on one or more stages of the whole resync process. You can think of the resync process being composed of the following stages and each stage alone can lead to mode 5 problem:

1. OOEMC will trigger node resync.
2. OOEMC will send SNMP request to switch for bulk file creation
3. OOEMC will receive bulk file creation related traps: 60901, 60902, and 60903.

4. OOEMC will FTP config upload files from switch after it has received 60901 and 60902 from switch.
5. OOEMC will parse the config upload files
6. OOEMC will declare sync up done.

When mode 5 problem occurs on one of the nodes, you should ask yourself the following questions:

1. Is the problem caused by SNMP request? What can I do?

You can grep "RESYNC" from the ooemc log files. OOEMC will change node mode to 2 when it starts node resync. You should see something like the following from the log:

```
NOTICE: N17 <EMC_Node_c::InSync> SENDING RESYNC STATUS 2 FOR NODE 17 TO GUI - Node is
synchronizing.
```

This message tells you that OOEMC will start node resync for node with ID equal to 17 (N17). If you look further in the log, you should see log messages related to SNMP request and SNMP response. If the SNMP request is successful, the switch will responds to the request. The OOEMC will then process the SNMP response by invoking response function which may do nothing:

```
<EMC_SnmpFunc_c::ProcFunc_GenNodeBulkFile_1> entering
```

If the log messages indicate SNMP error, refer to snmpcomm log files for more failure information.

2. Is the problem caused by bulk creation traps? What can I do?

You can grep "60901", "60902", and "60903" from the log files. See C.5.1.3 Node Mode Remains in 1 for more information. Anyway, you should see something like the following:

```
INFO: <EMC_TrapClientImpl::onIncomingTrap> NTS NodeId 17 genericTrap 6 specificTrap 60901
INFO: <EMC_TrapClientImpl::onIncomingTrap> NTS NodeId 17 genericTrap 6 specificTrap 60902
```

3. Is the problem is caused by config file FTP? What can I do?

You can get "FTP" or "to ftp" plus config upload file name. You should see something like:

```
NOTICE: N17 <EMC_NodeFsmHandler_c::LoadShelf> to ftp /opt/svplus/tmp/CARD_01_CC.CF.17
INFO: <ParseFile_c::CheckFile> OOEMC9 CHECKSUM OK FOR FTP FILE
/opt/svplus/tmp/CARD_01_CC.CF.17
```

These messages indicate that FTP is successful and there is no checksum error in the file. Also from the log file, you should able to find out if there is FTP problem. Then you should refer to cwmftpd log files for more failure information.

4. Is the problem caused by shelf generic file or pnni file parsing? what can I do?

After you have located the starting pointing of checksum checking for shelf generic file (CARD_01_CC.CF.17 for example) or pnni file (PNNI_01_CC.CF.17 for example), continue to trace the log messages to see whether or not parsing error has occurred. If there is not error, you should see the following:

```
INFO: N17 <EMC_NodeFsmHandler_c::FinishShelf> Parse /opt/svplus/tmp/CARD_01_CC.CF.17
successfully.
```

Defect Information—Collect ooemc log files, nts log files, snmpcomm log files, and cwmftpd log files under /opt/svplus/log. Also collect config upload files in /opt/svplus/tmp

Possible alternative workaround—None

C.5.1.6 Cisco MGM DB Inconsistent With Switch Data After Successful Coldstart (Cisco MGM Server stop/start) or Periodic Resync

After successful node resync triggered by periodic resync, the Cisco MGM DB is found inconsistent with switch data.

Step 1 For this issues, what user can do is to collect ooemc log files and all config upload files for the node. OOEMC implement node based cache. User can dump and save the cache. First the user need to find out the process ID of the OOEMC process that manage the node by using the following commands:

The child ID is calculated from the following formula remainder (NEDBACCSSID / No. of OOEMC child) + 1

Save config upload files and ooemc log files.

Defect Information—Collect ooemc log files in /opt/svplus/log. Also collect all config upload files in /opt/svplus/tmp

Possible alternative workaround—User can manually resync the node. If the problem persists, user should try coldstart. If the problem is still not able to be resolved, collect log files and report the problem.

C.5.1.7 Cisco MGM CM GUI Shows Incomplete Connections After Successful Node Resync and Dbroker Sync Up

After EM node resync triggered by coldstart or periodic completes successfully and dbroker sync up also completes, the Cisco MGM CM GUI shows that some of connections are incomplete.

Step 1 For this issues, users have to determine which OOEMC process manages the node. OOEMC will manage the connection segment in Cisco MGM DB which terminates on the MGX. We have discussed in ISS: Node Mode Remains in 2 on how to find the child ID for the OOEMC process which manages your node. The purpose of finding the child ID of the OOEMC process is to find the correct OOEMC log files for inspection. The debugging process for this kind of issue mainly focuses on log files inspection.

Step 2 After you have identified the OOEMC log files, then grep "NotifyDataBroker" from the files to see some log message examples before you can modify your grep format to more efficiently grep the pair of log messages which corresponds to the local and remote ends of one end (master end point or slave end point) of a connection segment. In other words, each end (either master end or slave end) of a connection segment managed by OOEMC should be logged with one pair of messages: one for local end and one for remote end, and this pair of messages correspond to one atm_connection segment entry in DB for example. Now, you can verify the information that OOEMC sends to dbroker. DBROKER will base on these messages from OOEMC and constructs user_connection DB entry. Cisco MGM CM GUI will display connection with information from user_connection DB entry. Whether or not the connection will be displayed as complete or incomplete depends on the information in user_connection DB entry. Therefore, it is important to verify that OOEMC has sent correct information to DBROKER. Also verify that the segment DB entries are populated correctly.

Step 3 If you have made sure that correct number of messages have been forwarded to DBROKER and the data in the messages is correct, but the user_connection DB entry still contains invalid data, you should see C.15.2 Data Inconsistency for more debugging information, or contact DBROKER DE for further investigation. If the problem is due to wrong data populated in segment DB entries, then EM DE should look at the problem.

Defect Information—Collect ooemc log files and dbroker log files in /opt/svplus/log. Also collect config upload files in /opt/svplus/tmp

Possible alternative workaround—User can manually resync the node. If the problem persists, user should try coldstart. If the problem is still not able to be resolved, collect log files and report the problem.

C.5.1.8 Cisco MGM GUI Shows Mismatched Information Between GUI Views and DB Data

After OOEMC first time node resync such as coldstart, GUI views such as Network Monitor Tree View, Inspector View, Chassis View etc. display information which is not matched to newly provisioned or updated DB data. The problem persists even after each subsequent manual or periodic resync.

Step 1 For this issues, users have to determine which OOEMC process manages the node. We have discussed in ISS: Node Mode Remains in 2 on how to find the child ID for the OOEMC process which manages your node. The purpose of finding the child ID of the OOEMC process is to find the correct OOEMC log files for inspection. The debugging process for this issue mainly focuses on log files inspection.

Step 2 After first time node resync such as coldstart, OOEMC will start sending newly provisioned or updated DB data to NMServer. The current supported DB tables for NMServer message forwarding includes the following

- node
- card
- line
- ausm_port
- cesm_port
- frp
- rpm_port
- svc_port
- virtual_port
- aps
- ima_group
- ima_link
- linedistribution
- au4tug3
- controller
- license_in_use
- mfr_bundle
- mfr_link
- peripheral
- redundantcard
- sensor

Step 3 To determine whether or not OOEMC sends newly provisioned or updated DB data to NMServer, grep "ComposeNMSMsg" from OOEMC log files. The key words in log messages which correspond to the supported DB tables in "step 2" above are listed in the following:

- EMC_DBProperty_Node_c::ComposeNMSMsg
- EMC_DBProperty_Card_c::ComposeNMSMsg
- EMC_DBProperty_Line_c::ComposeNMSMsg
- EMC_DBProperty_AusmPort_c::ComposeNMSMsg
- EMC_DBProperty_CesmPort_c::ComposeNMSMsg
- EMC_DBProperty_FrPort_c::ComposeNMSMsg
- EMC_DBProperty_RpmPort_c::ComposeNMSMsg
- EMC_DBProperty_SvcPort_c::ComposeNMSMsg
- EMC_DBProperty_VtPort_c::ComposeNMSMsg
- EMC_DBProperty_Aps_c::ComposeNMSMsg
- EMC_DBProperty_ImaGroup_c::ComposeNMSMsg
- EMC_DBProperty_ImaLink_c::ComposeNMSMsg
- EMC_DBProperty_LineDist_c::ComposeNMSMsg
- EMC_DBProperty_AU4TUG3_c::ComposeNMSMsg
- EMC_DBProperty_Ctrlr_c::ComposeNMSMsg
- EMC_DBProperty_LicenseInUse_c::ComposeNMSMsg
- EMC_DBProperty_MfrBundle_c::ComposeNMSMsg
- EMC_DBProperty_MfrLink_c::ComposeNMSMsg
- EMC_DBProperty_Peripheral_c::ComposeNMSMsg
- EMC_DBProperty_RedCard_c::ComposeNMSMsg
- EMC_DBProperty_Sensor_c::ComposeNMSMsg

Step 4 Note that DB data will not be sent to NMServer during first time node resync such as coldstart. It is after first time resync that OOEMC starts sending updated or newly provisioned DB data to NMServer. Each OOEMC log message from grep will contain detail information for the identity of the NE object and the required fields from the corresponding DB table. The following is an example of NMServer message for line table:

```
ooemc10.24370.log.old.5:( 24370: 4) 23:15:17 INFO: N0:C7:B2:L2
<EMC_DBProperty_Line_c::ComposeNMSMsg> (MODIFY::LINE) aNMSEvent.node:0 type:4 subType:1
lpbkType:1 alarmState:1 adminState:1 sectStatus:6 pathState:2
```

In this example, the identity of the NE object is N0:C7:B2:L2 which is the line with node id = 0, slot = 7, bay = 2, and line# = 2. The DB operation is update. The rest of the message shows the values of the required fields from the line table.

Step 5 If grep returns log messages which indicate matched data, then you need to continue investigation on NMServer. See C.6.1 Cisco MGM Configuration Center, Chassis View, Diagnostic Center or Statistics Report Basics which describes the "nmController".

Defect Information—Collect ooemc and NMServer log files from /opt/svplus/log.

Possible alternative workaround—User can manually resync the node. If the problem persists, user should try coldstart. If the problem is still not able to be resolved, collect log files and report the problem.

C.5.2 Cisco MGM DB and Switch Data Inconsistency Issues After Node Provisioning for MGX

This section includes the following information:

- C.5.2.1 DB Table Population Through Traps and SNMP Upload
- C.5.2.2 Switch Data Does Not Match With Cisco MGM DB Table After Node Provisioning

C.5.2.1 DB Table Population Through Traps and SNMP Upload

Except for node and/or card resync, another mechanism that Cisco MGM OOEMC uses to populate the DB table entries is through trap processing and followed by snmp upload if necessary. User can provision the switch through switch CLI, Cisco MGM GUI or Cisco MGM service agents. All three cases will involve trap processing and snmp upload on OOEMC. Only connections can be provisioned by Cisco MGM CM GUI. Other provisioning such as line, port etc. have to go Cisco MGM service agents. Of cause, switch CLI can do both.

C.5.2.2 Switch Data Does Not Match With Cisco MGM DB Table After Node Provisioning

After switch provisioning through switch CLI, Cisco MGM GUI or Cisco MGM service agent, the switch data does not match to Cisco MGM DB.

Step 1 If the issue is caused by trap, for example, if user provisions a connection on a switch or through Cisco MGM GUI or service agent, and the Cisco MGM does not populate the DB entry or the information in the DB entry does not match with switch data, it is possible that the trap is not received by Cisco MGM. Or the trap is received by Cisco MGM, but it is buffered in the trap queues of OOEMC and the processing of the trap will be delayed. On the other hand, if the data in Cisco MGM DB is not correct, it is also possible that the SNMP upload fails to upload correct data. In any case, we need to study the log files and understand the root cause of the inconsistency problem.

Step 2 There are some key words in ooemc log files that you can grep and determine whether or not trap is received and processed. For example, to find out the channel traps from node_id=4, slot = 6, vpi = 1 and vci = 326, you can grep "TRAPLIST" as shown in the following:

```
cwmult60% grep "TRAPLIST: N4:" ooemc* | grep "Channel Trap" | grep "C6" | grep "vpi 1 vci
326"
ooemc10.5760.log.old.55:( 5760: 10) 23:21:12 INFO: TRAPLIST: N4: Channel Trap 60310 from
C6 B2 L1 P20 Ch299 ifIndex 17176597 vpi 1 vci 326 upCntr 0 vpcFlag 2 operS 1 alarm 67
ooemc10.5760.log.old.55:( 5760: 10) 23:21:12 INFO: TRAPLIST: N4: Channel Trap 60310 <
PROCESSED > from C6 B2 L1 P20 Ch299 ifIndex 17176597 vpi 1 vci 326 upCntr 0 vpcFlag 2
operS 1 alarm 67
ooemc10.5760.log.old.73:( 5760: 10) 23:23:48 INFO: TRAPLIST: N4: Channel Trap 60310 from
C6 B2 L1 P20 Ch299 ifIndex 17176597 vpi 1 vci 326 upCntr 0 vpcFlag 2 operS 1 alarm 66
```

For other kinds of traps, you can use the following key words to supplement "TRAPLIST" in your grep statement:

1. Port Trap
2. RscPart Trap
3. Svc Trap
4. SonetLn Trap
5. SctCard Trap
6. SonetPath Trap
7. FunMod Trap
8. LineMod Trap
9. RedCard Trap
10. TrapMiss Trap
11. VsiCtrlr Trap
12. DS3Line Trap
13. AtmPhy Trap
14. Peripheral Trap
15. CoreSwth Trap
16. TrapLost Trap
17. AtmAddr Trap
18. Restart Trap
19. Node Trap
20. SonetAps Trap
21. LMIPort Trap
22. Pnni IF Trap
23. Bulkfile Trap
24. Vism Trap
25. Vism Ann Trap
26. SubIf Trap
27. NBSMCnfg Trap
28. NBSMChan Trap
29. NBSMLine Trap
30. AusmLine Trap
31. AusmPort Trap
32. AusmChan Trap
33. AusmIma Trap
34. FrChan Trap
35. FrPort Trap
36. CesmPort Trap

37. CesmChan Trap
38. HsFrPort Trap
39. HsFrChan Trap
40. LineDist Trap
41. DS3Path Trap
42. Chan Upload
43. Party Trap
44. PrefRoute Trap
45. CardIma Trap
46. DS1 Line Trap
47. SctPort Trap
48. SvcDerouteGroomTrap
49. Channel Trap
50. TUG3Path Trap
51. Cug Trap
52. AddrCug Trap
53. RSC Upload
54. APS Upload
55. FrPort State Upload
56. MPSM Upload
57. Vism ToneDetect Trap
58. License Trap
59. PortAtmIf Trap
60. VxsmPvcRed Trap
61. ChanProt Trap
62. VxsmGwDsp Trap
63. VxsmGwIp Trap
64. VxsmGw Trap
65. VxsmSysRes Trap
66. VxsmGw1 Trap
67. VxsmMgc Trap
68. VxsmMgcIp trap
69. VxsmMgcGrpParam Trap
70. VxsmMgcGrpMgc Trap
71. VxsmMgcGrpProt Trap
72. VxsmAal2Prof Trap
73. VxsmCodec Trap
74. VxsmSvc Trap

75. VxsmAal2CrossConn Trap
76. VxsmAal25DataProfileTrap
77. VxsmSensor Trap
78. VxsmSensorThrhd Trap
79. VxsmModule Trap
80. DS0Grp Trap
81. VxsmAnnounce Trap
82. VxsmAudioFile Trap
83. VxsmDs0XConn Trap
84. VxsmMegaco Trap
85. VxsmCrr Trap
86. VxsmTone Trap
87. VxsmAs Trap
88. VxsmAsp Trap
89. VxsmAs Trap
90. VxsmLapd Trap
91. VismABCDBitTemplate Trap

Of cause, you may need to study the log messages with "TRAPLIST" and decide how you can grep the messages for your need. In the above example, there is another key word "PROCESSED" which indicates that the trap has been processed. This gives you the starting point in the log file so that you can study the log messages. if the DB is not populate correctly, then the subsequent log messages in the log messages should provide you information on DB inconsistency problem. Some trap processing may invoke SNMP data upload. From the log messages, you can verify whether or uploaded data is correct. Other possible reasons for DB inconsistency are:

1. SNMP upload failure and maximum retrials exceeded, SNMP timeout, or throttle error. You can verify the problem in snmpcomm log files
2. DB operation error. You can verify the problem in ooemc log files

If you do not know exactly what traps sequence is sent by switch to Cisco MGM, you should try a working scenario and study the log for the trap sequence, or you can use HPOV to determine the trap sequence.

Step 3 The previous step takes care of the cases that trap has been received and processed. The grep in the previous step also allow you to find out whether traps have been received and has been buffered in the trap queues, or related traps are not received at all. For the latter case, you need to refer to NTS logs to verify whether traps have been received by NTS from switch and forwarded by NTS to OOEMC. If the trap has been buffered in trap queue, the possible reasons are:

1. Node is syncing due to regular node resync or due to -2 trap.
2. Card is syncing and the trap is related to the card. The traps will buffered in queue until card resync completes.
3. Summary alarm trap is processed. Summary alarm is being uploaded or parsed. You can grep the log files for information related to summary alarm traps

To verify that the trap has been put into queue, you can do the following

```
grep EMC_TrapQueue_c::append ooemc_log | grep trap_num
```

You should see something like the following:

```
INFO: <EMC_TrapQueue_c::append> entering. ======> append trap# 60303 to trap queue;
getHdlrLevel=5, getTrapLevel=5, #=174
```

Defect Information—Collect ooemc log files, nts log file, and snmpcomm log files under /opt/svplus/log.

Possible alternative workaround—User can manually resync the node. If the problem persists, user should try coldstart. If the problem is still not able to be resolved, collect log files and report the problem.

C.6 Configuration Center, Chassis View, Diagnostic Center and Statistics Report Problems

This section includes the following information:

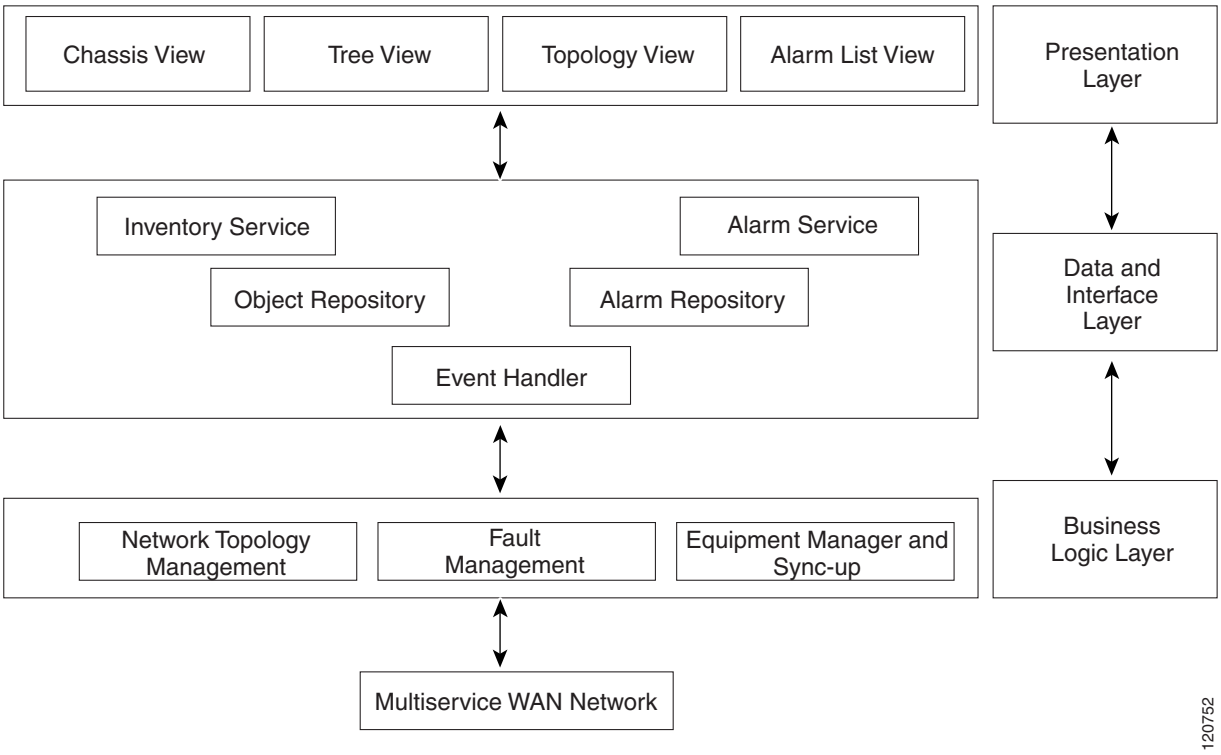
C.6.1 Cisco MGM Configuration Center, Chassis View, Diagnostic Center or Statistics Report Basics

Cisco MGM manages MGX NEs. The Topology module discovers the nodes and trunks. Once the nodes are discovered, the EM module syncs up with the nodes to discover the card, line, port, etc. All the discovered nodes, trunks and its elements are published by NMServer, which in-turn are displayed in the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs. The Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs have Tree View, Inspector View. The Tree View and Inspector View are shared by Configuration Center, Diagnostic Center, Finder, Statistics Report and Chassis View GUIs. The Tree View and InspectorView feed-off the data published by NMserver.

Cisco MGM is notified of all subsequent changes in the network through traps.

Figure C-1 shows the end-to-end architecture.

Figure C-1 Cisco MGM End-to-End Architecture



NMServer provides Inventory and alarm information for Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs. The node information is pushed by topod to NMServer. The initial inventory of card, lines, ports, etc., is read from the database. The dynamic updates are pushed to NMServer from topod, ooemc and sdbroker.

There are two utilities under /opt/svplus/util/ directory which are shipped with Cisco MGM to debug issues in NMServer:

- nmControl—This utility provides means to check the NMServer cache and its state. It allows the following operations. Output is redirected to /opt/svplus/log/nmControl.log. Cache dumps are redirected to /opt/svplus/log/nmControl.dump. All the listed operation are non-destructive and they perform the tasks in a passive mode. Do not use Option 2 (to dump all the cache_ for a large network which has more than 1000 nodes.

  MGM% nmControl:

  - Resync Node—Resyncs the node (specified by the node_id).
  - All Cache—Dumps all the data in its cache to the dump file.
  - Topology Cache—Dumps Topology (node) data to the dump file.
  - Node Cache—Dumps a node's data (specified by node_id) to the dump file.
  - MGM Alarm Cache—Dumps the Cisco MGM specific alarms to the dump file.
  - ClientManager Cache—Dumps the information about all the Clients to the dump file.
  - Error Statistics—Dumps the error information associated with the sync-up to the dump file
  - Syncup Status—Dumps the sync-up state to the dump file
  - Configuration—Dumps the Configuration data to the dump file

- nmClient—This utility is used to isolate an issue between client and server. It is used to query the NMServer the same way as the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI queries the Server. It allows the following operations. Output is redirected to /opt/svplus/log/nmClient.log. Cache dumps are redirected to /opt/svplus/log/nmClient.dump.

  The user has to first register with the Server (Option 1), before performing other operations. Like-wise, when the user is done using the client, unregister the Client (Option 3).

  MGM% nmClient:

  - Register Client—Registers with the Server
  - Update Filter—Updates the subscription/filter with the server passing the FDN
  - Unregister Client—Unregisters with the Server
  - Get Topology—Get the Topology Information of Networks and Nodes
  - Get Children—Get the list of children for a particular object in the tree.
  - Get CwmInfo—Get the Cisco MGM sync-up state information
  - Get ManagedObject—Get the detailed information about an object in the tree.
  - Subscribe for all events—Subscribe for all updates from the Server
  - Unsubscribe for all event—Unsubscribe for all updates from the Server

The GUI Client's log files (CMSCclient.log) are saved under log dir in the user's home directory. For example, in Windows, D:Documents and Settings\<userId>\log\, or in Unix: /opt/svplus/log

C.6.2 Basic Issues

This section includes the following information:

C.6.2.1 Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs Do Not Show Any Nodes

No nodes show in the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

Step 1 Check whether the nodes are discovered. See C.4.2.1 No Nodes Are Discovered.

Step 2 Check whether NMServer has the nodes and trunks in its cache. This can be done by using the command nmControl (Option 3) on the Cisco MGM CLI.

Step 3 If the node(s) are in NMServer cache, open a new GUI and verify whether the node(s) are shown in the new GUI.

Defect Information—Collect the following information for further analysis:

- Collect topod.log, ILMITopoc.log, NMServer.log
- Collect nmControl.dump for option 3.
- Collect CMSCclient.log

Possible alternative workaround—Open a new GUI and a new Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI.

C.6.2.2 Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs Are Unable to Connect to Server

Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI is unable to connect to Server.

Step 1 Check whether the client registers in NMServer.log.

Step 2 Enable orbix logs by creating orbix dir in /opt/svplus/log/ dir.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log, NMServer.log
- Collect Orbix logs for NMServer.

Possible alternative workaround—None.

C.6.2.3 Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs Do Not Show a Newly Added Node

A newly added node is not shown in the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

Step 1 Check whether the nodes are discovered. See C.4.2.1 No Nodes Are Discovered.

Step 2 Check whether NMServer has the nodes in it's cache.

This can be done by using the command nmControl (Option 3) on the Cisco MGM CLI.

Step 3 If the node(s) are in NMServer cache, Open a New GUI and verify whether the node(s) are shown in the new GUI.

Defect Information—Collect the following information for further analysis:

- Collect topod.log, ILMITopoc.log, NMServer.log
- Collect nmControl.dump for option 3.
- Collect CMSCclient.log

Possible alternative workaround—Open a new GUI.

C.6.3 Topology Discovery Issues

This section includes the following information:

C.6.3.1 Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs Do Not Show a Node

A node is not shown in the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

Step 1 Check whether the nodes are discovered. See C.4.2.1 No Nodes Are Discovered.

Step 2 Check whether NMServer has the nodes in it's cache.

This can be done by using the command nmControl (Option 3) on the Cisco MGM CLI.

Step 3 If the node/trunk(s) are in NMServer cache, Open a New GUI and verify whether the node are shown in the new GUI.

Defect Information—Collect the following information for further analysis:

- Collect topod.log, ILMITopoc.log, NMServer.log
- Collect nmControl.dump for option 3.
- Collect CMSCclient.log

Possible alternative workaround—Open a new GUI and a new Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

C.6.3.2 Node Information Incorrect on Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs

The node information like node name, IP Address, alarm state, etc., of a node shows incorrectly on the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

Step 1 Check the node information in database using selnd command.

Step 2 Check the node information in NMServer's cache.

This can be done by using the command nmControl (Option 3) on the Cisco MGM CLI.

Step 3 Check the CMSCclient.log for the node information.

Step 4 Using nmClient, use getTopology option to retrieve the node information and verify whether it matches with database and the GUI.

Step 5 If the node information is correct in NMServer cache, Open a New GUI and verify whether the node is shown correctly in the new GUI.

Defect Information—Collect the following information for further analysis:

- Collect topod.log, ILMITopoc.log, NMServer.log
- Collect selnd o/p
- Collect nmControl.dump for option 3.
- Collect CMSCclient.log

Possible alternative workaround—Open a new GUI and a new Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI.

C.6.3.3 Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI Shows a Node That Is Not in the Network

The Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI shows a node that is not part of the network anymore.

Step 1 Check the node information in database by querying the node, packet_line table. Verify whether the node is active.

Step 2 If the node is active, see C.4.2.1 No Nodes Are Discovered.

Step 3 Check the node in NMServer's cache.

This can be done by using the command nmControl (Option 3) on the Cisco MGM CLI.

Step 4 Check the CMSCclient.log for the node/trunk.

Verify whether a delete message was received for the node.

Step 5 Using nmClient, use getTopology option to retrieve the node information and verify whether it matches with database and the GUI.

Step 6 If the node is not present in NMServer cache, Open a New GUI and verify whether the node is shown in the new GUI.

Defect Information—Collect the following information for further analysis:

- Collect the ILMITopoc.log, topod.log, NMServer.log
- Collect the dump outputs of ILMITopoc, topod and NMServer. The dump can be captured by issuing a kill -USR1 signal to the process.
- Collect the output of the switch CLI, selnd and dbnds.

Possible alternative workaround—None

C.6.3.4 Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI Shows Incorrect SyncState for a Node

The Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI shows incorrect SyncState for a node.

Step 1 Check the node information in database by querying the node table.

This can be done by using the command selnd on the Cisco MGM CLI. Check the status

Step 2 Check the node in NMServer's cache.

This can be done by using the command nmControl (Option 3) on the Cisco MGM CLI.

Step 3 Check the CMSCclient.log for the node.

Verify whether the correct message was received for the node.

Step 4 Using nmClient, use getTopology option to retrieve the node information and verify whether it matches with database and the GUI.

Defect Information—Collect the following information for further analysis:

- Collect the ILMITopoc.log, topod.log, NMServer.log
- Collect the dump outputs of ILMITopoc, topod and NMServer. The dump can be captured by issuing a kill -USR1 signal to the process.
- Collect the output of the switch CLI, selnd and dbnds.

Possible alternative workaround—None

C.6.3.5 Duplicate Nodes Are Displayed on Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs

Duplicate Nodes Displayed on Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

Step 1 Check whether node table has duplicate node id.

The node table can be queried using the below command.

tballraker18% echo "select * from node where node_id=2 and slot=1" | dbaccess stratacom

Step 2 Check whether both nodes in database have active =1. If only both are active then collect the logs.

Step 3 If duplicate nodes do not exist in database, then check the cache of NMServer using nmControl (Option 3).

Step 4 Check the CMSCclient.log for the node.

Step 5 Using nmClient, use getTopology option to retrieve the node information and verify whether it matches with database and the GUI.

Step 6 If duplicate nodes is not present in NMServer cache, Open a New GUI and verify whether the node is shown in the new GUI.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under /opt/svplus/log. For PC Client, collect CMSCclient.log file under D:\Documents and Settings\<username>\log.
- Collect node data from node table for that specific node.
- Collect ILMITopoc.log, topod.log need to be collected if there are duplicate nodes in database.

Possible alternative workaround—None

C.6.4 Network Element Discovery Issues

This section includes the following information:

C.6.4.1 All the Cards Under a Node Are Missing

No Cards are shown under a node in the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

Step 1 Check whether the node is synced up.

This can be done by using the command selnd on the Cisco MGM CLI.

Step 2 If the node has not synced up, then wait for the node to sync-up.

Step 3 If the node has synced up, then check whether cards are populated in the card table. If the Card table is empty, Collect the EM logs. See C.5 Equipment Management Problems.

Step 4 Check whether NMServer has cards in it's cache.

This can be done by using the command nmControl (Option 4) on the Cisco MGM CLI.

Step 5 If cards are not present in NMServer cache, collect the logs.

Step 6 If cards are present in NMServer cache, use nmClient and verify whether getChildren for node's FDN, returns the cards in the nmClient.<pid>.dump file.

Step 7 If cards are present in NMServer cache, Open a New GUI and verify whether the cards are shown in the new GUI.

Defect Information—Collect the following information for further analysis:

- Collect topod.log, ILMITopoc.log, NMServer.log
- Collect nmControl.dump for option 4.
- Collect CMSCclient.log

Possible alternative workarounds:

1. Open a new GUI and a new Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI.
2. Use nmControl and perform "Resync Node" specifying the node id.

C.6.4.2 Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs Do Not Show a Card/Line/Port for a Node

A card/line/port etc. for a node is not shown the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

Step 1 Check whether the node is synced up.

This can be done by using the command selnd on the Cisco MGM CLI.

Step 2 If the node has not synced up, then wait for the node to sync-up.

Step 3 If the node has synced up partially, check whether card/line/port are populated in the database. Refer to the DB Schema Doc.

Step 4 If the entry is not populated in the database, see C.5 Equipment Management Problems.

Step 5 If entry is present in the database, check the NMServer cache.

This can be done by using the command nmControl (Option 4) on the Cisco MGM CLI. Check the nmControl.<pid>.dump

Step 6 If element is present in NMServer cache, use nmClient and verify whether getChildren for FDN, returns the entities in the nmClient.<pid>.dump file.

Step 7 If element is present in NMServer cache, Open a New GUI and verify whether the missing elements are shown in the new GUI.

Defect Information—Collect the following information for further analysis:

- Collect topod.log, ILMITopoc.log, NMServer.log
- Collect nmControl.dump for option 4.
- Collect CMSCclient.log

Possible alternative workarounds:

1. Open a new GUI and a new Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI.
2. Use nmControl and perform "Resync Node" specifying the node id.

C.6.4.3 Card/Line/Port Information Incorrect on Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs

The entity information like type, alarm state, etc., of an element shows incorrectly on the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUIs.

Step 1 Check whether the node is synced up.

This can be done by using the command selnd on the Cisco MGM CLI.

Step 2 If the node has not synced up, then wait for the node to sync-up.

Step 3 Check whether card/line/port are populated in the database. Refer to the DB Schema Doc.

Step 4 If the entry in the database matches the GUI, see C.5 Equipment Management Problems.

Step 5 If entry doesn't match with the database, check the NMServer cache.

This can be done by using the command nmControl (Option 4) on the Cisco MGM CLI. Check the nmControl.<pid>.dump

Step 6 Use nmClient and verify whether getChildren for FDN, returns the correct information for the element in the nmClient.<pid>.dump file.

Step 7 If element is present in NMServer cache, Open a New GUI and verify whether the missing elements are shown in the new GUI.

Defect Information—Collect the following information for further analysis:

- Collect topod.log, ILMITopoc.log, NMServer.log
- Collect nmControl.dump for option 4.
- Collect CMSCclient.log

Possible alternative workarounds:

1. Open a new GUI and a new Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI.
2. Use nmControl and perform "Resync Node" specifying the node id.

C.6.4.4 Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI Shows a Card/Line/Port That Is Not Present in a Node

The extra card/line/port etc. element is shown incorrectly on the Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI.

Step 1 Check whether the node is synced up.

This can be done by using the command selnd on the Cisco MGM CLI.

Step 2 If the node has not synced up, then wait for the node to sync-up.

Step 3 Check whether card/line/port are populated in the database. Refer to the DB Schema Doc.

Step 4 If the element is present in the database matches the GUI, see C.5 Equipment Management Problems.

Step 5 If element is not in the database, check the NMServer cache.

This can be done by using the command nmControl (Option 4) on the Cisco MGM CLI. Check the nmControl.<pid>.dump

Step 6 Use nmClient and verify whether getChildren for FDN, returns the element in the nmClient.<pid>.dump file.

Step 7 If element is not present in NMServer cache, Open a New GUI and verify whether the extra element is shown in the new GUI.

Defect Information—Collect the following information for further analysis:

- Collect topod.log, ILMITopoc.log, NMServer.log
- Collect nmControl.dump for option 4.
- Collect CMSCclient.log

Possible alternative workarounds

1. Open a new GUI and a new Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI.
2. Use nmControl and perform "Resync Node" specifying the node id.

C.6.5 Configuration Center, Chassis View, Diagnostic Center or Statistics Report GUI Alarm Issues

This section includes the following information:

C.6.5.1 Alarm Processing Basics

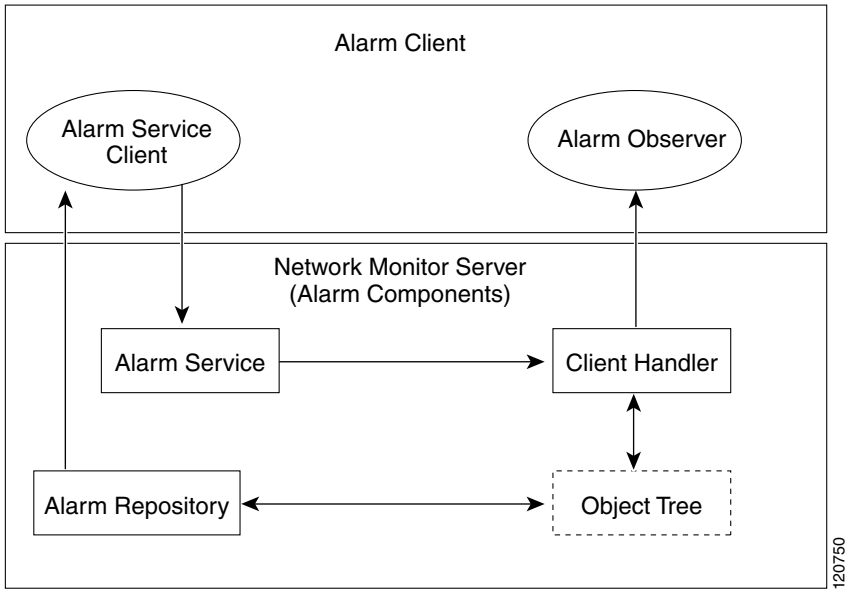
Alarm processing is done within the NMServer processes. Following are some vital points with regard to alarm processing:

1. Alarm rules are defined in an XML file (/opt/svplus/xml/ruledata.xml). For details on 'XML schema on alarm rules, see Figure C-2.
2. GUI clients register for alarms by providing the parent FDN
3. GUI clients pull initial alarms from NMServer. After initial pull of alarms, all alarms are pushed to registered clients by NMServer when alarms occur
4. Object severity for any and all network elements is determined by the XML alarm rule
5. Administrative states of network element states are not displayed in alarm list, only alarm states.

6. Alarm List displays mostly active alarms, however some 'Events' are also displayed. For details on 'Events vs. Alarms' see Figure 7.5.2, "INF: XML Schema for alarm rules," on page 153.
7. Some alarms result in the network element having a different alarm severity then the actual alarm. For details on 'Object Severity vs. Alarm Severity' see Figure 7.5.3, "INF: Alarm Severity vs. Object Severity," on page 156.

Alarms for various network elements are stored in memory cache in the NMServer Object Tree. GUI clients register for alarms from NMServer by providing the FDN of the network element for which they would like alarms for. All alarms for network elements under the FDN registered will be send if the parent FDN is registered. GUI clients may also update alarms, such as flag an alarm as acknowledged, or manually clear an alarm. These updates are done via the 'Alarm Repository' component of NMServer. Figure C-2 illustrates the client/server architecture for alarm components in NMServer.

Figure C-2 Client/Server Architecture for Alarm Components



C.6.5.2 XML Schema for Alarm Rules

Alarm rules are defined in XML, specifically a file named $HOME/xml/ruledata.xml. These alarm rules are read once when NMServer starts. When events are processed, the rules are queried from memory to determine what action with regard to alarms, should be taken on the event. There are 3 types of alarm rules defined in the XML schema: Correlated, Correlated Bitmap, and Transient. Specifics on each of these three types follows.

1. Correlated Alarm Rule Type

The correlated alarm rule type is the most common in ruledata.xml. This rule is used when a network element can only be in one of many states at any one time. If the entity were to change states, then the previous alarm state would be cleared. Most network elements managed by Cisco MGM fall into this category. A simple example is DB SyncUp status of a node. The syncup status can be one of 'Partial Syncup', 'Syncup Failed', or 'In Sync'. Any one of these states correlates out any other. See Figure C-3.

Figure C-3 Correlated Alarm Rule Diagram

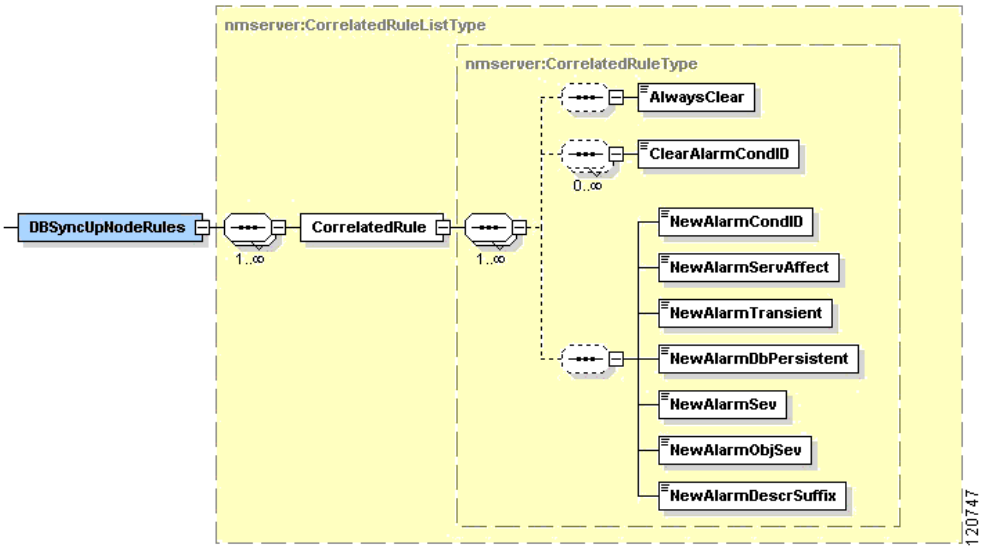


Figure C-3 XML annotation can be read as follows. A CorrelatedRule can have any of the following:

- 1 AlwaysClear (Used when a given element never has an alarm, such as top level Network)
- 0 or more ClearAlarmCondIds
- 1 New Alarm (which consists of NewAlarmConditionID, NewAlarmServAffect, etc.)

2. Correlated Bitmap Alarm Rule Type

The Correlate Bitmap alarm rule type is different then the correlated alarm rule type because the bitmap rule type can represent many states an entity can be in at any one particular time. The correlated bitmap rule type is used primarily to represent line alarms. Lines can have many different alarms associated with them at any given time, such as 'Loss of Signal', and 'Loss of Frame'. See Figure C-4.

Figure C-4 Correlated Bitmap Alarm Rule Diagram

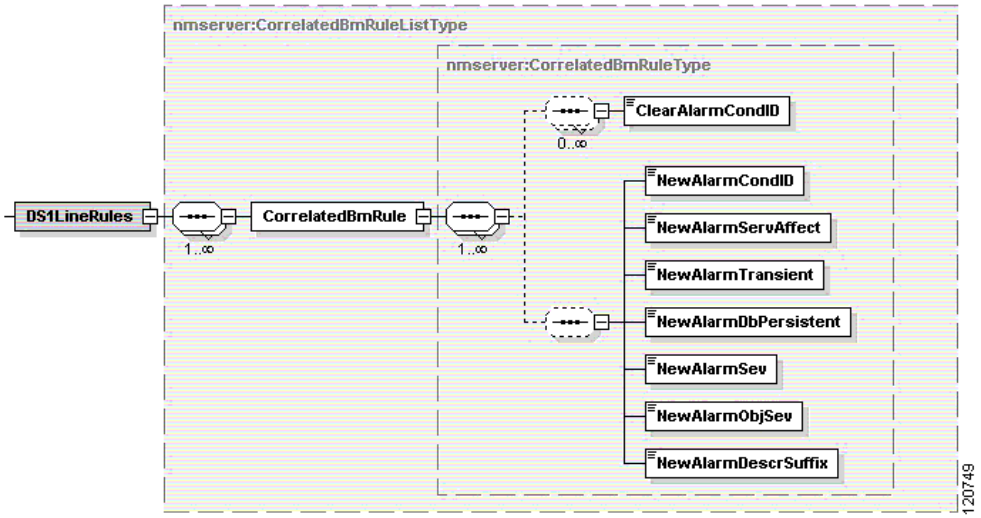


Figure C-4 XML annotation can be read as follows. A CorrelatedBmRule can have any of the following:

- 0 or more ClearAlarmCondIds
- 1 New Alarm (which consists of NewAlarmConditionID, NewAlarmServAffect, etc.)

3. Transient Alarm Rule Type

The Transient Alarm rule type is used to distinguish events vs. alarms. Alarm List does show some events. Events are normally associated with the NMS itself. Examples of events are 'Process restarted' or 'Primary Gateway disconnected'. These are NMS events that are not correlated, but are displayed in the alarm list. Another example of a transient event that is not related to the NMS is a card switchover. If APS is enabled on a card and there is an APS switchover, an event will be displayed in the alarm list. The primary distinction between 'Transient' Events and 'Correlated' Alarms is Transient events are not cleared by the network, whereas correlated alarms are. See Figure C-5.

Figure C-5 Transient Alarm Rule Diagram

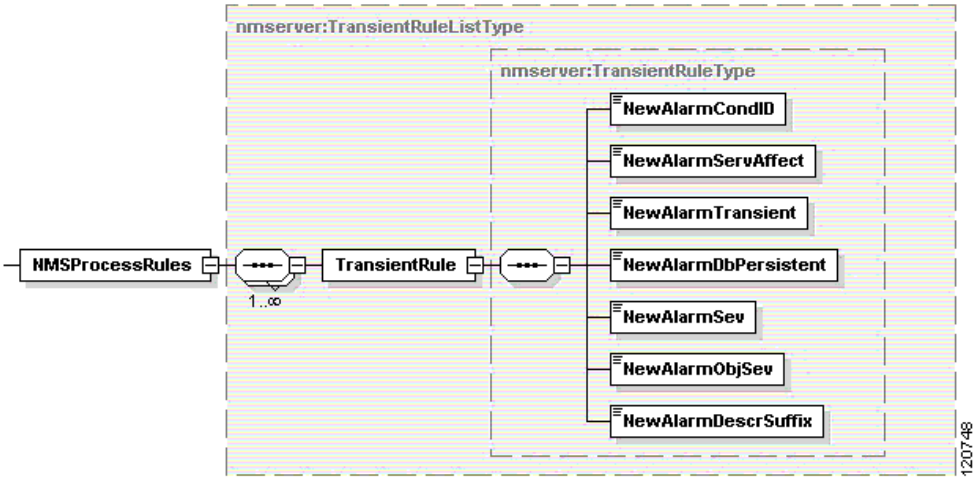


Figure C-5 XML annotation can be read as follows. A Transient can only one a New Alarm associated with it. Note, there are no 'ClearAlarmCondID' associated with a Transient rule. Transient alarms are either manually cleared by the user, cleared by the same transient alarm occurring twice, or purged by NMServer when a high threshold is hit.

C.6.5.3 Alarm Severity and Object Severity

There are two severities assigned to every alarm in alarm rules XML file. The two severities are called 'Object' and 'Alarm' severity. These severities do match for most alarms. There are some cases however, where these severities are different. Below is an example of XML alarm rule where object and alarm severity do not match:

```
<CorrelatedRule State="1 -1">
<ClearAlarmCondID>10302</ClearAlarmCondID>
<ClearAlarmCondID>10303</ClearAlarmCondID>
<ClearAlarmCondID>10304</ClearAlarmCondID>
<NewAlarmCondID>10301</NewAlarmCondID>
<NewAlarmServAffect>0</NewAlarmServAffect>
<NewAlarmTransient>0</NewAlarmTransient>
<NewAlarmDbPersistent>0</NewAlarmDbPersistent>
```

```
<NewAlarmSev>6</NewAlarmSev>
<NewAlarmObjSev>7</NewAlarmObjSev>
<NewAlarmDescrSuffix>Sync-Up has not started yet</NewAlarmDescrSuffix>
</CorrelatedRule>
```

This alarm will occur if the southbound processes (EMs) send a node message with EM syncup status as 1 or -1. If that does occur, then the node should be unreachable severity (value 7) in the tree view. Note there is no 'unreachable' severity in the alarm list. This is why we have two severities for each alarm. There is no such alarm severity as 'unreachable' in the alarm list. Unreachable alarms have 'Critical' (value 6) severity in the alarm list.

Another instance when 'Alarm' and 'Object' severity do not match is for 'Aggregate Port' alarms. Aggregate port alarms are alarms that summarize the condition of the connections on the port. Since these alarms should not effect the severity of the port, the object severity of these is alarms is 'Clear' (value 3). Following is the XML for an aggregate port alarm:

```
<CorrelatedBmRule StateBm="1">
<NewAlarmCondID>40801</NewAlarmCondID>
<NewAlarmServAffect>0</NewAlarmServAffect>
<NewAlarmTransient>0</NewAlarmTransient>
<NewAlarmDbPersistent>1</NewAlarmDbPersistent>
<NewAlarmSev>5</NewAlarmSev>
<NewAlarmObjSev>3</NewAlarmObjSev>
<NewAlarmDescrSuffix>Aggregate Port alarm, One or more connections on this port are in
primary failure</NewAlarmDescrSuffix>
</CorrelatedBmRule>
```

Note the alarm severity ('NewAlarmSev' tag) is 'Major' (value 5).

C.6.5.4 Severity Shown on Tree View Does Not Match Severity Shown on Platform

Severity of network element in tree view does not match the severity the switch is showing for the same network element.

Step 1 Verify customer is comparing the correct severity icon

- **a.** There are two severities associated with every object in the tree view, the Aggregate severity and the Self severity. The aggregate severity is on the left, the Self severity is on the right. Since the switch does aggregation of many faults, the customer should compare the aggregate severity of the object in tree view with the severity of the switch.
- **b.** If the customer is looking at the correct severity icon and there is still a discrepancy between the severities, continue to Step 2.

Step 2 Verify whether Cisco MGM has synced up with the node.

- **a.** Login to Cisco MGM server and type 'selnd'
- **b.** Verify the mode of the node in question is 3

Step 3 If the mode is 3, continue to Step 4.

Step 4 Verify whether discrepancy is caused by aggregated connection alarms

a. NMServer does more aggregation of alarms then the platform. For instance, NMServer aggregates connection alarms up the port and the switch does not. Therefore, if the tree view displays a higher severity then the switch, it maybe caused by one or more aggregated port alarms.

b. Right click the NE (network element) in the tree view and choose 'show alarms'. All of the alarms for this NE and its children should display in the alarm list.

c. Filter on the alarms that are greater severity then what the platform is showing

d. Are these alarms 'Aggregate Port' alarms? If so, this is expected behavior and there is no defect. If there are alarms that are greater severity then what is shown on the platform, and they are not 'Aggregate Port' alarms, continue to next step to troubleshoot whether the alarm is in DB.

Step 5 Verify whether DB has correct alarm state. Refer to the DB schema document for information on what table to lookup for this particular entity type.

Defect Information—Collect the following information for further analysis:

- Collect NMServer.log
- Collect nmControl.dump for option 3.
- Collect CMSCclient.log on client machine.

Possible alternative workaround—Open a new GUI and a new Cisco MGM MGXNE Specific GUI (CC,DC,CV,SRT)

C.6.5.5 Alarm List Shows Alarm That Does not Exist on Platform

There are several alarms that are correlated by NMServer and are not handled by the switch. This is the case because the NMS keeps track of alarm conditions that may not be relevant to the switch alone, but are relevant to the switch + the NMS. One example of such an alarm is the node syncup state. The switch itself is not interested in the fact that the NMS may not be synced up with it, but the NMS is interested in this information. Therefore if the node is still syncing up with the NMS, an alarm will be displayed for this node in Alarm List, but there will not be such an alarm on the platform. Below is a summary of alarms that may be seen in the Alarm List, but not seen on the platform.

Step 1 If there exists an alarm in the alarm list, and not on the platform, check if the suspect alarm is included in the following list:

1. Node Syncup status alarms
2. Node DB Syncup status alarms
3. Node Management State status alarms
4. Node Aggregate alarm status
5. Link0/Link1 Node alarms
6. Card Syncup status alarms
7. Aggregate Port (Connection) alarms

Step 2 If the suspect alarm is not in the list above, and it is displayed in the alarm list and not on the platform, it may be defect. See below for troubleshooting further

a. Verify whether DB has correct alarm state, refer to the DB schema document for information on what table to lookup for this particular entity type.

b. Collect the information requested in Defect information section.

Defect Information—Collect the following information for further analysis:

- Collect topod.log, linktopoc.log, ILMITopoc.log, NMServer.log, fileTopoc.log
- Collect nmControl.dump for option 3.
- Collect CMSCclient.log

Possible alternative workaround—Open a new GUI and a new Cisco MGM MGXNE Specific GUI (CC,DC,CV,SRT)

C.6.5.6 Transient Event Has Disappeared Unexpectedly

Transient alarms behave somewhat differently depending on whether the entity is managed network element, or the NMS itself. If the transient alarm is on a managed network element, such as a 'FTP transfer failed', then the alarm is self-clearing. This means if the same transient alarm happens twice or more, the previous active alarm is cleared by the latest.

If the transient alarm is not a managed network element, but rather the NMS itself, then the alarm is not self-clearing and there will be multiple of the same alarm conditions. Since these NMS alarms (or Events) that pertain the NMS, are not cleared by the NMS, NMS alarms are not correlated. They must be cleared manually by the operator. If these events are not manually cleared, the list will grow only to the value of MAX_ACTIVE_NMS_EVENTS that is specified in the NMServer.conf file. Once the list of NMS alarms reaches MAX_ACTIVE_-NMS_EVENTS, NMServer will automatically clear the oldest alarms in the list to make room for the new events. The number of events that will be cleared each time the max is reached is also specified in NMServer.conf. That configuration parameter is called EVENTS_TO_CLEAR_WHEN_MAX_REACHED.

If there was a transient event that has unexpectedly disappeared, it is most likely because NMServer is purged the event. Follow these steps below to investigate the issue.

Step 1 Filter the alarm list on Cisco MGM alarms

Step 2 Check the alarm count and compare it with the MAX_ACTIVE_NMS_EVENTS value in NMserver.conf. If the alarm count is close to the MAX_ACTIVE_NMS_EVENTS, then this explains why the transient event has been purged.

Step 3 If the alarm count for NMS alarms is nowhere near the MAX_ACTIVE_NMS_EVENTS the missing event may have been manually cleared. The NMServer log will indicate whether the event was manually cleared.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log, NMServer.log, CMSCclient.log
- Capture NMServer dump, option 3 in nmControl.

Possible alternative workaround—Restart Alarm List GUI.

C.6.5.7 Port in Tree View Displays an Aggregate Alarm, However No Children Exist Under Port

The tree view in Cisco MGM client GUIs display network elements from the top-level 'Physical View' down to the 'Port'. Alarm severities are aggregated from children up to parents. Since the port is at the lowest level of the tree, the question often arises as to how a port can have an aggregate alarm if it has no children? The answer to this question is simply: Connections are 'virtual' entities under ports in the tree view. Virtual, in the fact that the user will not see connections in the tree. But connection alarms are aggregate up to the port in the tree view.

If the customer sees an aggregate port alarm, but the customer believes there are no connections in alarm under the port, follow these steps to troubleshoot the issue.

Step 1 In general, the customer needs to compare the connection alarms with the aggregate port alarms. Follow these steps to accomplish this

a. In the Configuration Center GUI, click the 'Connections' tab at the top.

b. Find the port in the tree view and drag and drop it to the right window pane.

c. The Connection view window should launch.

d. Click the 'Get' button on the bottom of the frame.

e. The connections should be listed, and the alarm status should match alarm status in Alarm List.

Step 2 If the connection alarms do not match the aggregate port alarm(s) in Alarm List GUI, there may be a defect. Collect the defect information.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log, NMServer.log, sdbroker*.log, xdbroker*.log
- Capture NMServer dump, option 3 in nmControl.

Possible alternative workaround—none

C.7 Chassis View Problems

This section includes the following information:

C.7.1 Chassis View Basics

Chassis View is a read-only application which provides the physical view of WAN devices. For a specific node, it displays node, cards and lines. Chassis View does not display port.

Chassis View can handle the following events

- Node status changes
- Card status changes
- Line status changes

The Alarms handled by Chassis View are:

- Card alarm
- Line alarm

Chassis View shows an empty slot in the chassis when displaying un-supported cards. For Reserved Card, it shows the lines, but they are un-manageable (will not be selectable). Chassis View does not show lines under card when the card is in the any other state, other than active or stand-by.

Chassis View displays the Chassis by combining static data from the XML file and dynamic data from the Database. The first step in debugging is to check if data is populated properly in the Database. The next step would be to check that the card or line is defined in the XML file.

C.7.2 Lines Not Displayed in MGX Nodes

Lines are not displayed in the Chassis View in MGX node.

Step 1 Check if data about the lines are populated for the corresponding lines in the line table in the database.

Step 2 Check whether the lines are defined in the XML file Chassis View.xml.

Step 3 Make sure that the line numbers in the DB start from 1 and not from 2 or above.

Step 4 Make sure that the node is in sync (mode is 3).

Defect Information

If the details are not found in the DB, this probably is an EM issue. If the details are found, then proceed as follows:

Step 5 Use cwmver to get the Cisco MGM version.

Step 6 Get the node table information for the node using echo "select * from node where node_id=<NodeId> " | dbaccess " and save it in a file.

Step 7 Get the card table information for the card using echo "select * from card where node_id=<NodeId> and slot=<Slot>" | dbaccess and save it in a file.

Step 8 Save the line table information for the line using echo "select * from line where node_id=<NodeId> and slot=<Slot>" | dbaccess

Step 9 Save the log from the client machine from the location "D:\Documents and Settings\banatara\log\CMSCclient.log".

Step 10 Take a copy of the "chassisview.jar" from the location "/opt/svplus/java/jars/cwm/". We need to check that gif files used to draw the lines are available in the jar.

Possible alternative workaround—You can select the lines from the Tree View to launch other applications.

C.7.3 Card Not Displayed in MGX Nodes

Card is not displayed in the Chassis View in MGX nodes.

Step 1 Check that entries for the card is available in the card table.

Step 2 Check whether the lines are defined in the XML file ChassisView.xml.

Step 3 Make sure that the node is in sync (mode is 3).

Defect Information

If the details are not found in the DB, this probably is an EM issue. If the details are found, then

Step 4 Use cwmver to get the Cisco MGM version.

Step 5 Get the node table information for the node using echo "select * from node where node_id=<NodeId> " | dbaccess " and save it in a file.

Step 6 Get the card table information for the card using echo "select * from card where node_id=<NodeId> and slot=<Slot>" | dbaccess and save it in a file.

Step 7 Save the log from the client machine from the location "D:\Documents and Settings\<login-name>\log\CMSCclient.log".

Step 8 Take a copy of the "chassisview.jar" from the location "/opt/svplus/java/jars/cwm/". We need to check that gif files used to draw the lines are available in the jar.

Possible alternative workaround—You can select the cards from the Tree View to launch other applications.

C.7.4 DCA/DCB Status Not Displayed in PXM Cards

DCA/DCB status is always greyed in Chassis View. DCA/DCB status information is not received from the switch. So the status is not displayed or updated.

C.7.5 Ethernet Status Not Updated in PXM Cards

Ethernet status is received only when the Chassis View is launched. Dynamic changes in states of the ethernet status is not updated in Chassis View.

C.7.6 HIST, CBRX, CBTX Status Not Updated in MGX Nodes

For MGX nodes, only CPUOK LED status is updated in Chassis View. Chassis View is not managing the LEDs for HIST, CBRX, CBTX.

C.7.7 RPM Card Status not Updated

Dynamic event updates are not generated for RPM cards on MGX PXM1-based nodes. So, Chassis View does not get event updates on hot insertion or removal of RPM cards. Anyway the card will be identified when cold start is done.

C.7.8 RPM Secondary Card Status Is Blue

For RPM cards, stand-by state will show the card status in blue color as the card has only one LED(CPUOK) to show the status of the card unlike the other cards. For other types of cards, stand-by state will be indicated by yellow LED. This has been documented in Columbia Software Functional Spec.(EDCS 251024).

C.7.9 Lines Not Displayed in Secondary Card

If two cards are in a redundancy relationship, the primary card (i.e. the logical slot) is used to display the children and for all provisioning and troubleshooting activities, even if the primary slot becomes a standby. The secondary slot will not show any children under it even if it becomes active. Hierarchical views in all applications behave in this manner. Similarly, provisioning will be allowed only on the working line of an APS pair, irrespective of whether that line is currently active or not. However, monitoring will be done on both working and protection lines.

C.7.10 Lines Not Selectable

Some times lines become unselectable. For example, when trying to select line 3, line 1 may get selected or vice versa.

Step 1 Lines must be spaced sufficiently apart. If they are not spaced sufficiently apart, they may overlap resulting in this sort of a behavior.

Defect Information—Collect the following information for further analysis:

- Get the copy of ChassisView.xml file used.
- Take a copy of the "chassisview.jar" from the location "/opt/svplus/java/jars/cwm/". We need to check that gif files used to draw the lines.

Possible alternative workaround—Try selecting from the Tree View.

C.7.11 Wrong Tooltip Is Displayed

When we move the cursor over a line, wrong tooltip is displayed. For example when moving the cursor below the last line in the card, the tooltip of the line gets displayed instead of the tooltip of the card.

Step 1 Lines must be spaced sufficiently apart. If they are not spaced sufficiently apart, they may overlap resulting in this sort of a behavior.

Defect Information—Collect the following information for further analysis:

- Get the copy of XML file used. ChassisView.xml for MGX nodes and BPXIGX.xml for BPX/IGX nodes.
- Take a copy of the "chassisview.jar" from the location "/opt/svplus/java/jars/cwm/". We need to check that gif files used to draw the lines.

Possible alternative workaround—Try selecting from the Tree View.

C.8 Configuration Management - Elements

The Configuration Center management functions are divided into the following categories.

- Network elements - Manages the nodes and their components. For network element management, the Configuration Center communicates with the Config Server process.
- Connections - Manages the connections between the nodes. For connection management, the Configuration Center communicates with the Connection Management (CM) Server process.

This section describes trouble shooting guidelines for the element management (Configuration Center; Elements Tab). The Connection Management (Configuration Center; Connections Tab) section describes trouble shooting guidelines related to Connection Management.

This section includes the following information:

C.8.1 Configuration Center Framework

The Configuration Center uses the Cisco MGM framework and workflow mechanism to launch applications and drag and drop objects across application.

- Network elements can be selected in the tree view and the Configuration Center (Elements Tab) can be launched to view/modify the selected object.
- Network elements can dragged and dropped from other application to Configuration Center's Elements tab for modification.

This section includes the following information:

C.8.1.1 Cannot Launch Configuration Center

The Configuration Center cannot be launched using one of the following methods:

- Click the Configuration Center icon from the Launch Center or from any application.
- Choose Tools > Configuration Center from any application.
- Right-click the selected node from the Hierarchical Tree, and choose Configuration Center.

Step 1 Check configcenter.jar file

Make sure configcenter.jar file is under the /opt/svplus/java/jars/cwm directory on the target machine.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
- Collect Java Console information.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.1.2 Cannot Launch Other Application from Configuration Center

The Configuration Center does not launch other applications using one of the following methods:

- Choose the target application under the Tools menu item.
- Right-click on the selected object from the Hierarchical Tree, and choose target application.

Step 1 Check the target application jar file

Make sure the target application jar file exists under the /opt/svplus/java/jars/cwm directory on the target machine.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
- Collect Java Console information.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.1.3 Exception Raised When Configuration Center Is Launched

When the Configuration Center is launched, using one of the methods described above, an exception is raised and the Java Console shows the exception trace information.

Defect Information—Collect the following information for further analysis:

- Collect Java Console information.
- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.1.4 Exception Raised When Configuration Center Launches Other Application

When Configuration Center launches another application, using one of the methods described above, an exception is raised and the Java Console shows the exception trace information.

Defect Information—Collect the following information for further analysis:

- Collect Java Console information.
- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.1.5 Element Tab—Double Click In Tree View Does not Launch An Internal Frame

When Element tab is selected, the Double click on a supported network element does not create an internal frame or recycle the content of an existing internal frame to display the double clicked object

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
- Collect Java Console information
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.1.6 Element Tab—Drag and Drop Does not Launch An Internal Frame

When Element tab is selected, the Drag and Drop of supported network elements to the Element tab's content pane does not create an internal frame or recycle the content of an existing internal frame to display the dropped object.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
- Collect Java Console information
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.1.7 Element Tab—Create/Details/Modify/Refresh Button Issues

When Element tab is selected and an object is displayed in an internal frame, the Create/Details/Modify/Refresh buttons either do not launch other internal frames for further provisioning or they do not update the UI with data for the selected operation.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect Java Console information.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.1.8 Element Management—Drag and Drop Within Configuration Center

The Drag and Drop (DnD) of a network element from the Configuration Center Tree View to the Element tab's content pane:

- Fails to open an internal frame
- Fails to recycle the contents of an existing frame to display the object's attributes
- Results in the 'Operation Not Supported' message dialog box.

Step 1 Determine that the DnD operation is supported for the dropped object

The following objects can be dropped from the Tree View to the Configuration Center content pane; For the 'Element Tab', the Network, Node, Card, Line, Port, IMA, IMA links objects are supported and 'Folder' objects are not supported. For 'connection tab', the Node, Card, Line, Port objects are supported and 'Folder', IMA and IMA link objects are not supported.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect Java Console information (In particular any java raised exceptions)
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.1.9 Cross Application—Configuration Center as Drag Source

As drag source, the DnD of an object from Configuration Center's tree view or element tab to another Cisco MGM application fails to display the selected object in the target application.

Step 1 Determine the DnD operation is supported for the selected object

Determine that the target application supports the DnD operation for the dropped object.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect Java Console information (In particular any java raised exceptions)
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.1.10 Cross Application—Configuration Center Element Tab as Drop Target

The DnD of a network element from another Cisco MGM application to the Configuration Center's element tab content pane (a) fails to open an internal frame, (b) fails to recycle the contents of an existing frame to display the dropped object's attributes or (c) results in the 'Operation Not Supported' message dialog box.

Step 1 Determine the DnD operation is supported for the dropped object

The following objects can be dropped from the Tree View to the Configuration Center content pane; For the 'Element Tab', the Network, Node, Card, Line, Port, IMA, IMA links objects are supported and 'Folder' objects are not supported. For 'connection tab', the Node, Card, Line, Port objects are supported and 'Folder', IMA and IMA link objects are not supported.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect Java Console information (In particular any java raised exceptions)
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.1.11 Element Tab—Internal Frame Displays Incorrect Object or Object Data

The Element tab successfully creates the internal frame but displays either information related to another object or the object's attribute values are not valid.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect Java Console information (In particular any java raised exceptions)
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.1.12 Configuration Center's Element Tab Does Not Respond (GUI Is Grayed-Out)

The Configuration Center's Element tab does not respond and the GUI is grayed-out.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
- Collect Java Console information.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.8.2 Configuration Center; Element Management

The Configuration Center can be used to configure different network element object. The Configuration Center's element tab is the main window for creation, modification and viewing of network elements. The network element tab used the Cisco MGM 'Internal Frame' mechanism to display the attributes (groups and categories) associated with a particular network element. The following sections describe guidelines for trouble shooting issues related to creation, modification and viewing of network elements.

This section includes the following information:

C.8.2.1 XML Parsing Error

XML Parsing error is seen while launching a Configuration Center GUI (either by drag and drop method or right-lick method) for a network element. The pop-up window says "Internal Error: XML Parsing Error". The diagram below shows the error message dialog box:

Check if the network element which resulted in this error is supported in the Cisco MGM version being used. A list of the supported nodes/cards can be found in Reference

If this error is seen for a supported node/card go to step 2:

Step 1 Open /opt/svplus/log/configserver.log file and look for the message information when this error occurred.

a. A typical message in the log looks like this:
ERR: Fatal Error at file, line 0, char 0, Message: An exception occurred! Type:RuntimeException, Message:The primary document entity could not be opened.
Id=/opt/svplus/xml/configcenter/XXX/XXX-XXX.xml
(<someNumber>: <x>) <someTimeStamp> ERR: InternalError: XML Parsing Error

b. If the .xml file name mentioned above has two consecutive hyphens (example: ABC--XYZ.xml), or if it has a preceding hyphen (example: -ABC.xml) or terminates with hyphen before the file extension (example: ABC-.xml) proceed to step 3, where investigating incorrectly formed XML file names is discussed.

c. Check if the .xml mentioned in the log message (as shown in the above step) exists. If it does not exist, contact Cisco MGM engineers.

Step 2 This step is to investigate incorrectly formed XML file name strings. As a first note, the format of XML file names is <Platform>-<Card>-<InterfaceType>-<SomeEntityName>.xml. This format is generic with a few exceptions. Also note that Platform, InterfaceType are optional and will not be seen for many files (example: ABC-Card.xml is a valid XML file name).

a. If the Platform part of the XML file name is incorrect/missing, check the NODE table to see if it is correctly populated.

b. If the Card part of the XML file name is incorrect/missing, check the CARD table to verify if it is correctly populated.

c. If the InterfaceType part of the XML file name is incorrect/missing, check the appropriate table to verify if it is correctly populated.This table generally corresponds with the line/port table of the card for which this error is noticed.

d. If the EntityName part of the XML file name is incorrect, contact Cisco MGM engineers, with the Defect Information required (as given below).

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\<username>\log folder
- Collect Java Console information.
- /opt/svplus/log/configserver.log
- "dspcd" command output from the switch for the controller card and the service module where this error is detected.
- "dspln"/"dspport" command output, if this error seen for line/port.

Possible alternative workaround—None.

C.8.2.2 SNMP No Data Error

"SNMP NO DATA" error is seen while launching a Configuration Center GUI (either by drag and drop method or right-lick method) for a network element.

Check if the element for which this error is noticed is active, and that the node is synced up fine (use "selnd" command on the Cisco MGM machine. Check whether the correct community strings are being used.If this error is noticed for a an properly synced up node, on an active element, proceed as follows:

Step 1 Use your favorite SNMP Manager tool to check if the switch is responding to SNMP queries.

The SNMP MIB objects to be queried for a particular dialog can be obtained from .../svplus/log/configserver.log file. See the entries in this log file when this error occurs.

a. Using HP-OV SNMP operations we can perform a walk (on "system" MIB table for this example, using public community string) as: /opt/OV/bin/snmpwalk -c public nodeName system

b. If an error is seen during the SNMP operations (from the SNMP manager tool), verify the switch to cross-check if this information should really be present. If yes, proceed to Step 2.

Step 2 Collect the information from the .../svplus/log/configserver.log file when this error occurs.

a. From the configserver.log file identify the MIB objects that result in this error. Identify the MIB to which these objects belong. Check if these MIB objects are supported from this release.

b. If the objects are supported, but still the SNMP agent is not responding for SNMP queries, get in touch with Cisco MGM engineers for more information.

Defect Information—Collect the following information for further analysis:

- Collect all, complete screen snapshots for the investigative commands used for debugging this issue.
- .../svplus/log/configserver.log
- Related information on the switch.

Possible alternative workaround—None

C.8.2.3 Details/Create/Delete/Refresh Buttons Are Not Enabled (highlighted)

These buttons are enabled or disabled based on the requirement in the tabular view.

A button is disabled when the corresponding operation is not supported.

Open /opt/svplus/log/configserver.log for the MIB

Step 1 If "Create" button is disabled, use any SNMP tool to create the object using SNMP SET operation. If the SNMP SET operation passes, contact Cisco MGM engineers, else go to step 1.1

a. SSH or Telnet to CLI and try to up/add the element. If the operation succeeds, then contact Cisco MGM engineers

Step 2 If "Delete" button is disabled, use any SNMP tool to delete the object using SNMP SET operation. If the SNMP SET operation passes, contact Cisco MGM engineers else go to step 2.1

a. SSH or Telnet to CLI and try to down/delete the element. If the operation succeeds, then contact Cisco MGM engineers.

Step 3 The only reason why a "Details" button is disabled is that all the information related to the element are already displayed in the tabular view. Check the configserver.log file and find if any MIB Entry appropriate to the element is available. If so, go to step3.1

a. Perform a SNMP WALK on the MIB entry using any SNMP tools. If there are any information additional to what being displayed in the tabularview and if it is important to be displayed in the frame, contact Cisco MGM engineers

Step 4 The only reason why a "Refresh" button is disabled is that all the information displayed in the frame are READ_ONLY. If there are any editable fields and the "Refresh" button is disabled, contact Cisco MGM engineers

Defect Information—Collect the following information for further analysis:

- Collect all, complete screen snapshots for the investigative commands used for debugging this issue.
- /opt/svplus/log/configserver.log

Possible alternative workaround—For Creating/Deleting elements, we can either use SNMP SET operation on the Cisco MGM machine or CLI commands on the Switch.

C.8.2.4 SNMP Timeout Error

This error is thrown when an user tries to set/get values to/from SNMPCOMM and will look like the following.

Check the sync-up, link0, link1 status of the Node in the inspectorview.

Step 1 If it is "Unmanaged" or "Unreachable" or "Failed in Sync" or "Partially Synced", Check the connectivity of the Node using "ping" or "telnet" or any other such utility.

Defect Information—Collect the following information for further analysis:

- Collect all, complete screen snapshots for the investigative commands used for debugging this issue.
- /opt/svplus/log/configserver.log

Possible alternative workaround—None

C.8.2.5 SNMP Set Error

This error occurs when SNMP SET operation is done on an unmodifiable MIB object or with invalid values.

A sample snapshot of SNMP SET Error is shown below.

Step 1 Open the /opt/svplus/log/configserver.log.

Step 2 Check for the document name being used. Look for the last part of the document name.

For Example, if the document name is AAA-BBB-CCC.xml, then the document AAA-BBB-CCC.xml can be found at /opt/svplus/xml/configcenter/CCC/ directory. If the file is available, then go to step2, else contact Cisco MGM engineers.

Step 3 Open the document got from step1 and check the 'Access' of the MIB object in the XML file and check the same in /opt/svplus/mibs directory. If the 'access' from XML file and MIB definition are not same contact Cisco MGM engineers, else go to step3.

Step 4 Check the 'Range' of the MIB object in the XML file and MIB definition are not same contact Cisco MGM engineers, else go to step4.

Step 5 Perform a SNMP SET operation on the MIB object with the same value as given in the GUI and appropriate Community String(as displayed in /opt/svplus/log/configserver.log) using HP-OV. A syntax of SNMP SET operation is shown below.

/opt/OV/bin/snmpset -c private nodeName MIBVariable MIBDataType MIBValue

Step 6 If the SNMP SET operation succeeds, contact Cisco MGM engineers with appropriate defect information.

Step 7 SSH or Telnet to the switch and try to configure the same parameter with the value given in the GUI and SNMP tool. If the CLI does not report error contact Cisco MGM engineers with defect information

Defect Information—Collect the following information for further analysis:

- Collect all, complete screen snapshots for the investigative commands used for debugging this issue.
- /opt/svplus/log/configserver.log

Possible alternative workaround—None

C.8.2.6 Object Not Found In Tree View Error

This error is triggered when a network element is launched from the tabular view of Configuration Center.

Step 1 Collect the information of the object being launched. This can be done in 2 ways.

1. In the tabular view, there will be some minimal information like node name, slot number, line number, trunk number, port number etc.
2. Some minimal information regarding the object being launched will be displayed in the title of the window in the following format.
   a. For a node, the window title will have <NodeName>
   b. For a slot, the window title will have <NodeName>.<SlotNumber>

c. For a line, the window title will have <NodeName>.<SlotNumber>.<LineNumber>

d. For a port, the window title will have <NodeName>.<SlotNumber>.<PortNumber> and so on.

Step 2 With the information obtained from Step1, Check if that object is appearing in the tree view.

a. If it does appear, go to step 3.

b. If it doesn't appear, refresh the tabular view twice or thrice and check If the object still exists in the tabular view and if it continues giving the same error, contact Cisco MGM engineers with appropriate defect information

Step 3 If the object being launched is a node or card, check if that particular node or card is supported in the Cisco MGM version being used. A list of supported nodes/cards can be found in product literature.

a. If the node or card is supported, go to step 4

Step 4 Open /opt/svplus/log/CMSCclient.log file and check whether the FDN of the object being launched is matching with the information got from the Step1. Contact Cisco MGM engineers. A typical example of the log is shown below.

```
[DD Mon YYYY HH:MM:SS] DEBUG - [appsConfigCenter] :: CcElementInternalFrame :
modifyActionPerformed()
[DD Mon YYYY HH:MM:SS] DEBUG - [appsConfigCenter] CcTabularView : modify()
[DD Mon YYYY HH:MM:SS] INFO - [appsConfigCenter] Selected fdn =
/NW=X/RND=XX/CD=X/LN=X/PT=X
```

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\<username>og folder
- Collect Java Console information.
- Contents of /opt/svplus/log/configserver.log file.

Possible alternative workaround—None

C.8.2.7 Element Data Inconsistent With Switch

Information displayed in the GUI and Switch are not same.

Step 1 First Make sure that the window has been launched for the correct element in the GUI. If yes, go to step 2, else contact Cisco MGM engineers with the defect information.

Step 2 SSH or Telnet to the Switch and change few parameters and check if the change is reflecting in the GUI. If so, go to step3, else contact Cisco MGM engineers.

Step 3 Open /opt/svplus/log/configserver.log file and find the MIB OID of the element which displays inconsistent data.

Step 4 Check if the MIB OID is pointing to correct information that the user is looking for. If they are correct go to step 5, otherwise Contact Cisco MGM engineers.

Step 5 Perform a SNMP GET operation on the MIB object which shows inconsistent data using any SNMP tool. If the value got via SNMP GET operation and that is shown in the GUI are same go to step 6: , else contact Cisco MGM engineers. Syntax of SNMP GET operation in a HP-OV is shown below.

snmpget [-Cf] [options...] <hostname> {<community>} [<objectID> ...]

Step 6 Check the datatype of the MIB object that shows inconsistent data. If the datatype of the MIB object in the configserver.log is same as the datatype as defined in the MIB object definition (available at /opt/svplus/mibs/ directory), go to step 7: , else contact Cisco MGM engineers with defect information.

Step 7 Check the datatype of the MIB object.

a. If the datatype of the MIB object is Bitmap, then convert the decimal value of the MIB object to binary value and compare the bits SET/RESET with the values defined in the MIB object definition and displayed in the GUI. Contact Cisco MGM engineers with defect information.

b. If the datatype of the MIB object is IpAddress, Check if the value is coming in the appropriate format i.e. <aaa.bbb.ccc.ddd>. If the value is not in proper format, contact Cisco MGM engineers.

Defect Information—Collect the following information for further analysis:

- Collect all screen snapshots for the investigative commands used for debugging this issue.
- /opt/svplus/log/configserver.log

Possible alternative workaround—None

C.8.2.8 Config Server Reported Error Messages

This section describes the various kinds of errors that could happen on configserver.

Step 1 Open /opt/svplus/log/configserver.log

Step 2 If Datatype mismatch occurs, the following error message is displayed in the GUI.

And the corresponding error message seen in configserver.log file follows.

```
( 24560: 9) 07:49:14 CRIT: %SnmpCommException-2-NOT_INTEGER_VALUE:
SnmpVar::getInteverValue() incorrectly called for ASN type [4].
```

a. In this case, the datatype of the MIB object defined in the XML file is not same as the datatype of the MIB object definition. Contact Cisco MGM engineers with defect information.

Step 3 If the user tries to enter an invalid value, the following error message is displayed in the GUI with the parameter name being appended.

And the corresponding error message seen in configserver.log file follows.

```
( 17252: 6) 08:31:20 ERR: %SnmpCommException-3-ERR_BADVALUE: Snmp Error[3]: Bad Value;
object [] (index[2]) :
```

Step 4 If the user tries to up/add more than one element, the following error message is thrown in the GUI.

And the corresponding error message thrown in /opt/svplus/log/configserver.log file follows.

```
( 23868: 6) 14:01:09 ERR: %SnmpCommException-3-ERR_GENERR: Snmp Error[5]: General Error;
object [] (index[0])
```

Defect Information—Collect the following information for further analysis:

- Collect all complete screen snapshots for the investigative commands used for debugging this issue.
- Contents of /opt/svplus/log/CMSCclient.log file.

Possible alternative workaround—None

C.9 Connection Management Problems

This section includes the following information:

C.9.1 Configuration Center GUI; Framework Issues

The Configuration Center management functions are divided into the following categories.

- Connections - Manages the connections

For connection management, the Configuration Center communicates with the Connection Management Server process.

- Network elements - Manages the nodes and their components.

For network element management, the Configuration Center communicates with the Config Server process.

The Configuration Center's connection tab is the main window for creation, modification and viewing of network connections. The Connections tab content pane provides additional tabs for creating connections (Advanced Mode and Quick Mode tabs) and retrieving a list of existing connections (Connection tab).

The Configuration Center uses the Cisco MGM framework and workflow mechanism to launch applications and to create and display connection information.

- Connections can be selected in Cisco MGM applications and the Configuration Center (Connection Tab) can be launched to view/modify the selected connection.
- Connections can be dragged and dropped from other application to Configuration Center's Connection tab for modification.

The following sections describe guidelines for trouble shooting issues related to creation, modification and viewing of network connection using Configuration Center.

This section includes the following information:

C.9.1.1 Connections Tab—Double Click on a Tree View Does not Launch Connection's Internal Frame

The double click operation on a network element in the Tree View on Connection tab (a) fails to open an internal frame, (b) fails to recycle the contents of an existing internal frame to display the double clicked connections attributes or (c) results in the 'Operation Not Supported' message dialog box.

Step 1 Determine that the double click operation is supported for the selected object

The 'Connection tab' supports connection management for the Node, Card, Line and Port objects. The for connect 'Folder', IMA and IMA link objects are not supported.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect Java Console information (In particular any java raised exceptions).
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.9.1.2 Connections Tab—Drag and Drop Does Not Launch Connection's Internal Frame

The Drag and Drop (DnD) of a network element from the Configuration Center Tree View to the Connections tab's content pane (a) fails to open an internal frame, (b) fails to recycle the contents of an existing frame to display the dropped object's attributes or (c) results in the 'Operation Not Supported' message dialog box.

Step 1 Determine that the DnD operation is supported for the dropped object

The 'Connection tab' supports the DnD operation for the Node, Card, Line and Port objects. The DnD of 'Folder', IMA and IMA link objects are not supported.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect Java Console information (In particular any java raised exceptions).
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.9.1.3 Connection List Tab—Cannot Launch Internal Frame To Modify An Existing Connection (Using the Modify Button)

The 'Details' button fails to launch an internal frame to display the connection details for a retrieved connection.

Step 1 Check that the connection status is not in an 'Incomplete' state.

Only connection in 'Ok' and 'Fail' states can be launched for their details using the 'Details' button on the Connection list tab

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect Java Console information (In particular any java raised exceptions).
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.9.1.4 Advanced Mode Tab—Cannot Launch Connection Details Dialog (Using the 'Detail' Button)

The 'Details' button on the Advanced Mode tab fails to launch the 'Connection Details Dialog'.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect Java Console information (In particular any java raised exceptions).
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.9.1.5 Advanced Mode Tab—Cannot Launch Template Details Dialog (Using the 'Template Details' Button)

The 'Template Details' button on the Advanced Mode tab fails to launch the 'Template Configuration Dialog'.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect Java Console information (In particular any java raised exceptions).
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.9.1.6 Cross Application—Cannot Launch Other Application from Connection List

For a retrieved connection in the connection list tab, the right click pop-up menu (a) does not launch the selected target application for the connection or (c) results in the 'Operation Not Supported' message dialog box.

Step 1 Determine the operation is supported by the target application.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect Java Console information (In particular any java raised exceptions).
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.9.1.7 Cross Application—Connection List as Drag Source

As drag source, the DnD of a connection from Configuration Center's connection list to another CMSC application fails to display the selected connection in the target application.

Step 1 Determine target application supports connection object drop operations.

Determine that the target application supports the DnD operation for connection objects.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect Java Console information (In particular any java raised exceptions).
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.9.1.8 Cross Application—Connection Tab's Content Pane as Drop Target

The DnD of a connection object from another CMSC application to the Configuration Center's connection tab content pane (a) fails to open an internal frame, (b) fails to recycle the contents of an existing frame to display the newly dropped connection object or (c) results in the 'Operation Not Supported' message dialog box.

Step 1 Java VM

Determine that the source and the target application belong to the same instance of the Java VM. CMSC framework does not support DnD operations across applications belonging to different JVMs.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect Java Console information (In particular any java raised exceptions).
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.9.1.9 Configuration Center's Connection Tab Does Not Respond (GUI Is Grayed-Out)

The Configuration Center's connection tab does not respond and the GUI is grayed-out.

Step 1 Try to reproduce the problem in order to collect additional Java related data using Java DOS Window.

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
- Collect Java Console information.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.9.2 Configuration Center GUI; CM Server Reported Errors

For connection management, the Configuration Center communicates with the Connection Management (CM) Server process to (a) create, modify, delete, retrieve connections and (b) create, modify, delete or retrieve a connection templates. The CM Server throws application exceptions if it cannot successfully complete the requested operation. The CM Server exception contains an error message that describes the error condition. The Configuration Center displays the reported error message to the user for further analysis. In such cases, the problem must be researched on the CM Server side. The CM Server trouble shooting sections describe the steps required to further analyze the CM Server related issues. See C.9 Connection Management Problems. In this section, the required validation and data collection procedures related to the Configuration Center is presented.

This section includes the following information:

C.9.2.1 Connection Creation/Modification/Deletion/Retrieval Errors

When performing any connection addition/modification/deletion/ retrieval the CM Server could encounter an error and notify the Configuration Center by throwing an application exception error that contains information describing the error. As a result, the Configuration Center will display the error message. The following lists some CM Server related exceptions.

```
DATABASE_ERROR:"Database error [%s]."
UNKNOWN_EXCEPTION: "Program Error. Unknown Exception is caught in [%s]."
SUBSYSTEM_EXCEPTION:"Program Error. Subsystem exception [%s] caught in [%s]"
INTERNAL_ERROR: "Program or System Error. Function [%s] reports: [%s]"
CONNECTION_LOST: "Connection from host [%s] application [%s] lost during request."
UNKNOWN_PARAM_VALUE_TYPE: "Unknown parameter value type [%d] is processed in [%s]."
PARAM_TYPE_VALUE_MISMATCH: "Parameter value [%s] is does not match type [%d]"
VALUE_OUT_OF_RANGE: "Value [%d] is outside of the valid [%d] - [%d] range"
NO_SUCH_CONNECTION_TYPE_ENUM: "No such connection type enum [%d]"
```

```
NO_SUCH_SERVICE_TYPE_ENUM: "No such service type enum [%d]"

NO_SUCH_ENDPOINT_TYPE_ENUM: "No such endpoint type enum [%d]"

NO_PORT_TABLE_INFO_FOR_CARD: "No port table information for card family [%d]"

NO_LINE_TABLE_INFO_FOR_CARD: "No line table information for card family [%d]"

FILTER_REQUIRED:"Filter [%s] is required"

UNEXPECTED_PARAMSET: "CM Server does not expect parameter set [%d]."

UNSUPPORTED_ENDPOINT: "CM Server does not support end point with card type [%s], vs[%s],
interface type [%s], node platform [%s], controller type [%s] for connection type [%s]
service type [%s], endtoend type [%s]."

UNSUPPORTED_PARAMETER_FOR_VISM: "Unsupported parameter setting on the [%s] end. CM Server
does not support [%s] + [%s] PVC's for VISM cards with firmware revision less than [%s]
and card mode set to [%s]."

PROTECTED_CONNECTION: "[%s] end of the connection is protected. Protected connections
cannot be deleted."

UNSUPPORTED_NODE_PLATFORM: "CM Server does not support node platform [%d]."

UNSUPPORTED_CONN_TYPE: "CM Server does not support Connection of type [%d]."

UNSUPPORTED_SERV_TYPE: "CM Server does not support Connection type [%s] , Service type
[%s] and Endtoend type [%s] between Card type [%s] and [%s]."

UNSUPPORTED_SERV_TYPE_ONE_END: "CM Server does not support Connection type [%s] , Service
type [%s] and Endtoend type [%s] on Card type [%s]."

UNSUPPORTED_CARD_PAIR: "Connection between card type [%s] and card type [%s] is not
supported."

NO_SUCH_NODE_ID_IN_DB: "Node id [%d] not found in table [node]."

NO_SUCH_NODE_NAME_IN_DB: "Node name [%s] not found in table [node]."

NO_SUCH_CARD_IN_DB: "Card : Node[%d], Slot[%d] not found in table [card]."

NO_SUCH_LOG_PORT_IN_DB: "Card : Node[%d], Slot[%d], LogPort[%d] (%d - in database), not
found in table [%s]."

NO_SUCH_PHY_PORT_IN_DB: "Card : Node[%d], Slot[%d], Line[%d], PhyPort[%d] (%d - in
database), not found in table [%s]."

NO_SUCH_LINE_IN_DB: "Card : Node[%d], Slot[%d], Line[%d] not found in table [%s]."

NO_SUCH_CONNECTION_IN_DB: "Connection [%s] not found in database"

UP_CONN_FAILED: "Upping Connection Failed. Test Result from switch [%s]"

DOWN_CONN_FAILED: "Downing Connection Failed. Test Result from switch [%s]"

NO_ONE_SEGMENT_HYBRID: "Cannot create one segment hybrid connection."

INCORRECT_LINE_SUBTYPE: "Incorrect Line SubType. Line: Node[%d],slot[%d],ifindex[%d] is
[%d] not [%d]."

INVALID_LINE_NUMBER: "func [%s]:Invalid Line Number(s)."

NO_CONTROLLER_IN_PORT: "node[%s] slot[%d] port[%d] does not have controller of type
[%s]";

INVALID_FDN: "The given FDN format or value is invalid. [%s]"

INVALID_PORT: "Provisioning operations are not allowed on feeder trunk/routing trunk and
XLMI trunk ports. [%s]"
```

Step 1 Verify that the CM Server and databroker are up and running by perform a "psg sdbroker" and "psg cmserver" on the command line.

Step 2 Verify if the CmServer re-started while the operation was being done by checking the cmsvr.log and searching for the string "START OF THE PROCESS". Verify the timestamp if the server process was either re-started while the operation was being performed. Also check for any cmsvr coredumps under /opt/svplus/corefilesdir/

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect Java Console information (In particular any java raised exceptions).
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.9.2.2 Connection Template Creation/Modification/Deletion/Retrieval Errors

When performing any connection template creation/modification/deletion/retrieval the CM Server could encounter an error and notify the Configuration Center by throwing an application exception error that contains information describing the error. As a result, the Configuration Center will display the error message. The following lists some CM Server related connection template exceptions.

CONN_TEMPLATE_ALREADY_PRESENT: "The Connection Template[%s] is already present in the conn_template table";

CONN_TEMPLATE_NOT_PRESENT: "The Connection Template[%s] is not present in the conn_template table";

CONN_TEMPLATE_TABLE_INCONSISTENT: "The Connection Template table contains more than one entry for the template[%s]";

CONN_TEMPLATE_PARAMS_NOT_PRESENT: "The Connection Template[%s] is not present in the conn_templ_param table";

DATABASE_ERROR:"Database error [%s]."

UNKNOWN_EXCEPTION: "Program Error. Unknown Exception is caught in [%s]."

SUBSYSTEM_EXCEPTION:"Program Error. Subsystem exception [%s] caught in [%s]"

INTERNAL_ERROR: "Program or System Error. Function [%s] reports: [%s]"

Step 1 Verify that the CM Server and databroker are up and running by perform a "psg sdbroker", "psg xdbroker" and "psg cmserver" on the command line.

Step 2 Verify if the CM Server re-started while the operation was being done by checking the cmsvr.log and searching for the string "START OF THE PROCESS". Verify the timestamp if the server process was either re-started while the operation was being performed. Also check for any cmsvr coredumps under /opt/svplus/corefilesdir/

Defect Information—Collect the following information for further analysis:

- Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- Collect Java Console information (In particular any java raised exceptions).
- Collect cmsvr.log file under the /opt/svplus/log directory.
- Collect configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.9.3 Cmsvr Errors

The following are some of the most common errors seen when a Provisioning request is issued:

C.9.3.1 End to End Type Cannot Be PVC for Connections with PNNI Segment

When a connection addition is attempted, cmsvr checks its the endpoints and the End to End Type to make sure it is supported. The return error window on the screen states "EndtoEndType cannot not be PVC for connections with a PNNI segment ".

The problem must be fixed on the CM GUI while adding the connection.

Step 1 Verify that the endpoints that are being used to add the connection are not on PNNI nodes or feeders to PNNI nodes.

Step 2 Change the End to End Type in the CM GUI to either SPVC or Hybrid (as the case might be).

Defect Information—Collect the cmsvr logs, in the directory /opt/svplus/log.

Possible alternative workaround—None.

C.9.3.2 Unsupported Service Type for the Foresight Connections for PNNI/SPVC Endpoints

During connection addition, an eror in the return error window on the screen could state "CM Server does not support Connection type[], Service type[], and Endtoend type []between Card type and []." The parenthesis are filled with appropriate values.

We need to determine if the service type is applicable to the endpoints.

Step 1 Determine the cards on which the connection is being added and the service type given in the GUI.

Step 2 This error is thrown when the service type is either abr-fs, atfst for a PVC, SPVC or Hybrid end to end type and the card is either a pxm, axsm, rpm or frsm12 card.

Defect Information—Collect the cmsvr logs, in the directory /opt/svplus/log.

Possible alternative workaround—Change either the endpoints or the service type to add the connection.

C.9.3.3 Ce-Ce Connection Port Speed Should Be Same on Both

While adding a CE-CE connection this error message might be thrown "For Ce-Ce Connection Port Speed should be same on both sides. Port Type should be same except for Structured 8T1 and E1"

Step 1 Make sure that the port speed is same for both the local and remote endpoints.

Step 2 Also the port types should be the same for both the endtypes except for Structured 8T1 and 8E1.

Defect Information—Collect the cmsvr logs, in the directory /opt/svplus/log.

Possible alternative workaround—Change the endpoints accordingly to add the connection.

C.9.3.4 Cannot Create One Segment Hybrid

While adding a one segment connection, a check is made to make sure that it is not a Hybrid connection. The following error will pop up if that is the case. " Cannot create one segment hybrid connection."

Step 1 Make sure the End to End Type is not Hybrid for a single segment connection.

Defect Information—Collect the cmsvr logs, in the directory /opt/svplus/log.

Possible alternative workaround—Change the end to end type as something other than Hybrid.

C.9.3.5 Cannot Add Connection Between -byte Port Header and -byte Port Header for chan type NIW and NIW-replace

During a connection addition between two FRSM_12 ports, the cmsvr checks to see if the port headers are the same (4-byte or 2-byte) for both the end points. An error is thrown if they are not. "Cannnot add Connection between 4 byte port header to 2 byte port header for chan type NIW or NIW-replace."

Step 1 Determine what port header was used while creating the port in question. Then use ports with matching port headers to create the connection.

Defect Information—Collect the cmsvr logs, in the directory /opt/svplus/log.

Possible alternative workaround—None

C.9.3.6 Unsupported Service Type - General node-slot-port-version

During a Connection addition the cmsvr checks the node/slot/port versions to ensure that the service type is supported on that version of the node/card/port.

Step 1 Make sure that the said version of the node/slot or port support that service type from Cisco MGM.

Step 2 Check the ConnGroupService.mib as an additional check for the versions and the supported parameters.

Defect Information—Collect the cmsvr logs, in the directory /opt/svplus/log.

Possible alternative workaround—None

C.9.3.7 End Point Not Present in One of the Connection Tables During Modify

When a connection modification is attempted and an error window on the screen states "Connection [] not found in database"

Step 1 Verify that a row (entry) exists for the connection in the user_connection. A query in the form

%> echo "select * from user_connection where l_node_id = A and l_slot = B and l_port = C and l_subchnl_1 = D and l_subchnl_2 = E" | dbaccess stratacom

Step 2 If it does not look in the corresponding connection table (connection - for FR, atm_connection for atm segments, cesm_connection for cesm segments, rpm_connection for rpm segments and voice_conn for vism segments) to see if the connection exists there.

Step 3 If it doesn't look in the dbkr_temp table for an entry for that connection.

Defect Information—The following log files need to be collected:

Collect the cmsvr, sdbroker and corresponding em logs, in the directory /opt/svplus/log.

Collect the outputs of the database entries for the endpoints in the segment tables and user_connection table.

Possible alternative workaround—Resync the node or wait for synchup to complete

C.9.3.8 Cmsvr—Connection Diagnostics Issues

The cmsvr processes validates and services the Connection provisioning requests from the CM GUI.

If the request is for connection addition, modification, deletion or connection trace, the request is forwarded to cmgrd process through ILOG(IPC) request. If the request is for connection diagnostics like testdelay, testconn etc. (except conntrace), cmsvr sends to snmpcomm process for forwarding to switch.

C.9.3.9 TestConn or TestDelay Failed With Switch Error

Connection diagnostics(testdelay/testcon/up/down/reroute) failures with one of the following error messages:

- TestDelay failed with Switch error
- TestConn failed with Switch error

Step 1 Query the connection information from the user_connection table for that connection

If possible, execute the testdelay/testcon diagnostics for the same connection from ConnProxy (Service Agent) and verify the results

Step 2 Query the connection information from the switch CLI and verify the connection status (dspcon , dspchan etc.)

Execute the testdelay/testcon diagnostics from switch CLI and verify the results matches with what was reported in Cisco MGM(tstdelay, tstconn)

Defect Information

1. Capture selnd output
2. Copy all the cmsvr logs from /opt/svplus/logs directory
3. Capture the user_connection table query output from Cisco MGM DB for the given end point (if the request is not an addition request)
4. Capture the switch CLI output for the testdelay/testconn diagnostics on the same connection

Possible alternative workaround—

1. Check the status of the connection and clear any alarms due to line/port issues (adding loopback, correcting the physical cable issues by verifying the physical port connections etc.). After the connection comes up and is in clear state, rerun the testdelay/testconn diagnostics again.
2. Note that testcon is not applicable for single-end SPVC connections and on AXSM card types
3. Note that the connection status should be clear or fail for the testdelay/testcon diagnostics to be executed, otherwise the test will be blocked from cmsvr
4. Note that testconn/testdelay diagnostics cannot be done on RPM to RPM connections
5. Note that testdelay diagnostics is not applicable for VOICE and DATA connections
6. Note that for any connection if the local end of the connection does not support that particular diagnostics, cmsvr will verify if the diagnostics can be executed from the remote end. If the diagnostics is not supported by both the end points of a connection, an appropriate error message will be given to the user.

C.9.3.10 Connection Up/Down/Reroute Failed

Connection up/down/reroute diagnostics failures with switch error

Step 1 Query the connection information from the user_connection table for that connection

Step 2 Query the connection information from the switch CLI and verify the connection status (dspcon, dspchan etc.)

Execute the up/down/reroute diagnostics from switch CLI and verify the results matches with what was reported in Cisco MGM(upcon, dncon, rrtcon)

Defect Information

1. Capture selnd output
2. Copy all the cmsvr logs from /opt/svplus/logs directory
3. Capture the user_connection table query output from Cisco MGM DB for the given end point (if the request is not an addition request)
4. Capture the switch CLI output for the up/down/reroute diagnostics on the same connection

Possible alternative workaround:

1. Check the status of the connection and clear any alarms due to line/port issues (adding loopback, correcting the physical cable issues by verifying the physical port connections etc.). After the connection comes up and is in clear state, rerun the up/down/reroute diagnostics again.
2. Verify the connection status to find if the connection is already down, when trying to do a down operation or the connection is already up when trying to do an up operation.
3. Note that connection reroute might take the connection to FAIL state for a while, if it is rerouted.

C.9.3.11 Connection Trace Failures

Connection trace returns a failure.

Step 1 Make sure the connection is not in Fail state, connection trace does not work on failed connections, Cisco MGM does not block this request as well.

Query the connection information from the user_connection table for that connection

Step 2 Query the connection information from the switch CLI and verify the connection status (dspcon, dspchan etc.)

Execute the connection trace diagnostics from switch CLI and verify the results matches with what was reported in Cisco MGM(conntrc, dsptrcbuffer)

Defect Information:

1. Capture selnd output
2. Copy all the cmsvr logs from /opt/svplus/logs directory
3. Copy all the cmgrd logs from /opt/svplus/logs directory
4. Capture the user_connection table query output from Cisco MGM DB for the given end point (if the request is not an addition request)
5. Capture the switch CLI output for the trace diagnostics on the same connection

Possible alternative workaround:

1. Check the status of the connection and clear any alarms due to line/port issues (adding loopback, correcting the physical cable issues by verifying the physical port connections etc.). After the connection comes up and fine in clear state, rerun the trace diagnostics again.
2. Verify the connection status. If the connection status is down trace cannot be executed on the connection. If the connection status is failed, probability is more that the trace result will be an empty string
3. Note that connection trace cannot be executed on an incomplete, or DAX PNNI segment connections

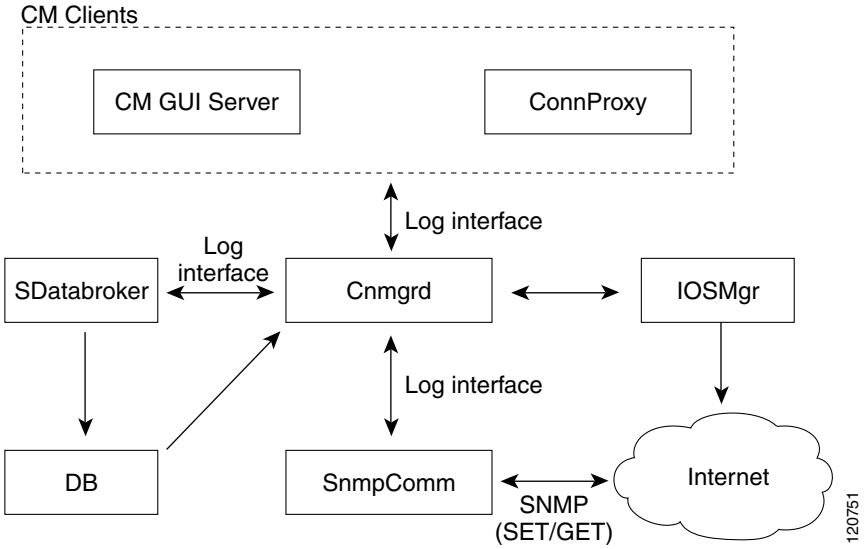
C.9.4 CMGRD

This section includes the following information:

C.9.4.1 High Level Connection Subsystem Architecture

Figure C-6 gives a high level view of the Connection Management Subsystem.

Figure C-6 Connection Management Subsystem



Related key index entries: connproxy, cmserver, xcmgrd, cmgrd

The Connection subsystem comprises the following modules:

- ConnProxy—Is the SNMP Agent Interface for Connection Management, client to cmgrd.
- CmServer—Provides the backend functionality to the Connection Management GUI, client to cmgrd.
- Cmgrd—Is the backend module which accepts requests from ConnProxy, CmsServer Clients and issues the SNMP Varbinds to the Switch for Addition, Modification and Deletion. Subsequently cmgrd informs sdbroker after an ADD/MOD/DEL operation for the status of the particular request, upon which sdbroker updates the Cisco MGM database.

The following errors are applicable to all types of connections PVC, SPVC, XPVC, and Hybrid.

C.9.4.2 Cmgrd - Sdbroker Errors

During an Addition request cmgrd could return errors which cmgrd has received from sdbroker, the following are some of the most common errors seen when a Provisioning request is issued.

This section includes the following information:

C.9.4.2.1 Cmgrd—Sdbroker Addition/Modification/Deletion Errors. Adding a Connection Results in an Error "Fail to Communicate with sDatabroker"

Related key index entries: cmgrd, sdbroker

When any Connection Add/Mod/Del request is made, cmgrd checks its ILOG connection with sDatabroker. The above error will result when cmgrd could not verify that sdbroker is available for servicing requests. In other words the ILOG connection between them is broken.

The problem must be researched on the sdbroker side.

Step 1 Verify that the sdbroker is up and running. Do a "psg sdbroker" on the command line.

Step 2 View the sDbroker log for ilog errors There could be multiple sdbrokers running on the machine, the way to check which sdbroker cmgrd talked to for that particular request is as follows.

a. vi the cmgrd.log file, and go to the very end of the file. Then do a backward search for the string sdbroker, that string should indicate the number (#) of the sdbroker that cmgrd could not talk to.

b. Do a "psg sdbroker" and then check the corresponding log file of this sdbroker.

Defect Information:

- stack trace of the sdbroker process "pstack <pid of sdbroker>"
- sdbroker and cmgrd logs.

Possible alternative workaround—None.

C.9.4.2.2 Cmgrd—Sdbroker Addition/Modification/Deletion Errors. Provisioning a Connection Results in an Error "sDatabroker process busy. Please retry"

Related key index entries: cmgrd, sdbroker

The return error window on the screen states "sDatabroker process busy. Please retry". This indicates that the CMGRD was able to process the request and send it to the sDbroker, but the sDbroker did not respond prior to the CMGRD'S request time-out. Communication between the CMGRD and sDbroker appear to be working though.

We need to determine if the sDbkr is "sleeping" or is overburdened with requests.

Step 1 Determine the sdbroker that should be processing the request. Use /opt/svplus/tools/dbcmap command.

Step 2 Check the message log to see if sDbkr is processing lots of other messages during the provisioning time frame. If the message log is unavailable, check the shared memory between EM and DMD. ('count' command). The column EMQDepth and Em R show current status of this shared memory. This will show the sdbroker's processing at the present time not when the provisioning request failed. If there is a large number of entries in the message log file, or the EM is pumping lots of messages to DMD, the sDbroker is truly busy and the operator should wait for the system to catch up with current alarm events.

Defect Information:

- If the sdbroker is processing many traps (> 20/second) during the time of the provisioning request then there is no sDbkr defect. Investigate the switch / NTS / EM if you feel that there should not be this large number of requests occurring at the given time.
- If the sDbroker appears to be "sleeping" we need to capture the current status of the sDbkr. Execute the "pstack <pid> " command twice and save the output.

Possible alternative workaround:

Repeated attempts at provisioning should be made. If there is a switch that is sending out many alarms, fixing the problem on the switch is the best solution. If the sdbroker has been 'sleeping' for a long period of time, then it should be killed and restarted.

C.9.4.2.3 Cmgrd—Sdbroker Addition Errors. Adding a Connection Results in an Error "MGM syncup in progress".

Related key index entries: cmgrd, sdbroker, sync-up

While the system is in the process of syncing up, the user cannot provision connections. The user will be returned the error "MGM syncup in progress"

We need to determine if the system is really in syncup or not. If the system is still syncing up then this is proper operation.

Step 1 View the sync log located in /opt/svplus/log/.DBKR_SYNCHUP_MESSAGE (note the "." before the filename). search for the last "xxx Start Begin at" line where xxx is ether 'Warm' or 'Cold'. Warm start will take a short time compared to Coldstart which could take several hours. If there is a line at the end of the file stating "Declare Syncup Complete" or "Warmstart Cache Rebuild Complete" then syncup is done and there is a problem with dmd.

Step 2 If syncup is not complete, view the start time of syncup. Compare this to the maximum sync time identified in the /usr/user/svplus/config/dmd.conf file next to the keyword SYNCHUP_ALL_NODES_SYNC_WAIT_LIMIT. If the time taken to sync is larger than the time identified in the dmd.conf file, then dmd has a problem.

Step 3 If the system is truly still syncing up, then the system behavior is correct.

Defect Information—If there is a DMD problem, save the dmd, cmgrd, sdbroker logs and message logs along with the .DBKR_SYNCHUP_MESSAGE and .DMD_SYNCHUP_MESSAGE* files located in the /opt/svplus/log directory.

Possible alternative workaround—The user can force the system to declare sync-up by sending the dmd a forced sync signal. This will not place the nodes into mode '3' any faster, but will allow the user to attempt provisioning some nodes, while other nodes are in the process of syncing up.

Step 1 Execute command 'selnd' from the cwm command line. Note the nodes in mode '3'. All connections provisioned after forced sync-up can only go through nodes with mode = 3. (they actually can go through specific cards on nodes in mode = 4, but let's stick with mode 3 nodes for now).

Step 2 Send the sync-up signal to the dmd by entering command "kill -ALRM dmd".

Step 3 view the .DBKR_SYNCUP_MESSAGE file for the sync-up completion.

C.9.4.2.4 Cmgrd—Sdbroker Addition Errors. Adding a Connection Results in an Error "No more vpi/vci available for local trunk end".

Related key index entries: cmgrd, sdbroker, vpi/vci

Provisioning fails and the error message is displayed.

"No more vpi/vci available for local trunk end" Also "Remote trunk"

"Local end of the connection already exists" Also 'Remote end" and "Both end"

"Vpcon already exists for Local Vpi" Also "Remote Vpi" and "Both ends"

Each of these error messages identifies the reason for the failure of provisioning. They sometimes can be displayed in error. The reason is a mismatch between the switch and the DMD's cache. To find this out, dump the DMD cache "pkill -USR1 dmd" and compare the values in the cache with those on the switch for endpoint associated with the error.

Defect Information—If the switch and DMD cache are not in sync, we will need the DMD logs and message logs, dmd cache dump and the EM logs for the node in question. We will also need the switch CLI screen shot of the connection in question.

Possible alternative workaround—If there is a cache inconsistency, the only work around is a complete cache resync(/opt/svplus/tools/CacheResync). If there is no DMD cache inconsistency, it is a normal operational scenario. Different connection add parameters should be chosen.

C.9.4.2.5 Cmgrd—Sdbroker Addition Errors. Adding a Connection Results in an Error "EndPoint Exists Local/Remote/Both end of the connection already exists.".

Related key index entries: cmgrd, sdbroker, endpoint exists

During a connection add, the cmgrd will request intermediate endpoint vpi/vci from sdbroker. If the sdbroker incorrectly chooses endpoints that are already in use by the switch the cmgrd will try to provision these endpoints and return the error "endpoint exists" to the user.

Step 1 Determine which of the endpoints already exist on the switch. If it is the intermediate endpoints then it is a databroker problem.

a. When provisioning hybrid connections the CMGRD requests intermediate endpoints from the sDbroker. The sDbroker then requests them from DMD and then forwards them back to CMGRD. First identify the DMD which is to process the node use /opt/svplus/tools/dbcmap command. Then dump that dmd's cache. Verify that the DMD does not contain the end points in question in it's cache.

b. We now need to determine why the dmd doesn't have the information on endpoints that exist on a switch. We first need to determine if the EM sent the add message to the DMD. See C.15.2.1 Connection Inconsistency Between the Switch and GUI . If the add message is not found and the logs do not go back to coldstart, then we will need to check to see if EM has done any processing of this endpoint. Check for the endpoint in the xxx_Connection table. If the endpoint is not there, check the EM to determine why it didn't process the endpoint. If the endpoint is in the xxx_connection table we know that EM processed it, but we don't know if it forwarded it to DMD.

Defect Information:

- If the problem is an intermediate endpoint and it is on the switch but EM didn't process it or didn't' send the message to DMD. Check the EM log, nts log from the /opt/svplus/log
- If the problem is within the DMD we ill need the dmd logs, dmd message logs and the dmd cache dump.

Possible alternative workaround—None

C.9.4.2.6 Cmgrd—Sdbroker Modification/Deletion Errors. Modifying or Deleting a Connection Results in an Error "sDatabroker Could not lock connection entry.".

Related key index entries: cmgrd, sdbroker, lock connection

During a Connection Modification or Deletion request the above error could result when sdbroker could not find the connection in its cache.

All scenarios of modify/delete connection failures display the same error to the user. To determine exactly what happened you must view the /opt/svplus/log/sdbrokerX.XXXX.log file.

Step 1 Search for the ERR: "<sDbkr_CmgrdModConn_c::Process> INTERFACE ERROR" near the end of the file. A detailed reason for the error will follow on the same line.

a. Note that for delete connections, search for sDbkr_CmgrdDelConn_c::Process instead of sDbkr_CmgrdModConn_c::Process.

Defect Information:

- If the problem is an intermediate endpoint and it is on the switch but EM didn't process it or didn't' send the message to DMD see section EM logs,nts logs from /opt/svplus/log.
- If the problem is within the DMD we ill need the dmd logs, dmd message logs and the dmd cache dump.

Possible alternative workaround—None

C.9.4.3 Cmgrd Errors

During an Addition request cmgrd could return errors which cmgrd has received from snmpcomm or the switch itself.

This section includes the following information:

C.9.4.3.1 Cmgrd—Addition/Modification/Deletion Errors. Provisioning a Connection Results in an Error "Fail due to Switch Timeout"

Related key index entries: cmgrd, time-out

When any Connection Add/Mod/Del request is made, cmgrd issues a request to the switch with a Snmp community string, either a SET or GET string. These community strings are overwritten by the process snmpcomm. This process uses the values of the strings which are present in the node_info table. Thus, when a provisioning request times out from the switch, one possible problem is that the node's community string in the node_info table does not match the string on the node itself.

The problem can be researched by checking the community strings on the node and the node_info table.

Step 1 Check the community strings on the nodes by issuing the command "dsnmp".

Step 2 Check the community string in the node_info table based on node_id, the strings are encrypted so use the decrypt binary which would display the string in the clear format.

Step 3 Once the strings are cross-referenced and a discrepancy is indeed present. Then the user can change the strings in the following possible ways:

a. Issue the command "cnfsnmp" on the node and change the community strings to match that of the Cisco MGM.

b. Or the user can use the application RunConfigurator to change the string in the Cisco MGM to match that of the switch.

Defect Information—If the above possible investigations do not work, collect the following

- The cmgrd.log which is located in /opt/svplus/cmgrd.log
- The output of the query "select * from node_info where node_id = X"

Possible alternative workaround—See Investigation.

C.9.4.3.2 Cmgrd—Addition/Modification/Deletion Errors. Provisioning a Connection Results in an Error “Agent not responding, request timed-out; or Fatal error, SnmpComm is not running.”

Related key index entries: cmgrd, snmpcomm

When any Connection Add/Mod/Del request is made, cmgrd issues a request to the switch, but the request is actually first issued to the process snmpcomm. Which in turn sends the SNMP SET/GET to the node. In this scenario the above errors can be returned by the process snmpcomm, the error could be a time out error from snmpcomm process or an ILOG Communication error.

The reason that snmpcomm can send a time-out error is because it is too busy processing requests and cannot accept more requests at the moment. And the reason for the "SnmpComm not Running" error is that cmgrd could not establish and ILOG connection with it. The following basic check can be done:

Step 1 Issue the command "psg snmpcomm" to ensure that the process is indeed running.

Step 2 Check for snmpcomm coredumps in the corefilesdir directory.

Re-issue the request after waiting for few minuteness will take care of the time-out error.

If it is indeed noticed that snmpcomm process is not running, then a warm-start has to be done to ensure that the process does come up.Whn the process starts-up the ILOG connection with cmgrd is established.

Defect Information:

- If after re-issuing the request and still getting the same time-out error than collect the cmgrd.log and snmpcomm .log.
- And if after warm-starting the snmpcomm process does not run, then collect the watchdog.log file.

Possible alternative workaround—Re-issue the request after some time, this interval could enable snmpcomm to clear its pending requests. Do a warm-start to ensure that the snmpcomm process starts up.

C.9.4.3.3 Cmgrd—Addition/Modification/Deletion Errors. Provisioning a Connection Results in an Error "Outstanding request exists for same object."

Related key index entries: cmgrd, outstanding request

When any Connection Add/Mod/Del request is made, cmgrd process these requests in a multi-threaded manner. Sometimes a request can take greater than 3 minutes to process, because of the different scenarios that the switch responds with (i.e. timeouts.). If the request takes greater than 3 minutes from the CMGui, then the GUI will time-out and indicate this to the user. And from the Connection Proxy path the time-out value is 2 minutes, subsequently it will indicate a time-out error to the user.

The tendency of the user will be to re-issue this request immediately, upon which cmgrd could return the error "Outstanding requests exists for the same object".

The reason that error is returned is because cmgrd is still processing the initial request which the clients (CMGui and Connection Proxy) timed out on. An ideal case for this would be when a switch time-out is received for a multi-segment case, and cmgrd is still busy backing-off other segments and waiting for the time-out response of some other segments. Just to be sure that cmgrd is still running, issue the following commands.

Step 1 Issue the command "psg cmgrd" to ensure that the process is indeed running.

Step 2 Check for cmgrd coredumps in the corefilesdir directory. If there indeed was a coredump collect the corefile.

Step 3 Do a "tail -f cmgrd.log in the logs directory to see if cmgrd is processing requests."

Re-issue the request after waiting for few minutes.

Defect Information—If after re-issuing the request and still getting the same error than collect the cmgrd.log.

Possible alternative workaround—Re-issue the request after some time, this interval could enable cmgrd to clear its pending request.

C.9.4.3.4 Cmgrd—Addition/Modification/Deletion Errors. Provisioning a Connection Results in an Error "Fatal error, IOSMGR is not running, may need to be manually started"

Related key index entries: cmgrd, iosmgr

When any Connection Add/Mod/Del. request is made with a Popeye1 RPM Card, cmgrd issues a request to the switch, but the request is actually first issued to the process iosmgr. Which in turn sends the request to the node, via an expect script session In this scenario the above error can be returned when cmgrd could not talk to iosmgr via the ILOG Communication.

The reason for the error is that cmgrd could not establish and ILOG connection with iosmgr. The following basic check can be done:

Step 1 Issue the command "psg iosmgr" to ensure that the process is indeed running.

Step 2 Check for iosmgr coredumps in the corefilesdir directory.

If it is indeed noticed that iosmgr process is not running, then a warm-start has to be done to ensure that the process does come up.Whn the process starts-up the ILOG connection with cmgrd is established.

Defect Information—And if after warm-starting the iosmgr process does not run, then collect the runiosmgr.log file.

Possible alternative workaround—None, iosmgr has to be running to be able to Provision on Pop1 RPM cards.

C.9.4.3.5 Cmgrd—Addition Errors. Provisioning a Connection Results in an Error "Vpi/vci ranges retrieval from svc_operation failed"

Related key index entries: cmgrd, svc_operation

This error is only present for Hybrid Connection Add request, cmgrd queries the svc_operation table of the Feeder Trunk ports for the vpi/vci ranges. These ranges in turn are given to sdbroker who in turn returns an available vpi/vci that cmgrd can use to SET on this Feeder Trunk Port.

The reason for the error is that when cmgrd queries the svc_operation table for the feeder trunk ports vpi and vci ranges the entry is not found in the table.

Step 1 Re-issue the Hybrid Addition but tail the cmgrd.log.

Step 2 In this log a query in the form of "SELECT MIN_SVCC_VPI, MAX_SVCC_VPI, MIN_SVCC_VCI, MAX_SVCC_VCI FROM SVC_OPERATION WHE RE NODE_ID = X AND SLOT = X AND PORT + 1 = X" will be seen. This is the actual query that is failing.

Step 3 Run the query from the command line or (dbaccess stratacom prompt) and the user can figure out which ports information is not present in the svc_operation table.

Step 4 The reason could be that for that port the resource partition is not configured on the CLI. The user should go to the CLI and do the command "addpart" for that port.

Step 5 After issuing the command "addpart" on the CLI, the user should check the Cisco MGM table svc_operation database to check for the existing of the row. If the row is present the connection request can be re-issued. If the row still is not present in the svc_operation then it is a probably an EM issue.

Defect Information—If after configuring the resource partition on the CLI, and the svc_operation table is still not populated then see C.5 Equipment Management Problems and collect the appropriate OOEMC logs.

Possible alternative workaround—None.

C.9.4.3.6 Cmgrd—Addition/Modification/Deletion Errors. Provisioning a Connection Results in an Error "Can't get segment info from Data-base."

Related key index entries: cmgrd, segment info

The above error will be returned by cmgrd when it could not get a row from one of the Cisco MGM database tables for the current connection request. If the request is an ADD, then the possibility is that the query for the intermediate endpoints from either the node or the bis_object tables failed. If it is a Mod/Del then in addition to the queries into the node and bis_object tables the problem could be that the connection is not found in the user_connection table.

In this error scenario there could be multiple reasons of failure which differ between and Add and Mod/Del request. But most of the time this error is returned if one of the queries to the node, bis_object and user_connection tables fail for the current request. Some basic checks would be to see if the nodes in question and in the intermediate nodes are really synced up with the Cisco MGM. Also the user should try the same request from both the CMGUI and Connection Proxy paths.

Because of the nature of this error it is best that a Cisco MGM DE investigate.

Defect Information—Collect cmgrd.log, cmsvr.log, ConnProxy*.log and sdbroker*.log.

Possible alternative workaround—None.

C.9.4.4 Cmgrd—Switch Errors

During an Addition/Modification/Deletion request cmgrd sends Snmp Requests to the switch, when the switch rejects the SNMP request, cmgrd queries the Error MIB Table and GETs the error string to display back to the user. Some of the common error strings are indicated below:

- C.9.4.4.1 Cmgrd—Addition/Modification Errors. Provisioning a Connection Results in a Switch Error "Agent reported bad/wrong value for one of the variables in the request."
- C.9.4.4.2 Cmgrd—Addition Errors. Provisioning a Connection Results in a Switch Error "Object Exists on the Agent or Specified VPI/VCI not available".
- C.9.4.4.3 Cmgrd—Addition/Modification Errors. Provisioning a Connection Results in a Switch Error "Requested cell rate (lscr/lpcr or rpcr/rscr) is too high"
- C.9.4.4.4 Cmgrd—Addition Errors. Provisioning a Connection Results in a Switch Error "SPVC is not allowed on this interface"
- C.9.4.4.5 Cmgrd—Addition Errors. Provisioning a Connection Results in a Switch Error "Local Channels not enough."
- C.9.4.4.6 Cmgrd—Addition/Modification Errors. Provisioning a Connection Results in a Switch Error "Error in Traffic Parameters."
- C.9.4.4.7 Cmgrd—Addition/Modification/Deletion Errors. Provisioning a Connection Results in a Switch Error "Network Busy, try later"
- C.9.4.4.8 Cmgrd—Modification Errors. Modifying a Connection Results in a Switch Error "Connection does not exist in CproDb/Agent returned no such name"

C.9.4.4.1 Cmgrd—Addition/Modification Errors. Provisioning a Connection Results in a Switch Error "Agent reported bad/wrong value for one of the variables in the request."

Related key index entries: cmgrd, bad value

When any Connection Add or Mod request is issued, an SNMP VarBind is SET on the switch via cmgrd. The switch can reject this VarBind with the above error.

The reason for the error is that cmgrd sent an invalid value for one of the mib objects. The Cisco MGM DE should do the investigation for this error, as it indicates that there is a problem in the data that cmgrd either received from the clients or internally mapped from the other side of the connection.

The user should try the same connection from both Connection Proxy and CmGui interface and note the behavior from both of the clients. If the provisioning result from both clients is the same, it tends to indicate that this is either a cmgrd issue or a sdbroker vpi/vci issue.

Defect Information—The cmgrd.log, ConnProxy*, cmsvr.log and sdbroker*.logs should be collected.

Possible alternative workaround—If the user is doing a Add, and default values are being used, then there is no work around. But, if the user is doing a MOD and then the user could change the value of the Object that is being modified and retry the connection.Also if this is a sdbroker vpi/vci issue, retry the connection as sdbroker does not re-use the previous vpi/vci combination.

C.9.4.4.2 Cmgrd—Addition Errors. Provisioning a Connection Results in a Switch Error "Object Exists on the Agent or Specified VPI/VCI not available".

Related key index entries: cmgrd, object exists

When any Connection Add request is issued, an SNMP VarBind is SET on the switch via cmgrd. The switch can reject this VarBind and the subsequent cmgrd query to switch error table can return the above errors.

The reason for the error is that the connection that Cisco MGM is trying to Add already exists on the switch. This could be a user endpoint or an intermediate endpoint.

Step 1 The user should retry the same connection, if this second attempt succeeds it indicates that the intermediate endpoints vpi/vci was already present on the switch. If this is the case look at the cmgrd-sdbroker error "EndPoint Exists Local/Remote/Both end of the connection already exists".

Step 2 If on the second attempt the switch still returns the same error. Then this has to be debugged by a Cisco MGM DE, as it could indicate an inconsistency between the Cisco MGM database and the Switch.

Defect Information—Save the cmgrd.log, ConnProxy*.log, cmsvr.log and sdbroker*.log.

Possible alternative workaround—Retrying the connection addition more than once, if that still fails a Cisco MGM DE has to look into the issue.

C.9.4.4.3 Cmgrd—Addition/Modification Errors. Provisioning a Connection Results in a Switch Error "Requested cell rate (lscr/lpcr or rpcr/rscr) is too high"

Related key index entries: cmgrd, cell rate

During a connection Addition/Modification request it is possible that the port the connection is being SET on, has no more resources available to accept the traffic parameters that the current Snmp SET is requesting, at this point the Switch will reject the request with the above error.

Step 1 For the user endpoint check the user port on the CLI via the command "dsppnportrsrc" this will indicate the resource available per port

Step 2 Check the Switch TSG EDCS-235791, section 1.3.4 for further information on how to debug this issue.

Step 3 If the failure is not happening on a user endpoint port, and instead on an Intermediate port (i.e. for Multi-Segment connections) then find out the local and remote endpoint feeder trunk ports (This can be done easily by using the Network Topology GUI). On the CLI check the "dsppnportrsrc" for these feeder trunk ports.

Defect Information—If after checking that the ports have enough bandwidth to add these connections and still the error is being returned then save the cmgrd.log.

Possible alternative workaround—Freeing up resources on the port which needs the bandwidth to add the connection, or lowering the traffic parameters value in the connection request.

C.9.4.4.4 Cmgrd—Addition Errors. Provisioning a Connection Results in a Switch Error "SPVC is not allowed on this interface"

Related key index entries: cmgrd, interface

During a connection Addition request it is possible that the user endpoint port that the connection is being SET on, has an incorrect signalling configured on it, the above error is indicative of this condition.

For non trunking ports the signalling on the port cannot be "pnni".

Step 1 For the user endpoint port check the CLI for the following:

a. Interface is pnni port or controller port, check interface using "dsppnport"

b. Change port to UNI port. Before doing this make sure that no calls are going through this interface.

dnpnport <portID>

cnfpnportsig <portID> -univer uni30

Step 2 After changing the configuration retry the connection request.

Defect Information—Not applicable, as the above error has to be a Switch Configuration issue.

Possible alternative workaround—Indicated in the Investigation part.

C.9.4.4.5 Cmgrd—Addition Errors. Provisioning a Connection Results in a Switch Error "Local Channels not enough."

Related key index entries: cmgrd, channels

During a connection Addition request it is possible that the user endpoint port or card that the connection is being SET on, has already reached its limit of allowable connections.

Check the port or card of the user endpoints on the CLI.

Step 1 Check the port resources of the endpoint via "dsppnportrsrc".

Step 2 If the number of LCNs is zero, delete some connections from this interface.

Step 3 After changing the configuration retry the connection request.

Defect Information—Not applicable, as the above error has to be a Switch Configuration issue.

Possible alternative workaround—Indicated in the Investigation part.

C.9.4.4.6 Cmgrd—Addition/Modification Errors. Provisioning a Connection Results in a Switch Error "Error in Traffic Parameters."

Related key index entries: cmgrd, traffic parameters

During a connection Addition/Modification request if the local endpoints remote parameters do not match the remote endpoints local parameters, then the above error is indicated by the switch. The particular parameter depends on the Service type of the connection.

This error cannot be easily debugged it has to be looked at by a Connection Management DE. Because the error indicates that the mapping of local to remote (and/or vice versa) has a problem in the value that is being SET on the Switch.

Step 1 Retry the connection from both CMGUI and Connection Proxy interfaces.

Step 2 If the result from both the interfaces is the same this could be a cmgrd bug. If the request succeeds from one of the interfaces then this is more possibly a Client issue.

Defect Information—Collect cmgrd.log, ConnProxy*.log and cmsvr.log.

Possible alternative workaround—Change some of the traffic parameter values in the connection request and re-try the connection.

C.9.4.4.7 Cmgrd—Addition/Modification/Deletion Errors. Provisioning a Connection Results in a Switch Error "Network Busy, try later"

Related key index entries: cmgrd, network busy

During a connection Addition/Modification request if the switch returns the above error, it indicates that there is some CPU intensive activity happening on the Controller Card. The Cmgrd request will be backed off the other segments and the error will be Returned to the user. But, for a Delete operation (since it is a Destructive command) the operation will not be backed off.

The error has no work around, the user has to wait and try the request on the Switch later. If after waiting and retrying multiple times and the error keeps repeating, then it has to be looked at from the Switch side.

Defect Information—Not applicable.

Possible alternative workaround—Wait and try the connection at a later time.

C.9.4.4.8 Cmgrd—Modification Errors. Modifying a Connection Results in a Switch Error "Connection does not exist in CproDb/Agent returned no such name"

Related key index entries: cmgrd, cprodb

During a connection Modification the switch could return the above error when the connection is truly not present on the switch.

The user should check the connection in the user_connection table. From this entry the user should check that all of the segments do exist on the switch CLI. If all segments are truly present in the switch CLI then the issue has to be looked at from the Switch side. But, if any one of the segments is not present on the switch then this could be a sdbroker or EM issue.

Defect Information—If it is deemed a sdbroker or EM issue collect the appropriate logs and also collect cmgrd.log. If all of the segments of the connection are present on the switch and the switch still returns this error, contact the switch DEs.

Possible alternative workaround—None.

C.10 Diagnostics Center Problems

The Diagnostics Center provides different diagnostics operations at the following different network elements levels.

Network Diagnostics

- Retrieve the current sync-status, alarm status of all the nodes in the network.
- Support the Network/Node Health Statistics and Manageability Checks. At the network level, only the node manageability checks results are supported.

Node Diagnostics

- Retrieve current sync status, node alarm status, ipaddress and several other node attributes.
- Retrieve the sync status of all the cards in the node.
- Request to do the Node Resync.
- Request VSI Partition Data and also perform VSI Consistency Checks on the node.
- Support Node Health Statistics such as SNMP Success Count, FTP/TFTP Success/Failure Counts etc.
- Perform Node Manageability Checks such as IP Reachability, SNMP Community String Check etc.

Card Diagnostics

- Retrieve Card Level information (sync status, card status, firmware rev etc.)
- Retrieve Card CPU Usage on cards that support this functionality.
- Retrieve the Memory Pool Usage Information on cards that support this functionality.
- Retrieve the Memory Buffer Pool Usage Information on cards that support this functionality.
- Retrieve Card Level Real Time Statistics if any.
- Retrieve information about all lines and paths that are in loopback on the card.
- Retrieve information about currently running BERT tests on the card.
- Retrieve information about currently running IMA Link tests.

Port Diagnostics

- Retrieve the Port Level Attributes such as Port Status etc.
- Perform Loopback.
- Perform start/stop/modify BERT
- Retrieve the results and/or current status of the BERT
- Monitor the Scheduled Grooming Results
- Configure the On Demand Grooming
- Retrieve the Port Level Real Time Statistics

Line Diagnostics

- Retrieve the Line Level Attributes such as Line Status, Loopback Status etc.
- Perform Loopback
- Perform start/stop/modify BERT
- Retrieve the results and/or current status of the BERT.
- Retrieve the Line Level Real Time Statistics.

Path Diagnostics

- Retrieve the Path Level Attributes such as Path Status etc.
- Perform Loopback
- Retrieve the Path Level Real Time Statistics.

Trunk Diagnostics

- Retrieve the Trunk Local and Remote End Real Time Statistics

IMA Group Diagnostics

- Retrieve the IMA Group Level Attributes such as IMA Group Status etc.
- Retrieve the accumulated delay on all the IMA Links under the IMA Group.
- Clear the accumulated delay on all the IMA Links under the IMA Group.
- Restart the IMA Group.
- Retrieve the IMA Group ATM Cell Layer Ingress/Egress Counters.
- Retrieve the IMA Group Level Real Time Statistics.

IMA Link Diagnostics

- Retrieve the IMA Link Level Attributes such as IMA Link Status etc.
- Start/Stop IMA Link Test
- Modify IMA Link Test Pattern
- Retrieve the IMA Link Level Real Time Statistics.

Connection Diagnostics

- Retrieve the Connection Level Attributes such as Connection Status etc.
- Retrieve the Local and Remote End Point Attributes such as A-bit, AIS, OAM etc.
- Retrieve the Local and Remote End Point Real Time Statistics.

The Diagnostics Server would interface with the CM Server to support the following Connection related Diagnostics Operations:

- Connection Loopback
- Up Connection
- Down Connection
- Connection Trace
- Test Connection
- Test Delay
- Test Connection Segment
- Test Ping OAM

This section includes the following information:

C.10.1 Diagnostics Center Framework

This section includes the following information:

C.10.1.1 Cannot Launch Diagnostic Center

The Diagnostics Center cannot be launched (main window will not appear) using one of the following methods:

- Click the Diagnostics Center icon from the Launch Center or from any application.
- Choose Tools > Diagnostics Center from any application.
- Right-click the selected node from the Hierarchical Tree, and choose Diagnostics Center.

Step 1 Check diagcenter.jar file under /opt/svplus/java/jars/cwm directory.

Defect Information—Collect the following information for further analysis:

1. Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
2. Collect screen snapshots. In particular, error/information message dialog boxes.

3. Collect cmsvr.log file under the /opt/svplus/log directory.
4. Collect DCSserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.10.1.2 Cannot Launch Other Applications from Diagnostics Center

The Diagnostics Center cannot launch other applications using one of the following methods:

- Choose the target application under the Tools menu item.
- Right-click on the selected object from the Hierarchical Tree, and choose target application.

Step 1 Check the target application jar file

Make sure the target application jar file exists under the /opt/svplus/java/jars/cwm directory on the target machine

Defect Information—Collect the following information for further analysis:

1. Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
2. Collect screen snapshots. In particular, error/information message dialog boxes.
3. Collect cmsvr.log file under the /opt/svplus/log directory.
4. Collect DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.10.1.3 Exception Raised When Diagnostics Center Is Launched

When the Diagnostics Center is launched, using one of the methods described above, an exception is raised and the Java Console shows the exception trace information.

Defect Information—Collect the following information for further analysis:

1. Collect Java Console information.
2. Collect CMSCclient.log file under the D:\Documents and Settings\<username>\log directory
3. Collect screen snapshots. In particular, error/information message dialog boxes.
4. Collect cmsvr.log file under the /opt/svplus/log directory.
5. Collect DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.10.1.4 Double Click Operation In Diagnostics Center Tree View Does not Launch An Internal Frame

Double click on an object in Diagnostics Center Tree View does not launch an internal frame in the content window to open the object in the context pane (Internal Frame).

Defect Information—Collect the following information for further analysis:

1. Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
2. Collect Java Console information

3. Collect screen snapshots. In particular, error/information message dialog boxes.
4. Collect cmsvr.log file under the /opt/svplus/log directory.
5. Collect DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.10.1.5 Drag and Drop Within Diagnostics Center

The Drag and Drop (DnD) of a network element from the Diagnostics Center Tree View to the content pane (a) fails to open an internal frame or recycle the contents of an existing frame to display the object's attributes or (b) results in the 'Operation Not Supported' message dialog box.

Step 1 Determine that the DnD operation is supported for the dropped object

The following objects can be dropped from the Tree View to the Diagnostics Center content pane; For the 'Element Tab', the Network, Node, Card, Line, Port, IMA, IMA links objects are supported and 'Folder' objects are not supported. For 'connection tab', the Node, Card, Line, Port objects are supported and 'Folder', IMA and IMA link objects are not supported.

Defect Information—The following log files need to be collected:

1. Collect the following information for further analysis:
2. Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
3. Collect screen snapshots. In particular, error/information message dialog boxes.
4. Collect cmsvr.log file under the /opt/svplus/log directory.
5. Collect DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.10.1.6 DnD from/to Diagnostics Center to/from Other Applications

As drag source, the DnD of an object from Diagnostics Center to another Cisco MGM application fails to display the selected object in the target application.

As a drop target, the DnD from another CMSC application to the Diagnostic Center's content pane (a) fails to open an internal frame or recycle the contents of an existing frame to display the dropped object's attributes or (b) results in the 'Operation Not Supported' message dialog box.

Step 1 Determine the DnD operation is supported for the selected object

Determine that the target application supports the DnD operation for the dropped object.

Step 2 Java VM

Determine that the source and the target application belong to the same instance of the Java VM. CMSC framework does not support DnD operations across applications belonging to different JVMs.

Defect Information—Collect the following information for further analysis:

1. Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory
2. Collect cmsvr.log file under the /opt/svplus/log directory.
3. Collect DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.10.1.7 Drop Target Displays Incorrect Object or Object Data

The Diagnostic Center's internal frame opens successfully but displays either information related to another object or the dropped object attribute values are not correct.

Defect Information—Collect the following information for further analysis:

1. Collect CMSCclient.log file under the D:\Documents and Settings\username\log directory.
2. Collect screen snapshots. In particular, error/information message dialog boxes.
3. Collect cmsvr.log file under the /opt/svplus/log directory.
4. Collect DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.10.1.8 Diagnostics Center Does Not Respond (GUI Is Grayed-Out)

The Diagnostics Center does not respond and the GUI is grayed-out.

Step 1 Check if Java DOS Window is already enabled.

1. Launch the WebStart Application
2. Click on File->Preferences
3. Select the Java tab
4. For the selected Java entry, check the 'Command' column entry (If need be, expand the column display all information) to determine if it is set to 'javaw.exe' or 'java.exe'.
5. If the 'Command' column settings is set to'java.exe', then the Java DOS Window is already enabled and a DOS Window task should be running on the machine. Otherwise, the Java DOS Window is not enabled ('Command' column entry is set to'javaw.exe').

Step 2 If Java DOS Window is already enabled, then proceed to the 'Defect Information' section to collect data.

Step 3 If Java DOS Window is not enabled, then the current log information might not be sufficient to determine the root cause.

a. Collect currently available log information.
b. Enable the Java DOS Window.

Enable the Java DOS Window by changing the'javaw.exe' to'java.exe'.

c. Verify that the WebStart/Java DOS is enabled.

Use PC Client to launch a CMSC GUI application and verifying that a DOS box is launched.

d. step 3-5: Try to reproduce the problem in order to collect additional Java related data using WebStart/Java DOS Window.

Defect Information—Collect the following information for further analysis:

1. Collect Java DOS Window data:
2. Select the Java DOS box.
3. Issue a 'Ctrl and Break' command. Hold the 'Ctrl' key down and click on the 'Break' (Pause) key.
4. This action should result in the DOS showing Java thread related information.
5. Copy the data to a log file for further analysis.
6. Collect CMSCclient.log file under the D:\Documents and Settings\<username>\log directory
7. Collect screen snapshots. In particular, error/information message dialog boxes.
8. Collect cmsvr.log file under the /opt/svplus/log directory.
9. Collect DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.10.2 11.2 Diagnostic Server (DCServer) Specific Issues

This section includes the following information:

C.10.2.1 XML Parser Error

XML Parsing error is seen while launching Diagnostics Center GUI (either by drag and drop method or right-lick method) for a network element. The pop-up window says "Internal Error: XML Parsing Error" and looks like the picture shown below:

Step 1 Check if the entity (Node / Card / Line / Port etc) which resulted in this error is supported in the Cisco MGM version being used.

If this error is seen for a supported node/card go to step 2.

Step 2 Open /opt/svplus/log/DCServer.log file and look for the message information when this error occurred

a. A typical message in the log looks like this: ERR: Fatal Error at file, line 0, char 0, Message: An exception occurred! Type:RuntimeException, Message:The primary document entity could not be opened. Id=/opt/svplus/xml/diagcenter/XXX/XXX-XXX.xml (<someNumber>: <x>) <someTimeStamp> ERR: InternalError: XML Parsing Error

b. If the .xml file name mentioned above has two consecutive hyphens (example: ABC--XYZ.xml), or if it has a preceding hyphen (example: -ABC.xml) or terminates with hyphen before the file extension (example: ABC-.xml) proceed to step 3, where investigating incorrectly formatted XML file names is discussed

c. Check if the .xml mentioned in the log message (as shown in the above step) exists under /opt/svplus/xml/diagcenter directory. If it does not exist, contact Cisco MGM Engineers with the Defect Information.

Step 3 This step is to investigate incorrectly formed XML file name strings. As a first note, the format of XML file names is <Platform>-<Card>-<InterfaceType>-<SomeEntityName>.xml. This format is generic with a few exceptions. Also note that Platform, InterfaceType are optional and will not be seen for many files (example: ABC-Card.xml is a valid XML file name).

a. If the Platform part of the XML file name is incorrect/missing, check the NODE table to see if it is correctly populated.

b. If the Card part of the XML file name is incorrect/missing, check the CARD table to verify if it is correctly populated.

c. If the InterfaceType part of the XML file name is incorrect/missing, check the appropriate table to verify if it is correctly populated.This table generally corresponds with the line/port table of the card for which this error is noticed.

d. If the EntityName part of the XML file name is incorrect, contact Cisco MGM Engineers, with the Defect Information required (as given below).

Defect Information—Collect the following information for further analysis:

1. Collect all, complete screen snapshots for the investigative commands used for debugging this issue.
2. DCServer.log file from the log directory.

Possible alternative workaround—None

C.10.2.2 SNMPCOMM_TIMEOUT Error While Polling mib Objects

The Diagnostics Center GUI shows an SNMP Timeout error when polling real time counters.

Step 1 Check the status of the node.

Step 2 If the node is reachable then check whether the community strings are set properly.

Step 3 Check in the DCServer.log file whether the community string used for querying the objects is set correctly.

Step 4 Check whether the query has been sent to the switch.

Defect Information—Collect the following information for further analysis:

- Collect CMSClient.log file under the D:\Documents and Settings\username\log directory.
- Collect DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None

C.10.2.3 Node Syncup Status Are Not Shown in the Diagnostic Center GUI

When Diagnostic Center is launched for a network element, the GUI does not show the Node syncup status for all the nodes in the network.

Step 1 Run "selnd" as svplus and check the status of all the nodes. If they are not shown properly then there should be some problem with the EM process. Check the EM logs.

Step 2 Check the node table entries for all the nodes.

Defect Information—Collect the following information for further analysis:

- node table entry for the corresponding node.
- DCServer.log file from the log directory.

Possible alternative workaround—None

C.10.2.4 Node Resync Fails

Node resync fails from Diagnostic Center.

Step 1 Check whether the node is reachable.

Step 2 Check for any exceptions in the DCServer.log file.

Defect Information—Collect the following information for further analysis:

- node table entry for the corresponding node.
- DCServer.log file from the log directory.
- emd.log from the log directory.

Possible alternative workaround—None

C.10.2.5 Polling of Real Time Counters Fails

Unable to poll Realtime counters from DC GUI

Step 1 Check whether the node is reachable and the community strings are set correctly.

Step 2 Check whether those objects are applicable. Check any appropriate commands from CLI.

Step 3 Use any snmp tool and check whether the mib objects are retrievable.

Step 4 Narrow down the problem by selecting one counter at a time and find out for what all counters the polling fails.

Defect Information—Collect the following information for further analysis:

- Collect the DCServer.log file from /opt/svplus/log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- CLI output of dspcd <slot No> for that card. Output of any appropriate CLI commands used.
- If step 4 was performed, provide the list of counters for which polling failed.

Possible alternative workaround—Use CLI to monitor the real time counters.

C.10.2.6 Some Real Time Counters Are Not Shown

Some Real Time counters are missing from DC GUI

Step 1 Check whether the counters are applicable to that card (version/mode if applicable).

Step 2 Check any appropriate commands from CLI.

Step 3 Use any snmp tool and check whether the mib objects are retrievable.

Defect Information—Collect the following information for further analysis:

- Collect the DCServer.log file from /opt/svplus/log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.
- CLI output of dspcd <slot No> of the card.
- Provide the list of missing counters for the particular node / card.

Possible alternative workaround—Use CLI to get the real time counter values.

C.10.2.7 Unable to Start/Stop/Modify BERT Operations

Unable to start/stop/modify BERT operations from DC GUI

Step 1 Check whether the node is reachable and the community strings are set correctly.

Step 2 Check whether the card is in Active state.

Step 3 Check whether correct varbinds are sent for snmpset.

Step 4 Check whether the options set for start/stop/modify BERT are applicable.

Step 5 Check whether BERT operations are successful in CLI with the options chosen from DC GUI.

Step 6 GUI sends only the mandatory and modified values to the DC server for snmpset. Use any snmptool with these values alone and do BERT operation. If it succeeds, then there is some problem with the Diagnostic Center.

Defect Information—Collect the following information for further analysis:

- Collect the DCServer.log file from /opt/svplus/log directory.
- Collect screen snapshots. In particular, the DC GUI BERT window, error/information message dialog boxes.

Possible alternative workaround—Use CLI/DiagProxy for BERT operations.

C.10.2.8 Unable to Start/Stop IMA Link Test Patterns

Unable to start/stop/modify IMA Link Test pattern from DC GUI

Step 1 Check whether the node is reachable and the community strings are set correctly.

Step 2 Check whether the card is in Active state.

Step 3 Check whether correct varbinds are sent for snmpset.

Step 4 Check whether the IMA Link Test pattern can be performed from the CLI.

Step 5 Use any snmptool and try to set the objects shown in the DCServer.log file.

Defect Information—Collect the following information for further analysis:

- Collect the DCServer.log file from /opt/svplus/log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.

Possible alternative workaround—Use CLI for IMA Link test patterns operations.

C.10.2.9 Cannot Perform Connection Diagnostics

Unable to perform connection diagnostics from DC GUI. The connection diagnostics are performed through the CM Server application. Diagnostics Server forwards all the connection diagnostics requests to the CM Server. If there are any connection diagnostics errors, it is more likely to be in the CM Server application.

Step 1 Check whether the Sync Up is complete.

Step 2 Check whether the node is reachable and the community strings are set correctly.

Step 3 Check whether the card is in Active state.

Step 4 Check whether correct varbinds are sent for snmpset.

Step 5 Check for any specific exceptions in the DCServer.log file.

Step 6 If there are no exceptions in the DCServer.log file then the problem could be from the Connection Manager front.

Defect Information—Collect the following information for further analysis:

- Collect the DCServer.log and cmsvr.log files from /opt/svplus/log directory.
- Collect screen snapshots. In particular, error/information message dialog boxes.

Possible alternative workaround—Use CLI/ SNMP Conn Proxy for connection diagnostics.

C.10.2.10 Miscellaneous Issues / Problems in Diagnostics Center

If you encounter any other issues/problems not listed above, contact the Cisco MGM Engineers with the Defect Information.

Step 1 Check whether the similar operation could be performed successfully through the CLI.

Defect Information—Collect the following information for further analysis:

- Describe the operation during which the problem/issue was encountered.
- Collect the DCServer.log and cmsvr.log files from /opt/svplus/log directory.
- Collect all the screen snapshots.
- Collect the CLI dump of this operation if applicable.

Possible alternative workaround—None

C.11 Performance Management Collection and Parsing Problems

PM collection is done on the entire node and statistics files are uploaded from all applicable cards on that node

Stats Parser parses these statistics files and stores the stats data in the database.

This section includes the following information:

C.11.1 PM Collection Issues

This section includes the following information:

C.11.1.1 pmcollector—Generic Troubleshooting

When performing generic troubleshooting, always check the following:

* If pmcollector process is running - run 'psg pmcollector' and check if you get a result.

* Make sure the stats files come to /opt/svplus/purge directory of the Cisco MGM. Check for all stats files, there should not be any missing file. There should be no files accumulated in /opt/svplus/spool directory.

* Check the file_err_log table for any failure of collection of file.

* Check the collsvr_err_log table for any failure during start/stop collection

* Check the coll_err_log table for entire collection server errors.

* Check the '/opt/svplus/cache/scm/scmcollout.log' for stats file request being done.

* Check the '/opt/svplus/cache/scm/scmcollin.log' for stats file been collected or not.

* Check the '/opt/svplus/cache/scm/scmcollout.log' for stats file collection errors.

C.11.1.2 PM Collection Fails for the Node - Logfile Shows "Node not discovered"

This can happen when the node is not in mode

Check the node_info table - echo "select node_not_discovered from node_info where node_id=<node_id> and slot=<slot>" | dbaccess

If the node_not_discovered is set to 1 means, node is not discovered.

Check the state of the Node. For that node-name - run the following command - echo "select * from node where node_name = '<node-name>' " | dbaccess

Check the mode of the node in the output - the mode must be 3.

Defect Information—Collect the following information for further analysis:

- pmcollector.log, output of 'selnd' or output of - echo "select * from node where node_name = '<node-name>' " | dbaccess
- Related key index entries
- pmcollector

Workaround

If the node is not mode 3, lookup troubleshooting for EM module.

C.11.1.3 PM Collection Fails for the Node - Logfile Shows "Card not discovered"

This can happen when the card is not in the active state.

Check the node_info table - echo "select card_not_discovered from node_info where node_id=<node_id> and slot=<slot>" | dbaccess

If the card_not_discovered is set to 1 means, card is not discovered

Check the card table - echo "select fc_state, fc_type, slot from card where node_id = <node-id> and slot = <slot-num> " | dbaccess.

The fc_state of the card must be 3

Defect Information—Collect the following information for further analysis:

- pmcollector.log, output of - echo "select fc_state, fc_type, slot from card where node_id = <node-id> and slot = <slot-num> " | dbaccess.
- Related key index entries
- pmcollector

Workaround—If the card is not in fc_state 3, lookup troubleshooting for EM module.

C.11.1.4 PM Collection Fails for the Node - Logfile Shows "Time not synchronized"

This can happen when the timestamp between the Cisco MGM and the Collector is not synchronized or the timestamp between collector and node is not synchronized.

Check the sync_info table - echo "select offset from sync_info where sync_node_id=<node_id>" | dbaccess

Check the time on the Cisco MGM/Collector and on the node and make sure the offset got from above query is the difference of time in seconds.

In case of feeders, check the time difference between Cisco MGM and the routing node of the feeder.

Defect Information—Collect the following information for further analysis:

- pmcollector.log
- Related key index entries
- pmcollector

Workaround—Set the time on the Cisco MGM/Collector and the node to the same timestamp.

C.11.1.5 PM Collection Fails for the Node - Logfile Shows "Snmp failed"

This can happen due snmp failure due to wrong community string or due to timeout.

Check the node_info table to check the get_str, set_str and make sure they are the one on the node. Check the snmp community strings on the node using the 'dspsnmp'.

check the log files for more detailed error, grep "snmp" scm*, if it is timeout error, change the timeout setting and retry setting in /opt/svplus/config/pmcollector.conf

Defect Information—Collect the following information for further analysis:

- pmcollector.log
- Related key index entries
- pmcollector, manual snmp results

Workaround—If the community strings are different on Cisco MGM and node, lookup troubleshooting for Topology module

C.11.1.6 PM Collection Fails for the Node - Logfile Shows "Ftp failed"

This could happen for various reasons, generally because of wrong user/password or due to timeout.

Check the node_info table to check the node_id, node_name, ipaddress and make sure they are the correct one.

Check the type of ip routing used while starting collection and for that ip routing check if the ip address is reachable/valid.

Check the ftp_user_name and ftp_user_passwd in the coll_info table and the ftp_user_name and ftp_user_passwd in the node_info table of stratacom database are matching and are valid.

Defect Information—Collect the following information for further analysis:

- pmcollector.log, dump of coll_info table, dump of node_info table of stratacom.
- Related key index entries
- pmcollector

Workaround—Use the atm or lan ip which is reachable.

C.11.1.7 PM Collection Fails for the Node - Logfile Shows "Polling failed and wait for major retry" or "Major retry failed and wait for critical retry" or "Critical retry failed and wait for history retry" or "History retry failed and wait for next retry" or "No more retry"

This could happen for various reasons, mainly due to ftp/tftp failures.

Check the node reachable[pingable] with nw_ip_address or lan_ip_address.

If only the nw_ip_address is reachable and the lan_ip_address is unreachable, then make sure the 'IP Routing' for stats collection is using the 'In Band'.

If only the lan_ip_address is reachable and the nw_ip_address is not reachable, then make sure the 'IP Routing' for stats collection is using the 'Out of Band'.

Use 'dspifip' command to check the lan_ip_address and nw_ip_address

Check the pmcollector.log, whether we are using the correct ip_address or not for stats collection.

Check for the existence of connections on the slot, for which, we are collecting the stats. Also check for the stats Flag. Use command 'sumDBShow' or 'sfmDBShow' on the node.

Check the ftp_user_name and ftp_user_passwd in the coll_info table and the ftp_user_name and ftp_user_passwd in the node_info table of stratacom database are matching and are valid.

Defect information—Collect the following information for further analysis:

- pmcollector.log, dump of node_info and coll_info.
- Related key index entries
- pmcollector

Workaround—Use the atm or lan ip which is reachable.

C.11.2 PM Parsing Issues

This section includes the following information:

C.11.2.1 StatsParser—Generic Troubleshooting

StatsParser reads the data from the stat files and inserts the data into the database.

When performing generic troubleshooting, always check the following:

* If statsparser process is running - run 'psg statsparser' and check if you get a result.

* Log level for the statsparser can be increased by editing the config file.

- Edit the ~/config/statsparser.conf and change the LOG_LEVEL field to 7.

C.11.2.2 StatsParser—Files Are Parsed But the Files Are Listed in the BadFileList

While parsing the stats files and inserting the data into the database, if the StatsParser encounters a problem with the parsing of data in the stats file or a problem with the format of the file, the file be put in the BadFileList.

- Node entry not available in the scmnode table. Perform the following query and verify that

* all the nodes that are under collection state are listed in the output.Also verify that the

* entries of the nodes are not duplicated. The query is

% echo " SELECT * from scmnode" | dbaccess

- File is corrupted. Read the file manually using the statsreader.

Usage is % statsreader < stats file name >

If the out put doesn't look normal or the file looks corrupted, then the problem would most probably on the switch side. Report the problem to the Cisco MGM team and the switch team

- There is no more space left on the machine to insert any more data.

Report the problem immediately.

Defect Information—Collect the following information for further analysis:

- statsparser.log, output of df -k and mount
- Related key index entries
- BadfileList

C.12 Statistics Report Problems

This section includes the following information:

C.12.1 Statistics Report

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

SRT GUI provides the user an ability to generate and view historical statistics reports. Reports like Raw statistics, Top Utilization are shown in table format and performance data reports are shown in graph and table format

C.12.2 If You Collected Data and You See No Data Available

If you started collection and you see no data available when generating raw reports

Step 1 Make sure the data is collected and parsed.

Step 2 Make sure the corresponding table as data for the specified time period

Defect Information—Collect the following information for further analysis:

- /opt/svplus/log/srtserver.log

Possible alternative workaround—None

C.12.3 If You Generate Report and Don't See Data for a Long Time

If you are trying to generate reports and you don't see any data for a long time and you only see the message Retrieving data.

Step 1 Check srtserver.log for any errors messages.

Defect Information—Collect the following information for further analysis:

- /opt/svplus/log/srtserver.log

Possible alternative workaround—None

C.12.4 You See FDNs for Other Entities When You Generate Report

You see FDNs for other entites when you generate reports. For example: When you generate raw report for trunk data for one card, you might see trunk data from different card also. This is because some of the tables doesn't have slot information and hence we get data only with node information

Step 1 This is not an error. You will see extra data

Defect Information—Collect the following information for further analysis:

- /opt/svplus/log/srtserver.log

Possible alternative workaround—None

C.12.5 You See Wrong FDN for Raw Report

The FDN reported is wrong. Either with wrong values or with junk values

Step 1 The data should be correct. This is an error in the server while forming FDN

Defect Information—Collect the following information for further analysis:

- /opt/svplus/log/srtserver.log

Possible alternative workaround—None

C.12.6 The Utilization Report Value Is Greater Than 100%

The Utilization report value is greater than 100%.

Step 1 This is an error. Collect the log file mentioned below

Defect Information—Collect the following information for further analysis:

- /opt/svplus/log/srtserver.log

Possible alternative workaround—None

C.13 Service Agent Problems

RtmProxy is the only component in Service agent that is used in Cisco MGM. Service Agent processes user request through SNMP and convey to switch agent and finally return the result to user.

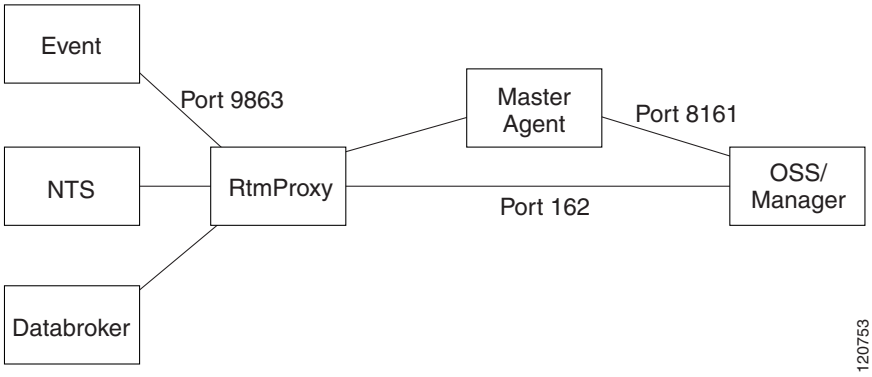
This section includes the following information:

- C.13.1 RtmProxy

C.13.1 RtmProxy

RtmProxy is Cisco MGM's northbound SNMP interface to provide traps from all switches to the customer applications. It is an interface with which the customer application registers for traps.The customer application use snmp to register with RtmProxy. Figure C-7 gives the flow of information.

Figure C-7 RTMProxy



The OSS/Manager send snmp request to port 8161 of the Cisco MGM machine. In this request they specify the port on which they are listening for traps. In the above example, the manager will be sent traps on port 162. The registration, de-registration and other such scripts can be found at /opt/svplus/scripts/proxyscripts/rtmproxy on a Cisco MGM machine. These scripts can be used as reference for registration and de-registration with RtmProxy. These scripts are meant only for internal use.

This section includes the following information:

- C.13.1.1 Registration with RtmProxy Failed
- C.13.1.2 Not Receiving Any Traps
- C.13.1.3 Manager Gets Deregistered
- C.13.1.4 Nodal Community Strings Do Not Work

C.13.1.1 Registration with RtmProxy Failed

Manager's snmp request to register with RtmProxy returned an error.

Step 1 Verify that the Cisco MGM core is up and running. This can be verified by doing ps -ef | grep RtmProxy on the Cisco MGM machine.

Step 2 Verify that the snmpset request was sent to port 8161.

Step 3 Verify that the community string for the snmpset is set to private

Step 4 Verify that the mib objects that are being set are correct.

The mib objects that should be set for the manager's registration are

stratacom.rtm.trapsConfig.trapConfigTable.trapConfigEntry.managerRowStatus

mstratacom.rtm.trapsConfig.trapConfigTable.trapConfigEntry.trapFilterRegisterCategory

stratacom.rtm.trapsConfig.trapConfigTable.trapConfigEntry.managerPortNumber

Step 5 Verify that the ip address to which you are sending the snmpset request is correct

Defect Information—Collect the following information for further analysis:

- Collect RtmProxy.log* and snmpd.log*

Possible alternative workaround—None

C.13.1.2 Not Receiving Any Traps

Traps are not being received on the port with which the manager registered.

Step 1 Verify that the registration with RtmProxy went through successfully. If the registration did not go through, seeC.13.1.1 Registration with RtmProxy Failed.

Step 2 Verify the port number that RtmProxy is sending traps to is the same as the port number on which the trap receive utility or manager is listening. This can be done by

tballraker29% /opt/OV/bin/snmpget -d -v1 -p8161 -t 3000 -r 0 -cpublic 172.28.131.137 stratacom.rtm.trapsConfig.trapConfigTable.trapConfigEntry.managerPortNumber.172.28.131.158

where 172.28.131.137 is the Cisco MGM IP Address and

172.28.131.158 is the Manager IP Address (or IP Address of the station where the trap receive utility is running)

Step 3 Verify that the manager is still registered with RtmProxy. This can be done by doing

tballraker29% /opt/OV/bin/snmpget -d -v1 -p8161 -t 3000 -r 0 -cpublic 172.28.131.137 stratacom.rtm.trapsConfig.trapConfigTable.trapConfigEntry.managerRowStatus.172.28.131.158

where 172.28.131.137 is the Cisco MGM IP Address and

172.28.131.158 is the Manager IP Address (or IP Address of the station where the trap receive utility is running)

The snmp should return 1.

Defect Information—Collect the following information for further analysis:

- Collect the RtmProxy.log* and snmpd.log*

Possible alternative workaround—Re-register with RtmProxy.

C.13.1.3 Manager Gets Deregistered

The Manager keeps getting de-registered from RtmProxy after a while

Step 1 Verify that the Keep Alive script is running. The manager will automatically get de-registered if no snmp is done on any of the tables in RtmProxy. To keep the manager registered with RtmProxy, run the keep alive script in the background, as follows:

```
#!/bin/sh
Usage="$0 <Agent Ip Address> <Manager IP address>"
if [ $# -lt 2 ]
then
echo "Usage :$Usage"
exit 1
fi
managerRowStatus=.1.3.6.1.4.1.351.120.1.1.1.3
managerPortNumber=.1.3.6.1.4.1.351.120.1.1.1.2
lastseq=.1.3.6.1.4.1.351.120.1.3.0
while true
do
sleep 60
CMD="/opt/OV/bin/snmpget -cpublic -p8161 -t3000 -r0 $1 $managerRowStatus.$2 $lastseq"
echo $CMD
$CMD
done
exit 0
```

Step 2 Verify that ip reachablity is not lost of the Cisco MGM station from the station where the manager is running.

Defect Information—Collect the following information for further analysis:

- Collect the RtmProxy.log* and snmpd.log*

Possible alternative workaround—Re-register the manager with RtmProxy

C.13.1.4 Nodal Community Strings Do Not Work

Snmpwalk using the nodal community strings returns error

Step 1 Verify that the snmp request is being issues to port 8161.

Step 2 Verify that the community string is correct.

Defect Information—Collect the following information for further analysis:

- Collect the RtmProxy.log* and snmpd.log*

Possible alternative workaround—None

C.14 Audit Trail Log Problems

This section includes the following information:

C.14.1 Audit Trail Logging Mechanism

This provides Cisco MGM with the ability to record user activities across different modules in a persistent file. All Cisco MGM Java front GUI application will send the information of user activities to Audit Logger server via CORBA interface. Audit Logger server, then, will write the data into the persistent log file.

This section includes the following information:

C.14.1.1 AuditLogger.conf Usage

The following can be configured in the configuration file:

Location of the log file - The default is (/opt/svplus/log/AL).

Number of days - By defining the number of days for the audit trail log files to be kept, all other obsoleted audit trail logs will be deleted automatically.

The name of the user group whose member can read the audit trail log files - it is a standard UNIX user group.

C.14.1.2 Audit Trail Log File Naming Convention

There is one audit trail log file per day. The file name convention is defined as: AuditTrail.<mmddyyyy>.log

Example audit trail log files: AuditTrail.10102001.log for October 10, 2001.

C.14.1.3 Open a Dialog Box in a Cisco MGM GUI, There Is No Record in the Audit Trail Log File

Open a dialog box in a Cisco MGM GUI.There is no open window event for this dialog box logged in the Audit Trail log file.

The detailed step by step debugging for the above is as follows:

Step 1 Open Cisco MGM Security Manager GUI, check the Audit-Read permission for that Cisco MGM GUI in the security profile associated with that particular user.

a. If the Audit-Read permission is not turned on, then no record is the expected behavior. Otherwise, go to step 2.

Step 2 Check if the Audit Logger server is running.

a. Use "psg AuditLogger" on the Cisco MGM machine. If no AuditLogger server is running, here is the problem. Then go to defect information, follow the steps to collect all the information needed.

Step 3 Check if any CORBA related exception thrown on the console.

a. If so, collect those error messages and/or call stacks.

Defect Information—Collect the following information for further analysis:

- Collect all, complete screen snapshots of the Cisco MGM GUI.
- Collect all the errors/exceptions thrown on the console, if any.
- Collect log: /opt/svplus/log/AuditLogger.log*, /opt/svplus/log/LogServer.log*, AuditTrail*.log (file location is set in /opt/svplus/config/AuditLogger.conf), /opt/svplus/log/watchdog.log.
- Collect all the core dump files in /opt/svplus/corefilesdir, especially for those AuditLogger core dump files.

C.15 Miscellaneous Problems

This section includes the following information:

C.15.1 NTS

This section includes the following information:

C.15.1.1 Nodes Stay in Mode 1 After Cold Start

The NTS cannot manage a particular switch successfully. In other words, NTS declared the switch to be in the "Unreachable" or "Unregistered" state. As a result, NTS notified its clients with a LINK_DOWN message. NTS declares a node to be in OK state if it is in the trap manager list of the node and can successfully perform SNMP operations on the node.

Step 1 Check the PING reachability. Run "ntsControl" and enter "ni" at the prompt. Then, enter "q" to exit ntsControl. This shows the NTS node information. A node has to be in OK state so that Cisco MGM can start syncing it up. If the node is not in OK state, first thing to check is PING. Run "ping <ip_address>". If the PING succeeded, go to Step 2. Otherwise, fix the network reachability between the switch and the Cisco MGM station.

Step 2 Check the Cisco MGM IP address configuration This only applies to Cisco MGM workstation with multiple IP interfaces. The NMS_IP_ADDRESS setting in /opt/svplus/config/svplus.conf has to match the interface users chose for Cisco MGM. To check the IP interfaces, run "ifconfig -a". Cisco MGM stations with only one IP interface does not need to have the NMS_IP_ADDRESS setting.

Step 3 Check the Trap Manager List on the switch. SSH or Telnet to the switch. Run "dsptrapmgr" command to show the trap manager list. Check whether the Cisco MGM is in the table. If so, go to Step. 4. Otherwise, if the table is already full, remove unwanted entries with "deltrapmgr" command. The NTS should be able to register the Cisco MGM into the table within a few minutes. If not, go to Step. 4.

Step 4 Check the SNMP community strings. In case the SNMP Community String on the switch has been changed from the default setting, the SNMP Community Strings on the Cisco MGM have to match the new ones on the switch. The SNMP Community Strings on the switch can be viewed with "dspsnmp" command. The setting on the Cisco MGM can be viewed in Domain Explorer.

Defect Information—Collect the following information for further analysis:

- Save the output of "selnd", "dbnds", nts log and EM log of the node in question. < see EM log section>

Possible alternative workaround—If community strings do not match, run the Cisco MGM Configurator GUI to correct them. (/opt/svplus/java/bin/runConfigurator)

Related key index entries: nts, traps

C.15.1.2 Config Change or Provisioning Activity Not Reflected on Cisco MGM

The NTS does not receive any traps from a particular switch when it actually had generated traps.

Step 1 Check if the node is in OK state. If the ntsControl node information says the particular node is not in the OK state, see C.15.2.1 Connection Inconsistency Between the Switch and GUI. If the node is indeed in OK state, go to Step 2.

Step 2 Check the Trap IP address setting on the switch. The Trap IP address has to be the primary IP address of the switch. Otherwise, NTS cannot correlate the trap with the Cisco MGM node information and has to discard that trap. SSH or Telnet to the switch. The primary IP address can be found with "dspndparms" and then "dspifip" commands. Enter "dsptrapip" to see the current Trap IP address setting. Use "cnftrapip" to correct. See C.15.1.3 How To Interpret NTS Log.

Defect Information—None

Possible alternative workaround—None

Related key index entries: nts, traps

C.15.1.3 How To Interpret NTS Log

Locating a specific trap from a particular node in NTS log.

Step 1 Verify Trap Handling

NTS log has information about what are the traps delivered to a specific client. NTS by default keeps 20 old logs in addition to the current one. You can form your "grep" command with the key fields such as node id, trap number, client name and pid. For example:

```
( 21359: 63) 19:24:40 WARNING: N42 Trap(6, 50017, #15668881) to EMC-5-24596
```

The above line says NTS delivered Node 42 Trap 50017 Sequence Number 15668881 to EMC child 5 PID 24610.

In normal case, you see the following cluster for each trap in NTS log.

(21359: 46) 01:46:49 WARNING: N15 Trap(6, 60303, #25278)

(21359: 46) 01:46:49 WARNING: N15 Trap #25278 buffered

(21359: 48) 01:46:49 WARNING: N15 Trap(6, 60303, #25278) to CSA

(21359: 50) 01:46:49 WARNING: N15 Trap(6, 60303, #25278) to RtmProxy

(21359: 60) 01:46:49 WARNING: N15 Trap(6, 60303, #25278) to ooemc-24610

(21359: 58) 01:46:49 WARNING: N15 Trap(6, 60303, #25278) to EMD

(21359: 49) 01:46:49 WARNING: N15 Trap(6, 60303, #25278) to HPOV

line 1 means "Trap(6, 60303, #25278)" is received by NTS.

line 2 means it is successfully buffered by NTS.

line 3 ~ 7 means it is delivered to the clients who registered to receive it in their XML filter setting.

Step 2 If you cannot find the particular trap, verify if the switch is sending traps with a wrong trap IP address. If the switch trap IP is wrong, traps from it is declared as coming from unmanaged node and dropped. The Trap IP address has to be the primary IP address of the switch. Otherwise, NTS cannot correlate the trap with the Cisco MGM node information and has to discard that trap. See C.15.1.2 Config Change or Provisioning Activity Not Reflected on Cisco MGM.

The NTS prints a different message when a trap comes from a node it does not yet manage (unknown node_id), for example:

```
nts.7275.log.old.2:( 7275: 45) 03:32:39 WARNING: Trap unmanaged 172.28.140.16
```

In that case, it prints the IP address only and throw it away.

Defect Information—None

Possible alternative workarounds—None

Related key index entries: nts, log

C.15.2 Data Inconsistency

This section includes the following information:

C.15.2.1 Connection Inconsistency Between the Switch and GUI

This section discusses strategies for debugging inconsistencies between the switch and the Cisco MGM GUI. The inconsistency in this section are not directly related to provisioning. The problems may be caused by coldstart, warmstart or provisioning, but they are noticed sometime after the fact. (i.e. You look at the system and suddenly realize there is an inconsistency).

This section will give a list of steps to try to determine more precisely the cause of the inconsistency. These steps should be performed in order.

1. Verify Node's Sync States
2. Isolate via Database Query
3. Isolate via Message Flow

Step 1 One common reason for inconsistency is nodes in a non-ok state after startup. This will result in connection counts being incorrect or the presence of incomplete connections.

a. Determine if sync-up has been completed.

b. If system has declared sync-up, verify that the nodes which you see inconsistency on are OK (in mode = 3). This can be done using the Cisco MGM CLI command "selnd" The second to last column identifies the mode for a given node.

Step 2 The information displayed on the connection manager GUI is taken directly from the user_connection table. The connection manager is rarely the problem. This section uses database access queries to help isolate the problem. If the problem is found in the user_connection table and the segment tables are incorrect, the problem is usually in EM. If the user_connection table is wrong but the segment tables are correct, we will need to continue with the investigation before we can determine a root cause.

Note All ports in the database and the messages are 0 based and all ports on the switch cli are 1 based. So if the switch said port 3, then you should query for port 2.

a. Query the user_connection table for one of the connections in question. For example, if the connection has a local endpoint of node=n, slot=s, logical_port= p, vpi/dlci = s1, vci = s2 then the query would look like this: "SELECT * from user_connection where l_node_id = n, l_slot = s, l_logical_port = p, l_subchnl_1 = s1, l_subchnl_2 = s2" If you are unsure which side is local and which is remote, try a query with both l_node_id = n and r_node_id = n (and slot, port etc.). If this row in the database is inconsistent with the switch, more investigation is required.

b. Verify that the databroker has received all traps from the EMs. To do this, view the columns inseg_tbl_2, inseg_tbl_2 and inseg_tbl_3. If the flag is set to '1' then all traps for the given segment have been received. These flags tell if the databroker received an add message for the given segment. If they are set to 0 it means the segment trap has not been processed by databroker. If the flag is set to 2 or 3, that means a only one end of the segment has been processed. (note that if the connection doesn't have 3 segments the non-used segments will be defaulted to '1')

c. We should now check the EM connection tables for the connections in question. <see EM section>

d. If we find that the segment tables are correct and the user_connection table is not, or if the inseg_tbl_x flags are not all = '1', we should continue with the testing from the next section. If we see that the segment tables are also incorrect, we should begin looking at the EM for debugging information.

Step 3 In some cases a more detailed review of the message flow between EM and DMD and sDbroker is necessary to determine the source of the error:

a. Verify that DMD received the message from EM. Search message log for the connection. This search is on the DMD first, followed by the sdbroker and xdbroker (xpvc only). The search is ether by connection object ID or node/slot/port/vpi/vci The DMD logs are checked, and if no messages are found then the OOEMC or other EM processes is checked. If the message is found, or the logs are incomplete, then we need to look deeper into the Databroker processes. If the DMD or the EM logs are complete and the message wasn't sent to DMD, then it is most likely an EM issue.

Find the dmd on interest by using the command /opt/svplus/dbcmap -d <node_id> the output will provide you with the dmd whose logs need to be queried.

grep "node <node_id> slot <slot #> .* port <logical_port> .* sCh1 <vpi or dlci> sCh2 <vci>" dmd<dmd_id #>Msg*

Each output line is similar to this:

```
( 7) 21:49:43 1058910582 MsgType=100 connObjId 65665 connStatus 1 secStatus 1
upperLevelAlrm0 oamStatus 0 channelNo -4272512 termination 1 masterFlag 0 wildCardFlag
0 controllerType 0 subType 55 lPercUtil 100 rPercUtil 100 persistentSlave 1
prefRouteId 0 directRouteFlag 0 Local node 11 slot 15 line -1 port 0 logPort 0 sCh1 1
sCh2 37 type 1 subType 0 nni -1 netprefix Remote node 11 slot 14 line -1 port 0
logPort 0 sCh1 32 sCh2 234 type 1 subType 0 nni 0 netprefix
```

Items of interest in the above example are:

21:49:43—time of event

Local node11 slot 15 .... sCh1 1 sCh2 37—This is the local endpoint

Remote node 11 ....—This is the remote endpoint.

MsgType=100—This is the message type of the message. The mapping is:

FEEDER_ADDUPD = 100,

MASTER_SPVC_ADDUPD = 101,

SLAVE_SPVC_ADDUPD = 102,

SINGLEENDSPVC_ADDUPD = 103,

PTOMPSPVC_ADDUPD = 104,

MASTER_PVC_ADDUPD = 105,

SLAVE_PVC_ADDUPD = 106,

MASTER_LOCALDAX_ADDUPD = 107,

SLAVE_LOCALDAX_ADDUPD = 108,

FEEDER_DEL = 109,

MASTER_SPVC_DEL = 110,

SLAVE_SPVC_DEL = 111,

SINGLEENDSPVC_DEL = 112,

SLAVE_SPVC_DEL = 111,

SINGLEENDSPVC_DEL = 112,

PTOMPSPVC_DEL = 113,

MASTER_PVC_DEL = 114,

SLAVE_PVC_DEL = 115,

MASTER_LOCALDAX_DEL = 116,

SLAVE_LOCALDAX_DEL = 117,

WILDCARD_DEL = 121,

grep conObjId xxxxxx dmd<dmd_id>Msg*".

grep "NotifyDataBroker> .*node x slot y .* sub1 v sub2 w" ooemc* < for more EM queries see section on EM>

b. If the DMD received the message but it is not reflected in the database. Identify which databroker module dropped the ball. First check the DMD to see if it forwarded the message. If it didn't check for the reason. The format may be wrong etc. one easy search/grep is node/slot/port/vpi/vci. This is output every time a cache query is done.

grep "DROP MSG: validation error" dmd<dmd_id>.<pid>.* - prints out dropped messages.

c. If the message made it to DMD, we need to see if the sdbroker received the message.

grep "node <node_id> slot <slot#> .* port <logical port> sCh1 <vpi/dlci> sCh2 <vci>" sdbroker*Msg*

d. If it looks like the message was received by the sdbroker but the database does not reflect the change, then we should verify if there is an inconsistency between the databroker Cache and the database. To dump the cache enter:

$ psg sdbroker - the process ID of the sdbroker will be returned

$ kill -USR1 <process id returned from the previous command>

The cache dump will be written to a file in /opt/svplus/log/sdbkrCache.dump Verify if the connection in question is correct in the cache.

Defect Information—We need the logs of the processes on both sides of the interface which the message was dropped. A dump of the specific user_connection table entry that is incorrect is also useful as well as the segment tables for this connection. The specific node, slot, logical_port, vpi, vci of both ends of the connection in question. If a cache dump was done, include that also.

Possible alternative workarounds—If the problem is between the sdbroker cache and the database, a cache resync can be done. TO do this execute the command /usr/usrs/svplus/tools/CacheResync [-t <time in seconds>]. If the problem still exists, collect the defect information.

Related key index entries: inconsistency, connection, databroker

C.15.2.2 Inconsistent Connection Status

The GUI display of 'Status' is from the 'state' field of the user_connection table. The field represents the worst condition of any of the segments in the connection. This field values are:

1 = clear

2 = fail

3 = Down

4 = incomplete

5 = Error

Step 1 If the value is not what is expected, check the connection level databases for each segment to see if they are correct.The last message on the segment in question is the important one.

Step 2 If the status is 'incomplete" it means that one of the segments of the connection is not in the user_connection table, check the "in_seg" flags in the user_connection table entry for this connection. Search the database and messages for the segment that has flag = 0. Also see next step on Error connection.

Step 3 If two master endpoints each have the same slave endpoint, then we have an errored connection. The first connection established will have a status of "error' and the second master endpoint connected to the slave will have a status of 'incomplete".

Defect Information: See C.15.2.1 Connection Inconsistency Between the Switch and GUI .

Possible alternative workaround—See C.15.2.1 Connection Inconsistency Between the Switch and GUI

Related key index entries: inconsistency, connection

C.15.2.3 Inconsistent Connection Secondary Status

The GUI display of 'Secondary Status' is from the 'Secondary_status' field of the user_connection table. The field represents the worst condition of any of the segments in the connection. This field is a bit map with each secondary status using 2 bits. The values of each status entry are

0 = unknown

1 = ok

2 = fail

The bit pattern is:

bits 1-2 local abit

bit 2,4 local ais

bit 5,6 local OAM

bit 7,8 local Conditioned

bit 9,10 remote abit

bit 11, 12 remote AIS

bit 13,14 remote OAM

bit 15, 16 remote Conditioned

Step 1 If the value is not what is expected, check the connection level databases for each segment to see if they are correct. See C.15.2.1 Connection Inconsistency Between the Switch and GUI . The last message on the segment in question is the important one.

Defect Information: See C.15.2.1 Connection Inconsistency Between the Switch and GUI .

Possible alternative workaround—See C.15.2.1 Connection Inconsistency Between the Switch and GUI

Related key index entries: inconsistency, connection

C.15.2.4 Incomplete Connections

A common issue is having 'to many' connections on a given card. This problem may be a result of incomplete connections. For example, if a feeder segment of a three-segment connection has not been processed by databroker, the incomplete connection would have an endpoint of a routing node, not the missing feeder. There would appear to be 'to many' connections on the routing node. A connection can be identified as incomplete if the 'state = 4' in the user_connection table

Step 1 Check the user_connection table for the number of segments and the inseg flags for the connection in question.

a. select num_segs, status, inseg_tbl_1, inseg_tbl_2, inseg_tbl_3 from user_connection where l_node_id = x and l_slot=y and l_port=z and l_subchnl_1 = v and l_subchnl_2 = w.

Defect Information—We need the logs of the processes on both sides of the interface which the message was dropped. A dump of the specific user_connection table entry that is incorrect is also useful. The specific node, slot, logical_port, vpi, vci of both ends of the connection in question.

Possible alternative workarounds—If the problem is between the sdbroker cache and the database, a cache resync can be done. TO do this execute the command /usr/usrs/svplus/tools/CacheResync [-t <time in seconds>]

Related key index entries: inconsistency, incomplete connection

C.15.3 Cisco MGM FTP Daemon

This section includes the following information:

C.15.3.1 FTP Daemon Overview

The cwmftpd process is an ILOG server that allows Cisco MGM modules to request a FTP put, get or directory listing service to and from network nodes or other Cisco MGMs. This server acts as an FTP client from FTP communication stand point and performs services similar to interactive "ftp" program.

The following processes use cwmftpd to ftp the files.

OOEMC

PM Collector

Related key index entries: ftp

C.15.3.2 Generic Troubleshooting

When performing generic troubleshooting, always check the following :

- Check whether 'cwmftpd' process is up and running.

  ```
  psg cwmftpd
  ```

- Check the free disk space.

  ```
  df -k /opt/svplus
  ```

- Check whether target switch/MGM is reachable.
- Check for debug level. If logs are not giving detailed information, debug level can be increased by editing ~svplus/config/cwmftpd.conf.
- Set config parameter, LOG_LEVEL, to 7 to get detailed logs.

Related key index entries: ftp

C.15.3.3 FTP Username and Password

cwmftpd will use the node_info table of stratacom database to retrieve the ftp username and password. For SCM requests scmcollsvr sends the password along with the request.

Related key index entries: ftp, username, password

C.15.3.4 cwmftpd—Files Are Not Transferred Due to Wrong Username/Password

Files are not transferred between Cisco MGM and switch or between Cisco MGMs due to wrong username/password.

The files are not ftp'd between switch and Cisco MGM or between Cisco MGMs due to wrong ftp username/password.

Step 1 Check whether ftp username and password are correct.

Step 2 Check whether cwmftpd.log is having exception like this, if ftp username/password are wrong.

(22589:204248) 10:12:27 ERR: %FtpException-3-LOGIN_FAILED: Login failed.

[login,host=172.23.30.111,user=superuser]

Defect Information—If username/password are correct, but still LOGIN_FAILED are shown in logs, collect cwmftpd.log, cwmftpd.request_log and logs of the process for which files are not getting transferred by cwmftpd.

Related key index entries: login failed.

C.15.3.5 cwmftpd—File Not Available On Switch

Files are not transferred since it file is not available.

Step 1 Check whether file is available in the target switch.

Step 2 Check whether cwmftpd.log is having exception like this.

FtpException-3-FTPERR_550: Requested action not taken. File unavailable (e.g., file not found, no access). [550 File "/stat/1-05-Con-062020031215" not found or permission problem]

Defect Information—If file is available, but file is not ftp'd and FTPERR_550 exception is thrown, then collect cwmftpd.log, cwmftpd.request_log and logs of the process for which files are not getting transferred by cwmftpd and report the problem.

Possible alternative workaround—None

Related key index entries: file unavailable, ftperr_550, requested action not taken.

C.15.3.6 FTP Sessions in Switch

Switch allows only four ftp sessions. When cwmftpd makes a request to open a session, if the switch cannot service the request because it has reached its session limit or if the file is locked, then it will respond with a special error message "499 Session limit reached, queuing <IP address> key <Nodename/XXXXXXXX>".

Key is a unique string for the node that is used later when the session is available. Cisco MGM waits on a TCP Port 5120 for the switch to connect to. When a session is available, switch connects to the pre-defined port and sends the [KEY] as data to Cisco MGM. Cisco MGM uses to <KEY> to identify which switch it needs to open the session with. The session should now be opened without encountering a failure and cwmftpd can proceed with the FTP request.

The switch will reserve the session for the Cisco MGM station for 30 seconds before it services other stations. MGMftpd will retrieve multiple files within a single FTP session. A maximum limit per session will be imposed.

This feature is supported in Cisco MGM 12 and above with MGX 8850 Release 4 and above. For SWSW lower than MGX 8850 Release 4, switch will respond with "421 Session limit reached, closing control connection".

The number of ftp sessions currently opened by switch can be determined by executing the switch command, dsptasks. For each ftp session, 'dsptasks' output will have entry like following.

FtpdServ1 0x9a00a1 0x82d8a8a0

If there are two sessions, there will be two entries.

Related key index entries: switch ftp session

C.15.3.7 421 Session Limit Reached

For SWSW lower than MGX8850 Release 4, switch will respond with "421 Session limit reached, closing control connection" , when it reached the limitation of four ftp sessions.

This is limitation on switch for SWSW lower than Release 4.

Step 1 Check whether really all four sessions are opened by opening a manual FTP session to switch or by switch command - dsptasks.

Step 2 Check whether it succeeds.

Defect Information—If manually opening the FTP session succeeds or dsptasks command shows less than four entries for 'FtpdServ', but still cwmftpd throws FTPERR_421, then report the problem with cwmftpd.log, cwmftpd.request_log and logs of the process for which files are not getting transferred by cwmftpd.

Possible alternative workaround—None

Related key index entries: service not available, closing control connection, 421, session limit reached, ftperr_421

C.15.3.8 499 Session Limit Reached

For SWSW MGX8850 Release 4 and later, switch will respond with "499 Session limit reached, queuing <IP address> key <Nodename/XXXXXXXX>", when it reached the limitation of four ftp sessions.

cwmftpd will throw the exception FTPERR_499, when it tries to connect to a switch which responded with error, "499 Session limit reached, queuing <IP address> key <Nodename/XXXXXXXX>".

Step 1 Check whether really all four sessions are opened by opening a manual FTP session to switch or by switch command - dsptasks.

Step 2 Check whether it succeeds.

Defect Information—If manually opening the FTP session succeeds or dsptasks command shows less than four entries for 'FtpdServ' , but still cwmftpd throws FTPERR_499, then report the problem with cwmftpd.log, cwmftpd.request_log and logs of the process for which files are not getting transferred by cwmftpd.

Related key index entries: 499, session limit reached, key, ftperr_499.

C.15.3.9 Acquiring a Session With Switch

For MGX8850 Release 4 and above, Cisco MGM will wait in predefined port to acquire the session, if it receives "499 Session limit reached" error. This wait time is 1 min by default and configurable. If Cisco MGM won't get response from switch within this wait time, it will timeout and throw the following exception and then again retries to open the session.

(9583: 6) 08:37:29 ERR: %CwmFtpDaemonException-3-SESSION_TIMEOUT: Session [Id[28], ClientSeq#[6521], Host[172.25.69.218], User[superuser], Priority[3]:get /stat/1-04-Con-052920030730 /opt/svplus/spool/MGX98101-1-04-Con-052920030730-2] timeout in 3 minutes and needs to be retried.

It will retry 5 times by default (It is configurable). If all retries fails, cwmftpd will throw the following exception.

(9583:172473) 08:37:58 ERR: %CwmFtpDaemon-3-SESSION_FAIL: Thread [Host [172.2

5.69.218] User[superuser] NoRequest] failed to acquire session after 5 retries. Session wait time[5].

Related key index entries: switch, session, ftp

C.15.3.10 Failed to Acquire Session After All Retries

cwmftpd failed to acquire a session with switch with all retries.

Step 1 Check whether really all four sessions are opened by opening a manual FTP session to switch.

Step 2 Check whether it succeeds.

Defect Information—If manually opening the FTP session succeeds, but still cwmftpd throws SESSION_FAIL exception, then report the problem with cwmftpd.log, cwmftpd.request_log and logs of the process for which files are not getting transferred by cwmftpd.

Possible alternative workaround—None

Related key index entries: session_timeout, session_fail

C.15.3.11 General Log Information

cwmftpd.request_log will have one entry for each request. It will have information about the request is succeeded or failed and how much time it took. It has information in a short/simple format and since there is not much data per request, the file has more data in terms of amount of time.

cwmftpd maintains information based on the IP address of the node. To track request for a particular node, grep for the IP address as the keyword in cwmftp.log and cwmftpd.request_log.

When OOEMC sends FTP requests, it also sends the nodeId along with the request as part of the destination file. This nodeId is used to retrieve the ftp user/password from the node_info table. This can be used for user/password validation.

Following keywords are from cwmftpd.log file.

TRANSFER_STARTED - Specifies that cwmftpd started transferring file.

TRANSFER_COMPLETED - Specifies file is transferred completely and also gives information about local and remote file size.

TRANSFER_RATE - Specifies rate of transfer with no. of bytes transferred and the time.

TRANSFER_RETRY - Specifies that transfer request need to be retried.

TRANSFER_FAILED - Specifies that cwmftpd unable to transfer the file.

CONTROL_CONN_TIMEOUT - This exception will be thrown where there is no transfer of information for X seconds once ftp session is opened.

Related key index entries: ftp log