NN10030-111

Multimedia Communications Portfolio

MCP Management Module

Basics

Standard MCP 1.1 FP1 (02.02) April 2003

NORTEL NETWORKS

Overview

The Management Module is a key component of the Multimedia Communications Portfolio (MCP) infrastructure. It supports the services used to communicate with and manage the network devices and components. The Management Module interacts with the System Management Console allowing Administrators to manage the system.

See the following overview sections for more information:

- “How this guide is organized” on page 3
- “Management Module functions and services” on page 4
- “Management Module interfaces” on page 5
- “Management Module hosting hardware” on page 7

How this guide is organized

This guide contains the following information:

- “Upgrades” on page 11

  Describes the upgrade strategy of the Management Module software.
- “Fault management” on page 15

  Describes the fault management strategy and manual failover of the Management Module.
- “Configuration management” on page 27

  Describes the configuration strategy and the property fields of the Management Module component services.
- “Accounting management” on page 32

  Describes the accounting activities of the Management Module.
- “Performance management” on page 33

Describes the performance management strategy of the Management Module software and hosting servers.

- “Security and administration” on page 36

  Describes the security issues and administrative tasks related to the operations of Management Module services.

Management Module functions and services

The Management Module component provides the services that support the communication between the MCP components and System Management Console. In conjunction with the System Management Console, the Management Module supports the following functionality:

- system operations administration
- system software management
  - — software inventory
  - — software updates
  - — deployment, launch, and monitoring
- system configuration
  - — query, add, modify, delete
- system maintenance
  - — lock and unlock services
  - — i2004 diagnostics
  - — firmware upgrades
- fault monitoring
  - — logs
  - — alarms
  - — archival of logs (which includes fault events)
- system performance monitoring
  - — counters and meters
  - — configurable collection period and archival of performance measurements
- network management interfaces
  - — Extended Markup Language over Transmission Control Protocol (XML/TCP), Perfect Channel Protocol (PCP)
  - — System Management Console

Management Module interfaces

In the MCP system communications scheme, the Management Module sits between the system components and the System Management Console.

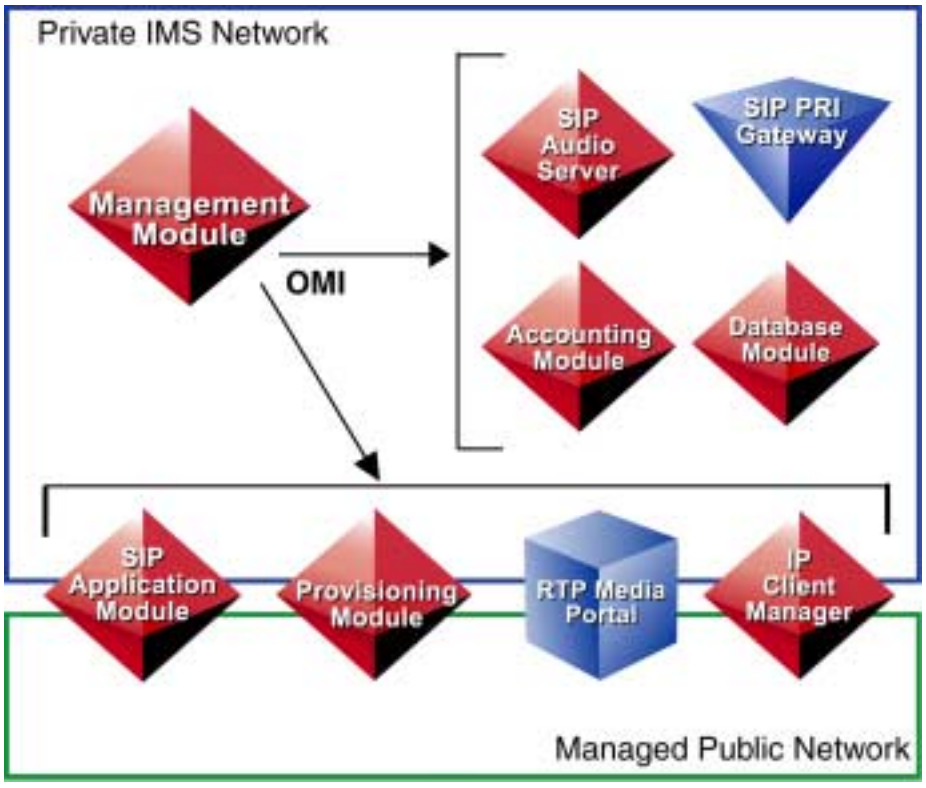
. The following are the interfaces of the Management Module:

- Open management interface (OMI)
- Perfect channel protocol interface (PCP)
- Structured query language interface (SQL)
- Simple network management protocol interface (SNMP)

Open management interface (OMI)

The Open Management Interface (OMI) is used for communicating management and configuration data from the Management Module to each of the managed network elements. The OMI protocol uses XML over TCP.

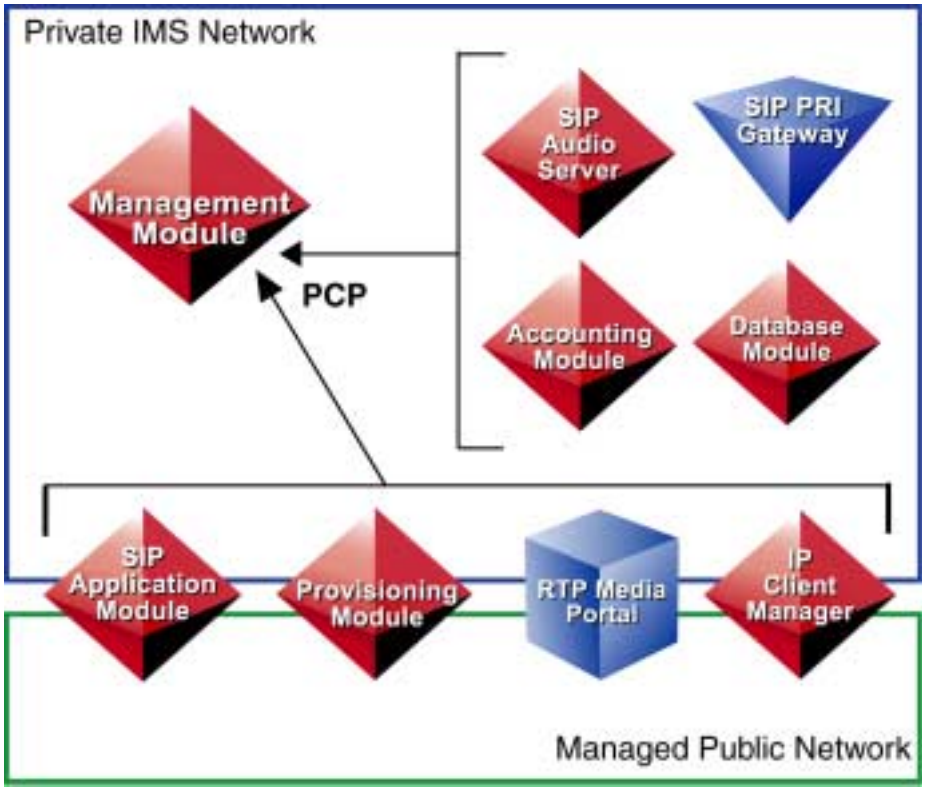
Figure 1 OMI interface logical view



Perfect channel protocol (PCP)

Perfect Channel Protocol (PCP) is used by network elements to communicate performance data, logs, and alarms from network elements upwards to the Management Module for viewing by the System Management Console. PCP is a TCP based protocol.

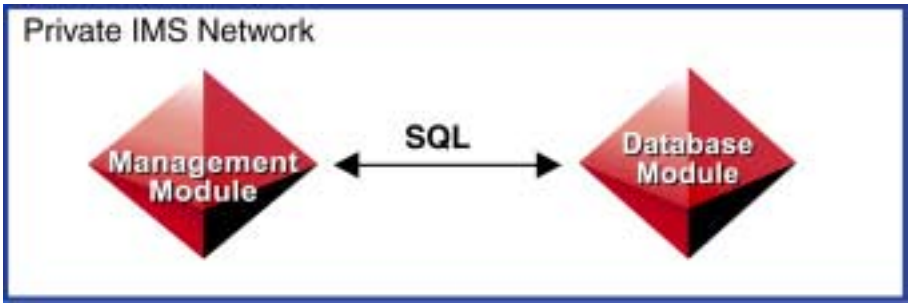
Figure 2 PCP interface logical view



Structured query language (SQL)

SQL (over a Java Database Connection – JDBC) is used for storing and retrieving system configuration data between the Management Module and the Database Module(s).

Figure 3 SQL interface logical view



Simple Network Management Protocol (SNMP)

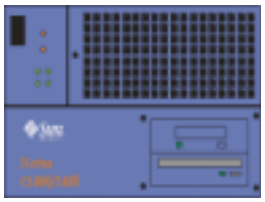
SNMP is used to poll MCP hardware devices for alarm events and operational measurements. Optionally, SNMP can be used to incorporate MCP operational information into an existing network management layer system.

Management Module hosting hardware

The Management Module software resides on two independent servers to ensure high availability. Both servers are either Sun Netra t 1400's (DC power) or 1405's (AC power) connected to a dedicated Sun D1000 disk array.

Hardware details of the hosting servers is described below.

Table 1 Management Module hosting hardware

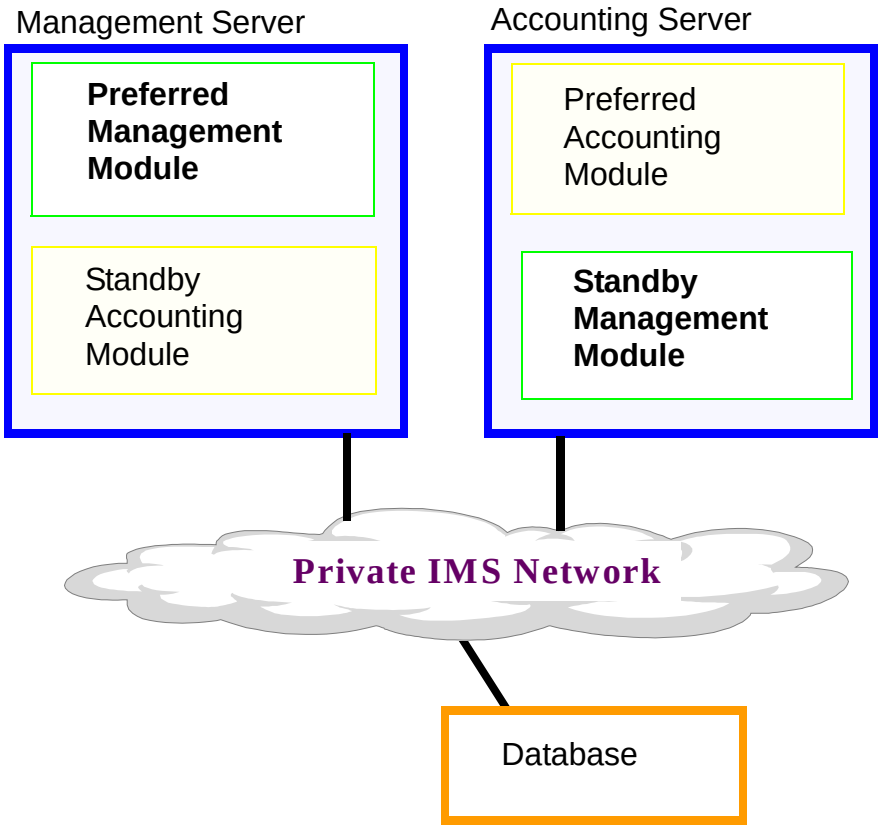
Hardware	Details
Server 	Sun Netra t 1400/t1405 with the following hardware features: • 4 440 Mhz CPUs • 4 GB RAM • 2 36.4 GB disks • 1 10x internal DVD-ROM drive • 1 20 GB 4mm DDS-4 internal tape drive • 1 Quad Fast Ethernet (QFE) PCI card • 1 PCI dual differential Ultra SCSI card • Universal Sliding Rack Mount Kit • 1 Netra T alarm card
Disk array 	Sun Netra D1000 RAID array: • Dual System attachment • 4 36 GB disks • Hot-swap and redundant disk drives

Hardware fault tolerance

The Management Module is hosted on two servers; the management server and the accounting server. The management server hosts the preferred Management Module and standby Accounting Module.The accounting server hosts the preferred Accounting Module and the standby Management Module. This arrangement ensures the high availability of these two fundamental modules. If the management server fails, a manual failover allows the transfer of the Management Module operations to the standby Management Module on the accounting server. Likewise, if the accounting server fails, administrator's can failover the Accounting Module to the standby on the management server. A logical view of the setup is shown in the following figure.

The database stores the system configuration data. The standby Management Module retrieves the latest configuration data from the database when it becomes active.

Figure 4 Management Module redundancy - logical view



Upgrades

Updates to the Management Module software should only be performed with involvement from Nortel Networks.

Management Module updates

For updates, system administrators use a script that automates the manual deployment of a new Management Module version, and the undeployment of the existing version.

> ***Note:*** The script must be executed as a Nortel Networks or root user. In most instances, this will require involvement of Nortel Networks.

When there is an preferred (active) and standby Management Module, the standby can be updated without interruption of Management Module services or the loss of the System Management Console connection. When updating the preferred Module, the Management Module processes are stopped and Management Console connection is lost.

Updating the Management Module software

System administrators require the following information when running the update script.

Table 2 Configuration information needed for deployment

Required configuration information
Management Module software version (load name)
Whether or not the database is replicated
Primary database logical IP address
Secondary database IP address if the database is replicated

Table 2 Configuration information needed for deployment

Required configuration information
Management Module logical IP address
Whether or not a Media Server will be deployed

In addition, the system administrator needs the physical IP address of the server hosting the Management Module being update.

from the administrator workstation

1 Log onto the server hosting the Management Module being updated using the physical IP address of the server.

2 Run the Management Module deploy script.

`/opt/sb/dsm2/bin/mgmtdeploy.pl`

A list of the available versions (loads) will be listed. The following is an example of a load list display:

```
[1] mgmtsvr_all_ims_1.1_build199
[2] mgmtsvr_all_small_ims_1.1_build199
[3] mgmtsvr_all_ims_1.1_build203
[4] mgmtsvr_all_small_ims_1.1_build203
[5] mgmtsvr_all_ims_1.1.1_build215
```

3 The script prompts the system administrator for required configuration information. The script uses the current configuration information to fill in the prompt defaults displayed in the closed brackets [ ].

`Please enter the number of the load to deploy:`

Enter the number of the Management Module version from the displayed list.

`Is the Database Replicated? [Y]:`

Enter either Y or N.

`Enter Machine Logical IP Address - Primary DB [current_ip_address]:`

Enter the logical IP address of the primary database. By default, the script uses the IP address from the current configuration.

`Enter Machine Logical IP Address - Secondary DB [current_ip_address]:`

If the database is replicated, enter the logical IP address of the secondary database. By default, the script uses the IP address from the current configuration.

Enter Machine Logical IP Address - MgmtSvr [current_ip_address]:

Enter the logical IP address of the Management Module. By default, the script uses the IP address from the current configuration.

Will a Media Server (SIP PriGwy or SIP Audio Svr) will be deployed? [Y]:

Enter either Y or N.

4 Once the configuration information is entered, the script lists the entered values.

```
Information obtained for Mgmtsvr
deployment/configuration:

mgmtsvr load name = <Management_Module_load>

Database Replicated = <Y_N>

Machine Logical IP Address - Primary DB =
<logical_ip_address>

Machine Logical IP Address - Secondary DB =
<logical_ip_address_if_DB_replicated>

Machine Logical IP Address - Mgmtsvr =
<logical_ip_address>

Media Server (SIP PriGwy or SIP Audio Svr) will
be deployed = <Y_N>
```

The script prompts the system administrator to confirm the configuration information.

Is the above data correct? [Y]:

5 The system checks for existing loads. The script prompts the user to undeploy the current Management Module version.

Do you want the <existing_load_name> load undeployed? [Y]:

Enter Y to undeploy the current version. When Y is entered, the current load will be undeployed before the new load is deployed.

Various progress and log information messages are sent to the workstation during the undeployment and deployment.

When the Management Module update is finished the following message is displayed:

```
/usr/bin/perl -I/opt/sb/dsm2/bin/ /opt/sb/dsm2
/bin/mgmtsvrUtility.pl /opt/sb/dsm2/bin was
successful
```

6 Log off the server.

The updated Management Module will be in the same state as version before the update. For example, if the Management Module was acting as the standby, the updated module will also be in the standby state.

If the update was performed on the preferred Management Module, the System Management Console connection will have been lost. The connection can now be re-established.

Fault management

The primary fault management information used by administrators are alarms and logs. The Management Module services collect and archive the alarms and logs generated by the system devices and components. Once collected, administrators can view the fault information using the System Management Console.

If a fault results in the preferred Management Module or its hosting server going down, administrators need to perform a manual failover to activate the standby Management Module.

See the following sections for more information:

- “Fault management tools and strategies” on page 15
- “Manual failover of the Management Module” on page 16
- “Manual failover of the Management Module” on page 16
- “Server alert message configuration” on page 21

Fault management tools and strategies

The following System Management Console tools are used for viewing and working with alarms and logs collected by Management Module:

- System Management Console general information area (GIA)

  Administrators use the GIA of the System Management Console to view high level operational information and alarm totals for the Management Module and its hosting server.

- Alarm browser

  Administrators use the alarm browser to view alarms generated by the services of the Management Module.

- Log browsers

  Administrators use the current and archive log browsers to view and save operational event information related to the services of the Management Module. Either a system or a manual action can generate a log. Logs include status and activity reports, hardware or

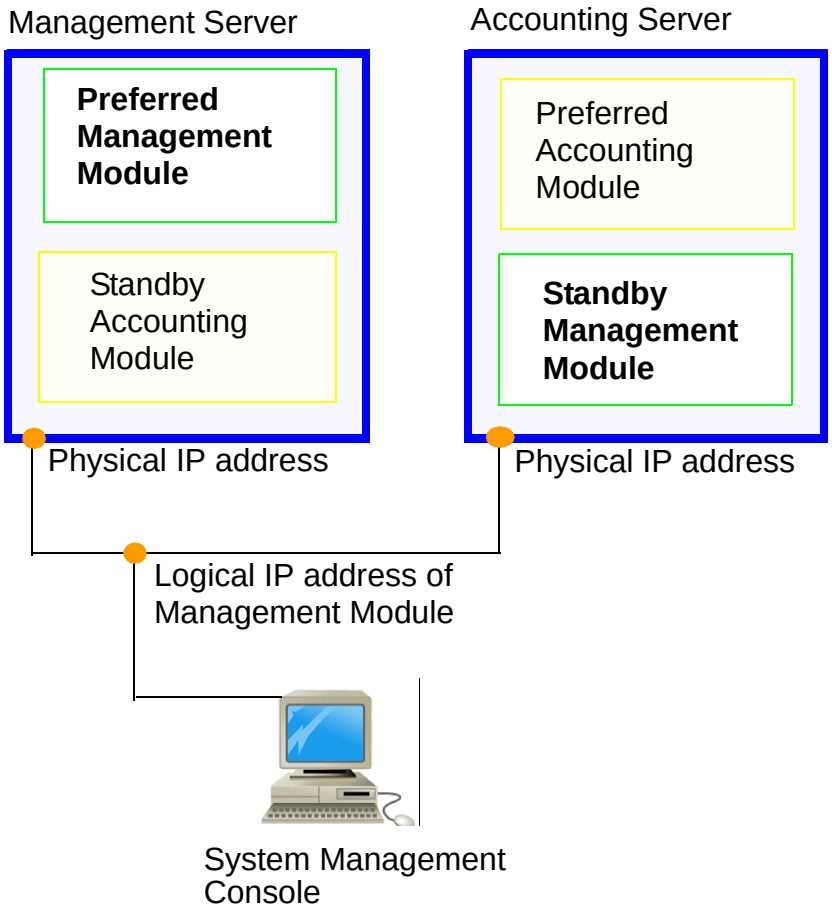
software alarms, changes in state, and other events or conditions affecting the Management Module.

For information on using the System Management Console tools, and alarm and log descriptions, please refer to the *MCP System Management Console Basics*.

Manual failover of the Management Module

Two servers host the Management Module software. The management server hosts the preferred Management Module and the accounting server hosts the standby. If the management server fails, a manual failover allows the transfer of the management operations to the standby Management Module. The active Management Module component owns the logical IP address used to connect with the System Management Console. In addition, all the managed elements use the logical IP address to send logs, alarms, and OMs to the Management Module. A logical view of the arrangement is shown in the following figure.

Figure 5 Redundancy of Management Module - logical view



When the management server or preferred Management Module goes down, the System Management Console loses its connection. In addition, logs and alarms from the managed elements are not reported. To resolve this fault, an administrator needs to perform a manual failover to the standby Management Module hosted on the accounting server.

The manual failover process involves stopping the Management Module processes and releasing the logical IP address from the management server, and starting the processes on the server hosting the standby Management Module. Both actions require the use of a Unix login account.

See the following sections for information on performing the failover task:

- “Determining the management server IP addresses” on page 18
- “Detecting a failure of the active SysMgr component” on page 18
- “Performing a manual failover” on page 18

Determining the management server IP addresses

Administrators need to know the physical IP addresses of the servers hosting the main and standby SysMgr components before performing the manual failover. The physical IP addresses of the servers can be determined by querying the SysMgr component in the management console.

This procedure needs to take place before the fault occurs.

From the System Management Console

1 Open the hierarchy tree to show **MgmSite** > **Servers** > **MgmtSvr** > **Components**.

2 Select the **SysMgr** component.

The information area of the Sytem Management Console displays the physical IP addresses for the preferred and standby servers.

Detecting a failure of the active SysMgr component

When the main SysMgr component or management server fails, the System Management Console losses its connection. The following connection lost dialog box appears on the adminstator’s workstation screen followed by a login prompt.

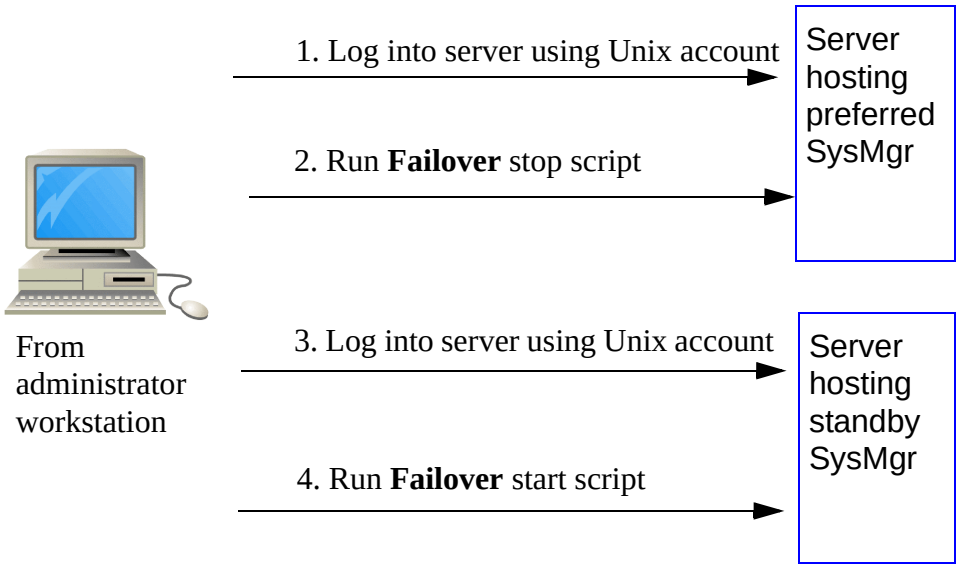
Figure 6 Connection lost dialog box

Performing a manual failover

When a the SysMgr component goes down, its associated processes and ownership of the logical IP address need to be stopped. Since the connection to the System Management Console is lost, administrators need to remotely log onto the servers from their workstation.

To log onto the servers, the administrators need to use the server Unix account. The following figure shows the sequence of actions performed during the failover procedure.

Figure 7 Steps in performing a manual failover



Stopping the Management Module processes

When the SysMgr component goes down, its associated processes and ownership of the logical IP address need to be stopped. Since the connection to the management console is lost, stopping the SysMgr processes requires administrators to remotely log onto the server.

from the administrator's workstation

1 Log onto the server running the active SysMgr component.

IP Address : physical address of server

Login ID : sysadmin

2 Navigate to the directory with the failover script.

```
cd /IMS/mgmtsvr/bin
```

3 Execute the failover shutdown script to stop SysMgr processes and release the logical IP address. The sudo command gives an administrator root priviledges limited to running the failover script.

```
sudo Failover.pl stop sysmgr
```

When the shutdown is finished, the screen will display the name and path of the log file associated with this event.

Starting the backup Mangement Module

Once the backup SysMgr component is started, the logical IP address becomes associated with the newly active SysMgr. Once the logical IP address is up, administrators can reestablish the System Management Console connection.

from the administrator's workstation

1. Log onto the server hosting the secondary SysMgr component.

   IP Address : physical address of server

   Login ID : sysadmin

2. Navigate to the directory with the failover script.

   `cd /IMS/mgmtsvr/bin`

3. Execute the failover startup script to start SysMgr processes and take ownership of the logical IP address.

   `sudo Failover.pl start sysmgr`

   When the startup is finished, the screen will display the name and path of the log file associated with this event.

Reverting back to the preferred Management Module

The procedure to revert back to the preferred Management Module is the reverse of the failover to the standby.

from the administrator's workstation

1. Close the System Management Console connection.
2. Log onto the accounting server running the active standby SysMgr component.

   IP Address : physical address of the accounting server

   Login ID : sysadmin

3. Navigate to the directory with the failover script.

   `cd /IMS/mgmtsvr/bin`

4. Execute the failover script to stop SysMgr processes and release the logical IP address.

   `sudo Failover.pl stop sysmgr`

5. Log onto the management server hosting the main SysMgr component.

   IP Address : physical address of management server

   Login ID : sysadmin

6 Navigate to the directory with the failover script.

```
cd /IMS/mgmtsvr/bin
```

7 Execute the failover script to start SysMgr processes and take ownership of the logical IP address.

```
sudo Failover.pl start sysmgr
```

8 Reestablish the System Management Console connection.

Failover impacts and recovery

Administrators need to be aware of the following system impacts of a Management Module failure and recovery:

- Stopping the preferred Management Module may not be possible due to network isolation of the management server.

  Impact:

  A remote login session may not be possible if the server is in a network isolated state. The standby Management Module can still be started and take ownership of logical IP address. However, if the preferred Management Module comes back online while the standby is running, there will be conflicts between the now two active components.

  Recovery:

  Administrators need to promptly shutdown one of the two active components. If necessary, physically cycle down the power on the management server until the backup Management Module is stopped.

- Running the standby Management Module uses the resources of its hosting server.

  Impact:

  The standby Management module is hosted on the accounting server. When the standby is active, it shares the server resources with the active accounting module. This may result in degraded capacity of both the management and accounting processes.

  Recovery:

  Administrators need to switch the management processes back to the management server as soon as it becomes available.

Server alert message configuration

Alert messages are generated by Solaris operating systems running on the system's Sun servers. The alert messages are normally logged to the local `/var/adm/messages` directory on the server. However, the

server's logs can be routed to the management server(s). Once on the management server, the Management Module's SysLogMonitor will generate alarms when messages from monitored servers match a configured alert pattern. Adminsitrators can then view the alarms in the System Management Console alarm browser.

The alert patterns and routing are configured during system installation and commissioning. However they can be modified to reflect specific system administration requirements after installation.

For information on configuring the SysLogMonitor, see "SysLogMonitor configuration tab" on page 28.

Changing the alert messages to monitor

Modification of alert pattens requires root access to the management server which in most cases requires the involvement of Nortel Networks.

Alert patterns definitions are located on the management server in the file:

```
/IMS/mgmtsvr/data/mgmtsvr/config/SysLogPatterns.dat
```

Each alert pattern is defined in the following format:

```
<severity>;<facility>.<level>;<facility>.<level>;...
```

Where:

<severity>	A numeric value of the alert severity level used to map it to an alarm severity. The mapping is as follows: 4 = Critical alarm 3= Major alarm 2 = Minor alarm 1 = Warning
<facility>	Indicates a Solaris monitored facility such as daemon, kernel, etc. Use an asterisk (*) to include all facilities. See the Solaris documentation for the complete list of facitilities and their descriptions.
<level>	The level of alert message as defined by Solaris such as emerg, crit, etc. See the Solaris documentation for the complete list of alert levels.

Example
4;daemon.emerg;kernal.emerg;*.alert

In the above example, a critical alarm is raised for the server's daemon and kernal facilities with messages with emerg severity level, and all facility messages with alert severity level.

The default patterns and alarm mappings are listed in the following table.

Table 3 Default alert patterns monitored

Alert pattern <severity>	Default patterns being monitored	Management Console alarm severity
4	*.emerg; *.alert	Critical
3	*.crit	Major
2	*.err	Minor
1	*.warning; *.notice	Warning

Note: The <severity> assigned to an alert pattern is not the same as the numeric severity level of the alarm.

from an administrator workstation

1. Log onto the management server. This requires root access.
2. Open the SysLogPatterns.dat file located on the management server located in the following directory path:

   /IMS/mgmtsvr/data/mgmtsvr/config/SysLogPatterns.dat
3. Modify the alert pattern definitions.
4. Log off the management server.

To begin monitoring the new alert patterns, the SysLogMonitor service needs to be restarted using a lock - unlock sequence.

from the System Management Console

1. Select the SysLogMonitor service of the SysMgr component.
2. Right click and select **Lock** from the popup menu.

Figure 8 Locking the SysLogMonitor service

3 Right click and select **Unlock** from the popup menu. The SysLogMonitor restarts and begins raising alarms based on the updated alart pattern definitions.

Adding a server to monitor

Monitored servers are configured during system installation and commissioning. Adding a server to monitor requires manual configuration of the server's syslog file to route alerts to the management server or Management Module component. This configuration requires root access to the added server which in most cases requires the involvement of Nortel Networks.

from an administrator workstation

1 Log onto the server that is being added. This requires root access.

2 Modify the /etc/syslog.conf file on the server, adding the line:

***.emerg;*.alert;*.crit;*.err;*.warning;*.notice @<mgmt_IP>**

where:

<mgmt_IP> is the IP address the alerts are routed to. The following table lists the IP address to use, depending on the network configuration.

Table 4 IP address to route syslog messages

Management Server network scenario	Use the following following IP address to route the alerts
Single management server without IP multipath enabled	Machine IP address of the management server
IP multipath enabled but no management module failover (i.e. single management server)	Logical IP address of the management server
IP multipath enabled and standby management module (i.e. more than one server hosting the Management Module component software)	Logical IP address of the SysMgr component. This IP address is also used in the `/var/adm/messages` directory of the management servers.
Note: Use the private IP address in network that uses both private and public IP addresses.	

This default configuration routes the logs for all facilities generating alerts with the severity of emerg, alert, crit, err, warning, and notice to the management server.

3 Stop and restart the Syslog daemon to apply the changes.

```
prompt> /etc/init.d/syslog stop
prompt> /etc/init.d/syslog start
```

4 Log off the server.

Configuration management

Nortel Networks' personal perform the manual installation and configuration of the Management Module. The installation process adds the management site, management server, and management module component. Only after the Management Module is installed and operational, can administers interact with the system using the System Management Console.

Configuration strategy

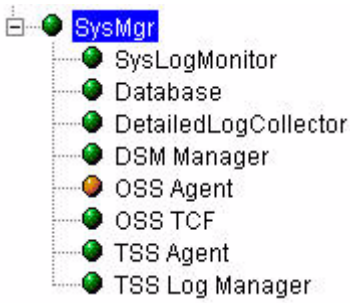
The Management Module component (labelled *SysMgr* in the hierarchy tree) has one service with configurable properties once deployed and operational. All service properties are pre-configured with default values.

Some properties of the management site and management server can be modified to reflect system changes. For information on modifying site and server properties, please refer to *MCP System Management Console Basics*.

Properties of the Management Module services

The Management Module component is made up of eight services. Only the SysLogMonitor service can be modified after deployment. The Database service has properties administrators can query but not modify.

Figure 9 Management Module services in the hierarchy tree



SysLogMonitor configuration tab

The SysLogMonitor service raises an alarm when system alert message logs are generated by servers running Solaris operating systems. The alarm clears after the configured interval. Configuration of servers to monitor is described in “Server alert message configuration” on page 21.

Figure 10 SysLogMonitor configuration tab

Table 5 SysLogMonitor tab property descriptions

Property	Format [default]	Description [range]
MonitoringInterval	Integer [15]	Defines how often (in minutes) the log monitor will raise an alarm if there is new ‘alert msgs’ in the /var/adm/messages file [15-1440 minutes].
MaxNumOfAlert	Integer [3]	Defines the maximum number of alert messages that are included in one alarm [3-10].
AlarmLifeTime	Integer [1]	Defines the time period (in minutes) before the alarm is auto cleared [1-14].

Database configuration tab

The Database service provides the interface that allows communication between the Management and Database modules. Property field descriptions are available in popup windows by moving the curser over the property field name. For information on modifying the Database configuration, refer to *MCP Database Module Fundamentals*.

Figure 11 Database configuration tab

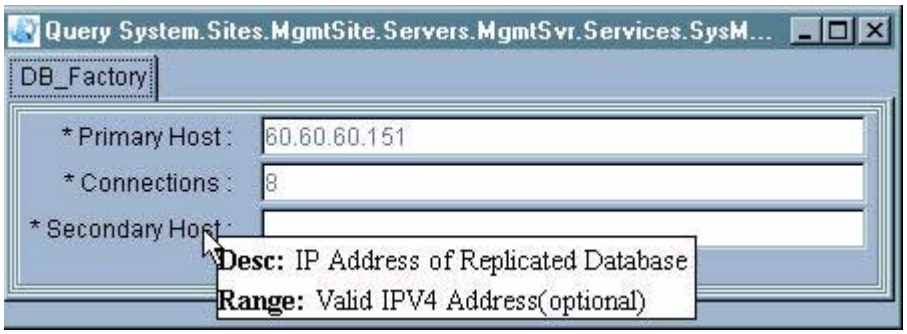


Table 6 Database tab property descriptions

Property	Format	Description
Primary Connection	IP address	IP address of primary database.
Connections	Type: Integer Range: 5 - 256	The number of database connections.
Secondary Host	IP address	IP address of replicated database.

Modifying the SysLogMonitor service properties

Administrators can modify the SysLog Monitor service properties without losing the System Management Console connection.

from the System Management Console

1. Select **SysLogMonitor** from the hierarchy tree.
2. Right click and select **Lock**.
3. Right click and select **Modify**. The configuration widow opens.
4. Modify the property values.
5. Right click and select **Unlock**.
6. Close the configuration window.

Stopping server monitoring

Locking the SysLogMonitor service stops the raising of alarms from server messages.

from the System Management Console

1. Select **SysLogMonitor** from the hierarchy tree.
2. Right click and select **Lock**.

The SysLogMonitor goes into a locked administrative state and no new server alarms are generated. Unlock the SyslogMonitor to restart the service and server monitoring.

Accounting management

Management Module configuration and operations have no impact or involvement in accounting functions.

For information on accounting management, including configuration and operations, refer to the *MCP Accounting Module Basics*.

Performance management

The Management Module collects and archives performance measurements from the MCP hardware and software components. Administrators view the measurements using the System Management Console.

Performance measurements related to the Management Module component are also viewable in the System Management Console.

All operational measurements (OMs) and their descriptions are listed in the *MCP System Management Console Basics* guide.

Performance monitoring tools

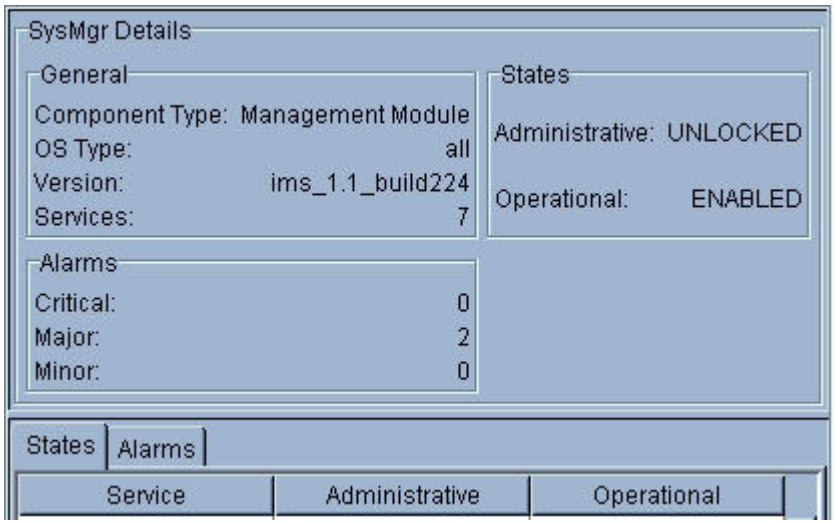
Administrators use the general information area (GIA) and the OM browsers of the System Management Console to view operational states and performance measures. For information on using the System Management Console, refer to the *MCP System Management Console Basics*.

GIA of the System Management Console

When administrators select the server hosting the Management Module in the hierarchy tree, the GIA displays the component's operational state.

Selecting a service of the Management Module in the system hierarchy tree displays the operational state of the service.

Figure 12 GIA displaying Management Module information

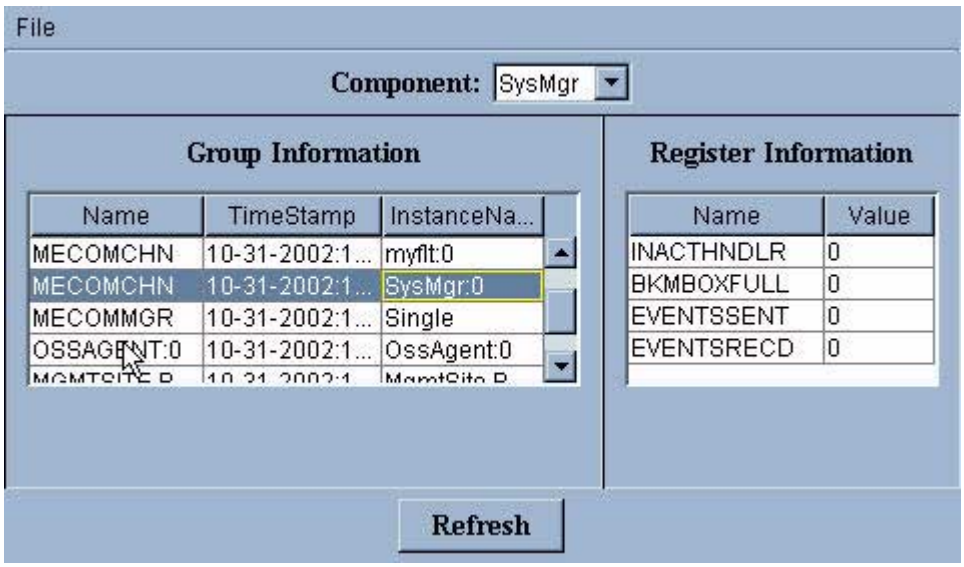


OM browsers

Administrators launch the active OM browser by selecting the server hosting the Management Module component in the system hierarchy tree. In the OM browser, administrators select the Management Module component from the component drop down menu to see active OMs.

All operational measurements (OMs) and their descriptions are listed in the *MCP System Management Console Basics*.

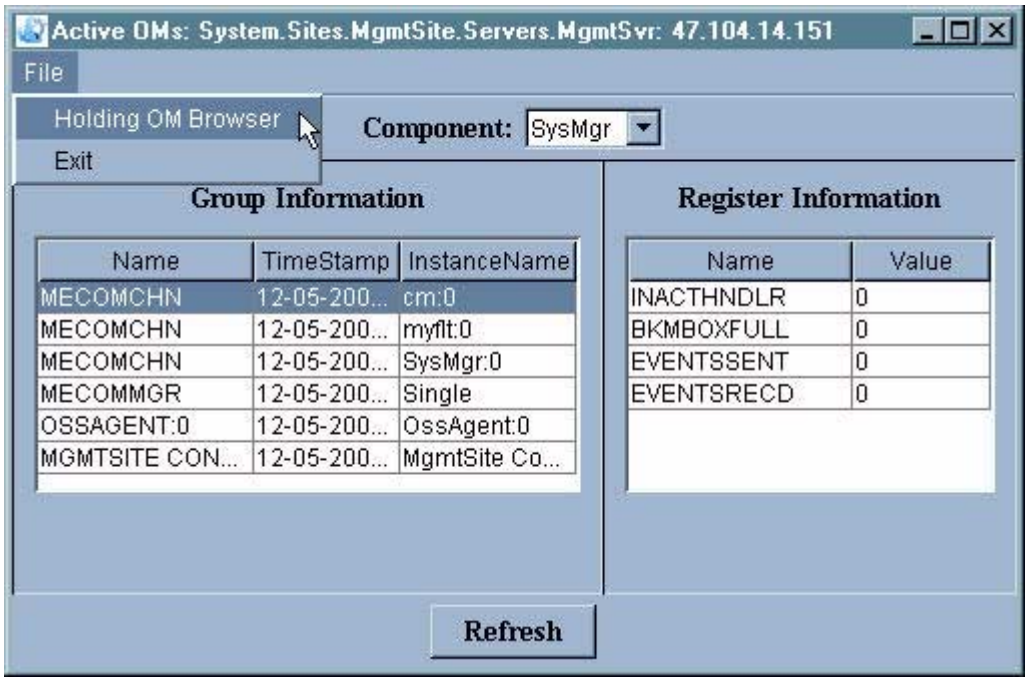
Figure 13 Active OM browser displaying Management Module OM



Once the Management Module component is selected, the Group Information window of the browser displays the OM groups. Select the OM group to display the group's OM in the register information window.

Holding OMs are viewed in the Holding OM browser launched from the Active OM browser menu bar.

Figure 14 Launching the Holding OM browser



Security and administration

Security

The Management Module operates within the private MCP network, isolated from public network security risks. System access is the primary security risk to the Management Module and hosting servers. Access to both are password protected. Access needs to be limited to trusted administrative personnel.

Administrators may need to log onto the server(s) hosting the Management Module software to perform a manual failover procedure. The login requires the use of the password ‘sysadmin’ and the physical IP address of the server.

To prevent non-trusted employees from logging into the servers, it is recommended that both the password and server’s IP address remain confidential.

Administration

There are no special administrative tasks involving the Management Module.

Multimedia Communications Portfolio

MCP Management Module

Basics

Publication number: NN10030-111
Product release: MCP 1.1 FP1 Standard
Document release: Standard MCP 1.1 FP1 (02.02)
Date: April 2003
United States of America