

Multimedia Communication Portfolio

Multimedia Communication Server 5100

FCAPS Summary

MCS 5100 3.0 Standard 03.02 July 2004



MCS 5100 FCAPS Summary

Introduction

The *Multimedia Communication Server (MCS) 5100 FCAPS Summary* document provides information on the MCS 5100 solution and its network elements.

The document is organized as follows:

- [Upgrades on page 5](#)
- [Fault management on page 11](#)
- [Configuration management on page 21](#)
- [Accounting management on page 31](#)
- [Performance management on page 35](#)
- [Security and administration on page 39](#)
- [Appendix A: Downgrade procedures on page 45](#)
- [List of acronyms on page 53](#)



Upgrades

How this chapter is organized

The Upgrades chapter is organized as follows:

- [Strategy on page 5](#)
- [Tools and utilities on page 6](#)
- [Task flows and sequencing on page 7](#)

Strategy

Maintenance releases are supported for all the Nortel Networks components of the Multimedia Communication Server (MCS) 5100 network. A maintenance release allows the current active software to be incremented in order to address emergency or general maintenance requirements. The update mechanism for the MCS 5100 maintenance releases have the following capabilities:

- supports migration of configuration data from one version to the next
- provides software rollback capability for use in the event of software or deployment failure
- bundles the maintenance release software into an update package to decrease the time required to identify the differences between releases and reduce the time required for the overall update process

Maintenance releases are installed and coordinated using both the MCS 5100 and the MAS interfaces.

Software update delivery methods

Nortel Networks can deliver MCS 5100 maintenance release software update packages on a compact disc (CD).

MCS 5100 maintenance release software update bundles are loaded onto the Management Server where property definitions are unbundled to drive the System Management Console. Once this is accomplished,

the software packages are then deployed to the appropriate MCS 5100 components.

For instructions on updating component software, refer to *MCS 5100 System Management Console Basics* and the corresponding component documentation.

Software update contents

Each MCS 5100 software update package contains the following items:

- the core maintenance pack (core application software CD, System Management Console CD, Solaris patch disk, Oracle patch disk)
- applicable OS patches
- Media Application pack (Ad hoc audio conferencing service updates and Windows 2000 service pack)
- Meet me audio conferencing pack (Meet me audio conferencing service updates and Windows 2000 service pack)
- a copy of the Installation Methods of Procedure (MOPs)
- a copy of the Release Notes that outline the content of the maintenance release

Tools and utilities

All software maintenance release updates are implemented from the Management Module through the System Management Console except for the upgrade of the Management Module itself and the Media Application Server. The Management Module update is performed by executing the *mgmtdeploy.pl* script. The maintenance software update bundles are loaded onto the Management Module and then deployed through the System Management Console. Rollbacks also are accomplished from the System Management Console.

To deploy maintenance release software for the Media Application Server, a new installation program is created using an InstallShield™ installation program. During an upgrade, the installation program stops the current Media Application Server framework, replaces its executable, and restarts the Media Application Server framework again. The entire upgrade process takes under one minute to perform.

Note: Patch releases are cumulative, the latest patch bundle installation program will contain all previous patches.

For information on the Management Module and System Management Console, refer to the *MCS 5100 Management Module Basics* and *MCS 5100 System Management Console Basics*. For instructions on

performing component software updates (and rollbacks), refer to the corresponding component documentation.

Task flows and sequencing

This section provides information on the following topics:

- [High-level maintenance update tasks](#)
- [Update tasks](#)
- [Downgrade and roll back tasks](#)

High-level maintenance update tasks

Once the maintenance release update software has been received, perform the following tasks to the target components before the software update bundles can be deployed:

- Update third-party maintenance releases.
- Extract the software update packages to the server hosting the active Management Module.
- Update the Database using the older version of the Management Module and System Management Console.
- Upgrade the Management Module before upgrading the System Management Console.

Note: Do not deploy any other software bundles using DSM. All other bundles should be deployed from the Management Console.

- Install the upgraded System Management Console software on the PCs being used as the administrator's workstation.

For information on installing the updated System Management Console, refer to *MCS 5100 System Management Console Basics*.

Update tasks

The order in which the maintenance release software updates to MCS 5100 are deployed is extremely important. Failure to perform updates in the specified order will result in loss of service.

[Table 1](#) shows the task sequence that the administrator must follow to update the MCS 5100 software components. The table also provides references to the procedures titles from applicable component

documents for the administrator to follow when updating the software components.

Note: Review the Release Notes for specific maintenance release before performing an upgrade because there may be some specific procedures you may need to perform before or in addition to the information available in the component documents.

Table 1 Maintenance release software updates tasks sequence

Step	Task	Procedure title	Document reference
1	Update third-party products with maintenance releases.	Refer to the third-party product documentation.	Refer to the third-party product documentation.
2	Update the Database Module	Updating the Database Module Component	<i>MCS 5100 Database Module Basics</i>
3	Update the Management Module	Updating the Management Module software	<i>MCS 5100 Management Module Basics</i>
4	Update all the System Management Console PCs.	Updating the System Management Console	<i>MCS 5100 System Management Console Basics</i>
5	Update the Accounting Module	Follow the applicable procedure: <ul style="list-style-type: none"> Updating the Accounting Module component in a non-redundant architecture Updating the Accounting Module component in a redundant architecture 	<i>MCS 5100 Accounting Module Basics</i>
6	<ul style="list-style-type: none"> Update the Provisioning Module Update the iPlanet Monitor 	Updating the Provisioning and iPlanet Monitor Module software	<i>MCS 5100 Provisioning Module Basics</i>

Table 1 Maintenance release software updates tasks sequence

Step	Task	Procedure title	Document reference
7	Update the Web Client Manager	Updating the WCM load	<i>MCS 5100 Web Client Manager Basics</i>
8	Update the SIP Application Module	Updating the SIP Application Module	<i>MCS 5100 SIP Application Module Basics</i>
9	Update the RTP Media Portal	Updating the RTP Media Portal Component	<i>MCS 5100 RTP Media Portal Basics</i>
10	Update the IP Client Manager	Updating the IP Client Manager load	<i>MCS 5100 IP Client Manager Basics</i>
11	Update the H.323 Gatekeeper	Upgrading the load or reverting to an earlier load	<i>MCS 5100 H.323 Gatekeeper Basics</i>
12	Update the Oracle Monitor	Updating the Oracle Monitor component	<i>MCS 5100 Database Module Basics</i>
13	<ul style="list-style-type: none"> Update the Media Application Server for Ad hoc audio conferencing services Update the Media Application Server for Meet me audio conferencing services 	Release 2.x to 3.0 upgrade procedures	<ul style="list-style-type: none"> Media Application Server — Ad hoc audio conferencing Basics Media Application Server — Meet me audio conferencing Basics

Note: Please note that the Database Module is the first MCS 5100 component to be updated. Thus, the Database Module is updated using the existing, old version of the Management Module and the System Management Console. Once the Database Module is updated, then the Management Module is updated (from the command line) using the *mgmtdeploy.pl* script, and the new version of the System Management Console is installed onto the administrator's PC. With the Database Module, Management Module, and System Management Console PC updated, all other

MCS 5100 components are updated from the System Management Console except the Media Application Server, which is accomplished through the InstallShield* installation program on the MAS Management Console.

Downgrade and roll back tasks

For information on downgrading a redundant system and downgrading a non-redundant system with a single database, refer to [Appendix A: Downgrade procedures](#) of this document.



Fault management

How this chapter is organized

The Fault management chapter is organized as follows:

- [Strategy](#)
- [Tools and utilities](#)
- [Task flows](#)
- [Disaster recovery](#)

Strategy

As part of its functionality, the Management Module provides fault management for MCS 5100 system components. Fault data is collected from each MCS 5100 core element and then sent to the Management Server. Software and application alarms are transmitted over TCP and consolidated at the Management Module. The Oracle Monitor, iPlanet Monitor, and MCP Trunking Gateway collect SNMP traps and send corresponding alarms to the Management Module. The fault data is formatted into Nortel Networks Standard (STD) logs as well as populated into the Nortel Networks' Reliable Fault Management Information Base (MIB). The formatted data may be sent to the System Management Console. For additional information on the Management Module, refer to *MCS 5100 Management Module Basics*.

The System Management Console views faults and manages the health of the MCS 5100 system and its components. For detailed instructions on using the System Management Console, refer to *MCS 5100 System Management Console Basics*.

In addition to being monitored from the System Management Console, alarms can be polled from the Management Module by the network management system (NMS)

through the use of an SNMP stream:

- SNMPv2c feed for alarms only
- All alarms are logged. Logs are stored to the local disk for a configured retention period of up to seven days. Logs may be viewed from the Management Console GUI. Logs may be exported from the Management Module for further evaluation.

The Media Application Server is remotely monitored and managed from the Management Module of the Media Application Server through the Microsoft Terminal Services Advanced Client (TSAC). TSAC provides remote access capabilities (using TCP/IP) through which the Microsoft Management Console (MMC), residing on the Media Application Server, can be viewed remotely from the Management Module. The Media Application Server MMC provides access to configuration, control, monitoring, and performance reporting capabilities. One of the following applications can be run on each server instance:

- Meet Me conference
- Ad hoc conference
- IM Chat
- Announcements
- Music on hold

Nortel Network's Optivity network management system (ONMS) provides a comprehensive set of discovery, fault, and diagnostic capabilities for identifying problems before they impact network services. In an existing ONMS deployment, MCS 5100 can be monitored using the BPS 2000 as its pass-through. The added value using ONMS is the physical topology representation, some statistical information and troubleshooting, auto discovery, and launch MCS 5100 GUI from the network management system (NMS) GUI.

For a comprehensive list of all MCS 5100 system alarms, refer to the *MCS 5100 System Management Console Basics*. For information about a specific component's faults, refer to the specific component document.

Tools and utilities

The System Management Console monitors all system level and server level MCS 5100 alarms and logs from the core of the solution. You can access the alarm and log browsers from the Tools menu on the System Management Console menu bar or by right-clicking on the specific component.

The rest of this section provides general information on alarms and logs. For more information on alarms and logs and for information on using the System Management Console to monitor alarms and logs, refer to *MCS 5100 System Management Console Basics*.

Alarms

During operation, services may detect faults that represent malfunctions under certain conditions. As these faults occur, alarms are raised by the corresponding services in order to alert the administrator that a problem exists. The administrator has a system-wide view of the alarm conditions.

When an alarm is raised, it is added to a list of currently active alarms. The alarm remains on the active list until it is resolved. Once the problem is resolved, the alarm is cleared and removed from the list of active alarms.

Note: The process of clearing alarms is automatic; you cannot clear alarms manually.

The information displayed in the alarm browser depends on the node selected in the System Management Console hierarchy tree. For example, if a server is selected, the alarm browser will show the alarms for all the components hosted on the server; if a component is selected, only the alarms generated by its hosted services are displayed. Administrators can launch more than one browser, allowing them to view alarms for specific nodes separately.

[Table 2](#) shows all alarm fields viewed in the alarm browser with their descriptions.

Table 2 Alarm attribute

Alarm attribute	Description
Timestamp	The time when the alarm was raised.
Severity	The severity assigned to the alarm (see Table 3).
Originator	The service originating the alarm.
Alarm Name	The name of the alarm.
Probable Cause	The general problem causing the alarm.
Family Name	Family originating the alarm.

There is a severity level associated with each alarm that indicates how serious the problem is. The severity levels that can be assigned to alarms are listed in [Table 3](#).

Table 3 Alarm severity levels

Severity level (and #)	Meaning
Critical (5)	The application is malfunctioning and is incapable of continuing to provide the desired functionality. The application may not recover until the problems have been resolved.
Major (4)	The application is experiencing difficulties in providing the desired level of services and soon may not be able to provide the services any longer.
Minor (3)	The application has detected a problem that is not presently affecting services. Services provided by the application could be affected if the problem persists.
Warning (6)	A problem may have occurred. It is not affecting service or the service can recover by itself.

Alarm log format

You also can view alarms through the log browser on the System Management Console. There is an associated log generated for every alarm generated. Thus, the administrator can search log files (current or archived) for alarm information and the time that the alarm occurred, and (if applicable) when the alarm was cleared.

SNMP alarm reporting

Alarm events are provided through an SNMP management information base (MIB), which includes a local copy of an active alarms table for resynchronization.

For more information on alarms, refer to *MCS 5100 System Management Console Basics*.

Logs

Logs capture and record information about events that occur during service component operation so that events can be analyzed at a later time.

Every log event is captured and archived in Standard (STD) format to disk on the Management Module for a configured retention period of up to seven days.

For more information on logs, refer to *MCS 5100 System Management Console Basics*.

Task flows

Perform all fault management tasks from the System Management Console. The following procedures outline high-level task flows, but do not include all possible tasks.

For more information and detailed procedures, refer to the overview information of each individual MCS 5100 component.

Procedure 1 Alarm analysis

At the System Management Console

- 1 View alarms.
- 2 Analyze alarms.
- 3 View alarm history through the logs.
- 4 Respond to system faults that caused the alarms.
- 5 View logs.
- 6 Analyze logs.
- 7 View log history.
- 8 Respond to system faults and conditions captured in the logs.

Disaster recovery

This section gives information on the following topics:

- [Hardware replacement](#)
- [Power outage recovery procedure](#)
- [Software recovery process](#)

Hardware replacement

The general rule for replacing any hardware is to follow the documentation that comes with the unit. The field replaceable unit (FRU) for MCS 5100 is as follows:

- Sun Fire v100 servers
- IBM xseries 335 Server
- MRV iTouch Terminal Server

Power outage recovery procedure

[Procedure 2](#) provides the steps to recover from a power outage.

Procedure 2 Recovering from a power outage

at the pc

1

ATTENTION

The following shows the preferred order, which is not the way the system comes up if all servers are powered on at the same time.

Power on the database fully. It takes from 5 to 8 minutes for the server to boot and load Oracle.

- 2 After the DBSvr powers on, telnet to the box and run a spot check to make sure it is ready.
 - a Make sure Oracle is loaded. The best way is to telnet to the database. Type **sqlplus** and fill in the user name and password (in other words, log in to as defined database *user*, not *root*). If Oracle is running, you should receive the `SQL>` command prompt. Type **quit** to exit from sqlplus.
 - b Verify that the snmp service is running on the database box. Type: **ps -ef | grep snmp**. You should see three snmp processes:

```
/usr/local/sbin/snmpd -f udp:161
/bin/sh
/opt/app/oracle/product/9.2.0/bin/dbsnmpwd
/opt/app/oracle/product/9.2.0/bin/dbsnmp
```

The snmp processes are not critical to getting the system up. However, if any of the snmp processes are not running, you will not be able to see accurate reporting of this box on the System Management Console.
 - c To stop or start the Oracle database, telnet to the database as sysadmin and then su to root. Go to the following directory: `/etc/init.d`. The stop command is **./dbora stop**. The start command is **./dbora start**. These commands will severely affect service.
- 3 Verify that the SysMgr processes on the MgmtSvr/AcctMgr box are running in order to control the MCS components from the System Management Console. Telnet to the MgmtSvr/AcctMgr box as *nortel*.
 - a Make sure that the SysMgr processes are running by typing: **meinit -p**. You should see three processes running. If any of

these processes are not running, you will not be able to launch the System Management Console:

```
Rel2.0    NTme_pids  mgmtsvr  mgmtsvr.3
```

```
Rel2.0    NTme_pids  tsscma   tsscma.5
```

```
Rel2.0    NTme_pids  tssfpma  tssfpma.6
```

- b** To stop or start the SysMgr, go to the following directory: `IMS/mgmtsvr/bin/mgmtsvr/` and type: **./MgmtSvrShutdown.pl**. This will kill any (or all) of the SysMgr processes.
 - c** To start the SysMgr, stay in the same directory and type **MgmtSvrConfigSetup.pl**. This will try to start all three processes. You will see messages on the telnet session that say something like “starting tsscma waiting 60 seconds.” The tssfpma process will start next, followed by the mgmtsvr processes.
 - d** If you want to watch the SysMgr startup logs, after performing step b above, go to the following directory: `/var/Rel2.0/mgmtsvr`. Then type: **tail -f mgmtsvr.3.log**
 - e** Verify that the snmp process is running on the MgmtSvr/AcctMgr box by typing: **ps -ef | grep snmp**

You should see one process running:
`/usr/local/sbin/snmpd -f udp:161`. If this process is not running or you get an alarm from the System Management Console that there is a problem with the MgmtSvr/AcctMgr's snmp, then kill the process. The process will automatically restart in about 30 seconds.
 - f** When you restart the AcctMgr process, and if any of the components send an alarm in the System Management Console indicating that the component cannot communicate with the primary or backup CAM, then restart the AcctMgr process again. Right click on the Accounting component in the System Management Console and select Restart. Confirm the request. A progress box will pop up and then disappear when the restart has begun. While the Accounting module is rebooting, the other MCS component will throw alarms to the System Management Console, but those will go away when the Acct component is fully operational.
- 4** Now verify the state of the other machines and the MCS components on them. Launch the System Management Console as you normally would. Expand the navigation tree fully so that each component is fully exposed.

- a When you restart the AppSvr and if the clients are having trouble communicating with the AppSvr, then restart the AppSvr again. Right click on the AppSvr component in the System Management Console and select **Restart**. Confirm the request. You should see a progress window and it disappears after the restart has begun. To view AppSvr startup logs, telnet to the AppSvr box (we recommend that you telnet as *nortel*) and go to the following directory: `/var/Rel2.0/appsvr`. Type: **tail -f appsvr.0.log**
- b Verify that the AppSvr's snmp process is running. This step is the same as 3e above.
- c When you restart the IPCM component, and if the i2004 phones are not responding to client registers, the hollow blinking icons in the i2004 display, then restart the IPCM component again. Right click on the IPCM component in the System Management Console and select **Restart**. Confirm the request. You see a progress window that will disappear after the restart has begun. To view IPCM startup logs, telnet to the IPCM box (recommend as *nortel*) and go to the following directory: `/var/Rel2.0/esm`. Type: **tail -f esm.1.log**
- d Verify that the IPCM's snmp process is running. This step is the same as 3e above. Most likely, the Provisioning Module and the WebClient Module are deployed on the same box as the IPCM. Therefore, you only need to verify the snmp service on the box once.
- e When you restart the Provisioning component, the best way to see if the Provisioning Module is behaving properly is to log in to the ProvClient. Launch a web browser to the IP address of the box where the Provisioning Module is deployed, such as `http:192.168.0.10/prov`. Log in as `admin/admin` and attempt any of the List options in the navigation tree, for example, List Devices or List Users. If the browser doesn't respond properly, then restart the Provisioning Module by right clicking on the Provisioning component in the System Management Console and select **Restart**. Confirm the request.
- f When you restart the WebClientMgr component, log in to the Personal Agent through your browser, such as `http://192.168.0.10/pa`. Log in as a subscriber, such as `myusername@mydomain.com`, and enter the subscriber's password. The Personal Agent should appear for that subscriber. If it does not, or the interface does not seem to respond correctly, restart the Provisioning Module described

in 4e above. (If you've already restarted it once and the ProvClient interface seems ok, but the Personal Agent interface is still not working correctly, it is probably a configuration issue.

- g Launch the WebClient GUI from inside a subscriber's Personal Agent page. Attempt to log in to the WebClient when the System Management Console completes loading.

Software recovery process

The software recovery process provides recovery of all operating system, application configuration and program store in the event of a catastrophic server failure. The backup process generates a snapshot of the software suite on a server that allows that server to be recreated after failure.

Server backup should be performed after every configuration change or software update.

The following list shows the sequence of restoring multiple servers.

Note: When you are restoring multiple servers and the server for the Database Module is one of them, then ensure that the server for the Database Module is the first one to be restored.

- Backup the server for the Management/Accounting/Database Modules
- Restore the server for the Management/Accounting/Database Modules
- Backup IP Client Manager/Web Client Manager
- Restore IP Client Manager/Web Client Manager
- Backup RTP Media Portal
- Restore RTP Media Portal
- Backup MCP Trunking Gateway
- Restore MCP Trunking Gateway



Configuration management

How this chapter is organized

The Configuration management chapter is organized as follows:

- [Strategy on page 21](#)
- [Tool and utilities on page 22](#)
- [Task flows on page 22](#)

Strategy

Nortel Networks delivers pre-configured SIP-based IP network solutions. All components within these pre-defined configurations can be ordered separately. Process and tool development is geared to this strategy. As a result, custom engineering is only offered at an additional cost through Nortel Networks Services.

Nortel Networks performs standard installation and base commissioning for the customer. After the base commissioning is done by Nortel Networks, the customer takes over. Nortel Networks and the customer assume different responsibilities to make the network fully operational.

After installation and base commissioning is done by Nortel Networks and Channel Partner, the customer can use the following checklist to verify completion:

- All appropriate hardware equipment and software loads have been installed and loaded as follows:
 - The network is cabled/connected.
 - All cards are installed.
 - Grounding is implemented for safety.
- All network topology (physical characteristics) is implemented as planned.
- Installation validation procedures are complete and components are found to be operational. (For example, when you install and load

software and turn pieces of equipment on, then the equipment is commissioned.)

- The sequence of translations, internal customer testing, and additional services, applications, and features have been planned.

Data can be uploaded from the publishable XML format that is native to the Provisioning Module's OSS. The OSS defines a suite of operations that are applicable to the known provisionable objects (Pos) of the Provisioning Module. The operations are specified according to the Web Service Definition Language (WSDL). Machine agents may use this interface to facilitate the automated flow-through of data to/from the Provisioning Module. OPI would be used for the purpose of transporting provisioning data from the OSS to the MCS 5100.

Tool and utilities

The configuration of the MCS 5100 SIP-based IP network has three phases—deploying and configuring the MCS 5100 components and network elements and provisioning the MCS 5100.

The tool for deploying and configuring all MCS 5100 components and network elements is the System Management Console.

The tool for provisioning the MCS 5100 is the Web-based Provisioning Client. A command line interface (CLI) tool also is provided to enable bulk provisioning. The Bulk Provisioning Tool provides a command set for bulk provisioning tasks, such as the query/import of data to/from flat files and to update/delete data based on flat file input. For more information, refer to the *Bulk Provisioning Tool Reference Guide*.

Task flows

Configuration management and provisioning tasks can vary from one MCS 5100 deployment to another. However, most of these high-level tasks for configuring MCS 5100 components and network elements and for provisioning MCS 5100 domains are identified in the following sections:

- System Management Console configuration tasks
- Provisioning Client provisioning tasks
- Media Application Server configuration tasks

When configuring a new MCS 5100 system at deployment, you should configure the managed objects on the different nodes and bring everything online before beginning provisioning tasks.

System Management Console configuration tasks

[Table 4](#) shows the sequence of the MCS 5100 component and network element configuration tasks that a administrator must follow from the System Management Console.

Table 4 System Management Console configuration tasks sequence

Step	Description	Tasks
1.	Configure MCS 5100 system level elements (add/remove sites, servers, and MCS 5100 service components)	Add/remove sites, servers, and MCS 5100 service components. Note: Before you can delete a server, you must delete all the service components for that server. Similarly, before you can delete a site, you must delete all the servers from that site.
2.	Configure the Accounting Module.	From the System Management Console: <ul style="list-style-type: none">• Select the server to host the Accounting Module.• Select Components>Add > Component. The load list window opens.• Select the software version to install and click Apply. The component configuration window opens. There are separate tabs for each component service with configurable properties.• Configure the Accounting Module Service Component Name.• Configure the properties within the Central Accounting Module tab.

Table 4 System Management Console configuration tasks sequence

Step	Description	Tasks
3.	Configure the SIP Application Module.	<p>From the System Management Console:</p> <ul style="list-style-type: none"> • Select the server to host the SIP Application Module. • Select Components>Add > Component. The load list window opens. • Select the software version to install and click Apply. The component configuration window opens. There are separate tabs for each component service with configurable properties. • Configure the SIP Application Module Service Component Name. • Configure the properties within all tabs of the SIP Application Module.
4.	Configure the IP Client Manager.	<p>From the System Management Console:</p> <ul style="list-style-type: none"> • Select the server to host the IP Client Manager • Select Components>Add > Component. The load list window opens. • Select the software version to install and click Apply. The component configuration window opens. There are separate tabs for each component service with configurable properties. • Configure the IP Client Manager Service Component Name. • Configure the properties within all tabs of the IP Client Manager.
5.	Deploy the UFTP bundle (required for i2002 and i2004 Internet Telephone firmware downloads).	<p>From the System Management Console:</p> <ul style="list-style-type: none"> • Select the server to host the UFTP bundle. • Select Components>Add > BaseSoftware. The load list window opens. • Select the software version to install and click Apply.

Table 4 System Management Console configuration tasks sequence

Step	Description	Tasks
6.	Configure the Provisioning Module.	<p>From the System Management Console:</p> <ul style="list-style-type: none">• Select the server to host the Provisioning Module• Select Components>Add > Component. The load list window opens.• Select the software version to install and click Apply. The component configuration window opens. There are separate tabs for each component service with configurable properties.• Configure the Provisioning Module Service Component Name.• Configure the properties within all tabs of the Provisioning Module.
7.	Configure the Web Client Manager.	<p>From the System Management Console:</p> <ul style="list-style-type: none">• Select the server to host the Web Client Manager• Select Components>Add > Component. The load list window opens.• Select the software version to install and click Apply. The component configuration window opens. There are separate tabs for each component service with configurable properties.• Configure the Web Client Manager Service Component Name.• Configure the properties within all tabs of the Web Client Manager.

Table 4 System Management Console configuration tasks sequence

Step	Description	Tasks
8.	Configure the RTP Media Portal.	<p>From the System Management Console:</p> <ul style="list-style-type: none">• Select the server to host the RTP Media Portal.• Select Components>Add > Component. The load list window opens.• Select the software version to install and click Apply. The component configuration window opens. There are separate tabs for each component service with configurable properties.• Configure the RTP Media Portal Service Component Name.• Configure the properties within all tabs of the RTP Media Portal.

Table 4 System Management Console configuration tasks sequence

Step	Description	Tasks
12.	Configure the Oracle Monitor.	<p>From the System Management Console:</p> <ul style="list-style-type: none"> • Select the server to host the Oracle Monitor. • Select Components>Add > Component. The load list window opens. • Select the software version to install and click Apply. The component configuration window opens. There are separate tabs for each component service with configurable properties. • Configure the Oracle Monitor Service Component Name. • Configure the properties within all tabs of the Oracle Monitor.
13.	Configure the iPlanet Monitor.	<p>From the System Management Console:</p> <ul style="list-style-type: none"> • Select the server to host the iPlanet Monitor. • Select Components>Add > Component. The load list window opens. • Select the software version to install and click Apply. The component configuration window opens. There are separate tabs for each component service with configurable properties. • Configure the iPlanet Monitor Service Component Name. • Configure the properties within all tabs of the iPlanet Monitor.

For more information about configuration management and for instructions for performing configuration tasks at the sites and server levels, refer to *MCS 5100 System Management Console Basics*. For information on performing configurations tasks of MCS 5100 components, refer to the corresponding component documentation.

Provisioning Client provisioning tasks

[Table 5](#) shows the sequence of the provisioning tasks that a administrator must follow from the Provisioning Client.

Table 5 Provisioning Client provisioning tasks sequence

Step	Description	Task(s)
1.	Define roles and rights and use to create a new Administrator.	Add role and assign rights.
		Add Admin.
2.	Define new domain(s).	Add domain(s).
		Add sub-domain(s) if required.
3.	Define service parameters and assign to domain(s).	Define service parameters.
		Assign services to domain.
4.	Define domain service package.	Create service package.
		Assign service package(s) to domain(s) and sub-domain(s).
		Assign services to sub-domain(s).
5.	Define voice mail servers and assign to domain(s).	Add voice mail server (SIP/Trunk/Line) and assign to domain(s).
6	Add IPCM and assign to domain.	Add IPCM.
		Assign IPCM to domain.
7	Add domain status reason(s).	Add reason.
8	Add users to domain(s).	Add user(s).
		Add user(s) to sub-domains.
		Add i2002 and i2004 device properties.
9	If not autoprovisioning, assign devices to domain(s).	Add device.
		Assign users to a device.

Table 5 Provisioning Client provisioning tasks sequence

Step	Description	Task(s)
10	Define gateway, gateway routes, and trunk groups.	Add gateway.
		Add gateway route.
		Add trunkgroup.
11	Define domain telephony routes and parameters.	Add routing Class of Service (COS).
		Add telephony routes: Private, SIP, or Gateway.
		Change routing parameters.
		Add route list.
12	Define banned users for a domain.	Ban users.

For more information on Provisioning Client provisioning tasks and instructions for using the Provisioning Client to perform these tasks, refer to the *Provisioning Client User Guide*.

Media Application Server configuration tasks

Perform the following steps for proper operation of a Media Application Server (MAS) and the MAS-based service that resides on the Media Application Server:

- network configuration – configuring connectivity to the Media Application Server where a particular MAS-based service will reside.
- service configuration – configuring connectivity to the MAS-based service.

Network configuration

To allow the Media Application Server to communicate with the rest of the network, the system administrator must provide the following information during the installation of the Media Application Server:

- SIP UDP port – The signaling port where SIP messages will originate and terminate to this Media Application Server.
- SIP Application Servers – The address(es) of SIP Application Module(s) that this Media Application Server allows incoming service requests to come from. Incoming service request messages

from nodes not configured for this Media Application Server are rejected.

For complete information on configuring the Media Application Server during installation, please refer to the *Media Application Server - Installation Module*.

Service configuration

After network configuration of the Media Application Server is completed, the services that will be hosted on the Media Application Server must also be configured. The service configuration steps are unique for each MAS-based service. In general, configuring a service consists of two steps:

- creating a service access point
- associating routes to the service access point

For more information about the service configuration steps required by a specific MAS-based service, refer to the *Configuration* chapter of the document describing that particular MAS-based service.



Accounting management

How this chapter is organized

The Accounting management chapter is organized as follows:

- [Strategy on page 31](#)
- [Tools and utilities on page 32](#)
- [Task flows on page 32](#)

Strategy

The accounting management system for the MCS 5100 provides the framework for collecting, formatting, and transmitting accounting data from the MCS 5100 system to the service provider's back-end billing system. It is comprised of two logically separate entities:

- Local Accounting Manager (LAM), which resides on the SIP Application Module
- Central Accounting Manager (CAM), which resides on the Accounting Module

Local accounting manager

The primary function of the LAM is to collect raw accounting data from active sessions on the SIP Application Module and transport it to the CAM.

The MCS 5100 call model is event-based. Certain triggers in a call/session/transaction generate a raw data record on the SIP Application Server. For example a basic SIP-to-SIP call generates four accounting records. This raw data record is also referred to as a recording unit (RU). Trigger examples may be service initiation, session answer, session, and reject.

The LAM resides as part of the SIP Application Module. Its prime function is to collect and store accounting information as events occur in raw format on the local machine and then forward the information to the CAM.

Central accounting manager

The Central Accounting Manager is an application and referred to as the Accounting Module. The functions of the CAM include:

- accepting and formatting the raw accounting data (recording units) received from the LAM into IPDR/XML records
- store IPDR/XML records on disk until manually removed
- depending on configuration, transmit IPDR/XML records to pre-configured destinations via TCP/IP or FTP Push or Pull

The Central Accounting Manager accepts the Recording Units and formats the data to IPDR-like record.

High availability of the accounting management system

To ensure high availability of the accounting management system, the minimum MCS 5100 network configuration consists of four Sun Fire v100 Servers. One Server is for Management and Accounting Modules, one for the Database Module, one for IP Client Manager and Web Client Manager, and one for the Application Server. However, this minimum configuration does not offer redundancy. For redundancy, the customer requires eight Sun Fire v100 servers configuration. The LAM only runs in the SIP Application Module.

Since many SIP Application Modules can run in a site, there can be many LAMs connecting to the CAM.

For additional information on MCS 5100 Accounting Module, refer to *MCS 5100 Accounting Module Basics*.

Tools and utilities

The MCS 5100 accounting management system is configured, monitored, and maintained through the System Management Console. For more information on the MCS 5100 accounting management system, refer to *MCS 5100 Accounting Module Basics*. For information on using the System Management Console to configure, monitor, and maintain the accounting management system, refer to *MCS 5100 System Management Console Basics*.

Task flows

This section identifies the high-level MCS 5100 accounting management tasks. The specific tasks you need to perform for your accounting management system will vary depending on the level of support purchased for your MCS 5100.

Accounting management tasks

The accounting system is configured during the deployment of the Accounting Module (CAM) and SIP Application Module (LAM) components.

Accounting Module properties are configured under the Central Accounting Manager tab on the Accounting Module within the System Management Console and cannot be modified in real-time.

The CAM is configured for

- Data Transport Protocol
 - CAM IP address
 - Primary CAM port
 - Recovery CAM port
- file management
 - file rotation size
 - file rotation time
 - file compression
- disk full condition
 - disk monitor major threshold
 - disk monitor critical threshold
- TCP/IP transport to OSS
 - TCP/IP enabled
 - TCP/IP address
 - TCP/IP primary host port
 - TCP/IP recovery host port
- FTP transport to OSS
 - FTP push enabled
 - primary FTP directory
 - recovery FTP directory
 - remote FTP node ID
 - FTP user ID
 - FTP user password

Local Accounting Manager properties are configured under the Local Accounting Manager tab for the SIP Application Module within the

System Management Console and cannot be modified in real-time. For further information, refer to *MCS 5100 SIP Application Module Basics*.

The LAM is configured for

- file management
 - file rotation size
 - file rotation time
- disk full conditions
 - disk monitor major threshold
 - disk monitor critical threshold

For details on all task flows for MCS 5100 accounting management, detailed procedures for performing these tasks, and details on the accounting records produced, refer to *MCS 5100 Accounting Module Basics*.



Performance management

How this chapter is organized

The Performance management chapter is organized as follows:

- [Strategy on page 35](#)
- [Tools and utilities on page 36](#)
- [Task flows on page 36](#)

Strategy

Performance measurements (PMs) are statistics collected about the system. Performance is measured by operational measurements (OMs).

OMs provide statistical information on the server operations and performances. OMs are usually represented in terms of groups, which contain registers (counters and gauges) that provide performance related data. For example, call processing can provide an OM group related to call control and an OM group related to call progress. One group provides data such as number of successful calls, number of calls rejected, unauthorized attempts, while the other group provides data such as average call holding time, duration of a call, and so on.

There are two types of OMs: active and holding. Active OMs are displayed as they are reported by the server to the System Management Console. Holding OMs have already been archived to files on the Management Module.

As the OM group registers are updated, they are collected into an OM report. A snapshot of this report can be viewed through the OM Browser located on the System Management Console.

MCS 5100 OM data belongs to one of the following categories:

- Platform-related OMs—obtained from the SNMP agent(s) at the MCS 5100 components and System Manager Node. The OMs are then channeled through the MCS 5100 management framework.

Note: This method applies only to Database Module and Provisioning Module, not to the entire system.

- MCS 5100 applications-related OMs—obtained through the MCS 5100 management framework.

Service provider can access OMs through FTP or view OMs using the OM Browser on the System Management Console. OMs for MCS 5100 are collected and archived at the Management Module in a comma separated value (CSV) file format. These files then can be accessed through FTP by a performance management (PM) System.

For more information on OMs and a comprehensive list of all MCS 5100 OMs, refer to *MCS 5100 System Management Console Basics*.

Tools and utilities

The Management Module provides the performance management framework for all MCS 5100 components. The system administrator can configure performance data collection and reporting from the Management Console by selecting the “OAM Configuration” menu item. The OAM Configuration menu option is available when the system administrator selects a deployed application or the “System” node in the system hierarchy tree and then right clicks (to display the pop-up menu). In addition, the system administrator can monitor performance data from the OM browser on the System Management console. For information on using the System Management Console to perform performance management tasks, refer to the *MCS 5100 System Management Console Basics*.

Task flows

Performance tasks for the various MCS 5100 components are documented in detail in the performance information provided for each individual MCS 5100 component. The following list of performance management tasks may not apply to every component. In addition, the order in which these tasks must be performed may vary from component to component. However, typical MCS 5100 performance management tasks include the following activities.

Procedure 3 Performing MCS 5100 Performance Maintenance Tasks

At the System Management Console

- 1** Retrieve/view current performance data
- 2** Retrieve/view archived performance data
- 3** Configure performance data collection
- 4** Configure performance data reporting



Security and administration

How this chapter is organized

The Security and Administration chapter is organized as follows:

- [Security on page 39](#)
- [Administration on page 40](#)

Security

Security Strategy

For the MCS 5100 Solution, Nortel Networks has incorporated security mechanisms within the SIP protocol for registration and *invite* messages. Customer must implement authentication using Digest. Digest scheme is based on a challenge-response approach. Digest scheme makes a challenge using a nonce value. Valid response includes a *checksum* (MD5 by default - IETF 1321) of the username, password, given nonce value, the method, and the requested address/URI. This ensures that the password is not sent in clear. Additionally, an optional header allows the server to specify the algorithm used to create the *checksum* or Digest. As mentioned, MD5 algorithm is used by default. Also, user is authenticated with a username and password. Endpoints are identified by unique URLs. For more information on the MCS 5100 security strategy, refer to the *MCS 5100 Network Engineering and Deployment Guide*.

Administration

Tools and utilities

The tools for performing MCS 5100 administration functions are as follows:

- **System Manager Console**—Depending on the level of administration access and security privileges, use this GUI to
 - add sites and servers
 - to deploy and configure MCS 5100 components
 - perform maintenance functions, such as login/logout,
 - display system topology in a directory tree
 - use maintenance commands
 - edit properties
 - browse alarms, logs and performance metrics
 - monitor admin and operational states
- **Provisioning Client Module**—Provisioning administrators use this tool to manage subscribers at the provider and enterprise domain level.
- **Personal Agent**—This web-based GUI is used by the system administrator. It is also used by the subscriber, for example, to register and fill in person details according to the limits defined by the Domain Administrator/Administrator. It allows the user to
 - enroll for services
 - register their PC with the proxy server to answer and place SIP calls
 - view logs of missed calls
 - keep a personal phone directory
 - maintain routing information

Task flows

Use the administration tools to perform the following tasks. The tasks and the order in which they must be performed may vary from component to component. For detailed information on task flows, refer to the overview information of the individual MCS 5100 component or to the manufacturer's documentation that comes with the product, for example, the Sun Microsystems's documentation on Sun Fire V100 servers.

Administration tasks for the System Management Console

An administrator who manages subscriber information may perform the following types of tasks:

- adding a user
- deleting a user
- editing user information
- reviewing audit trail
- changing passwords
- setting privileges
- modifying a user
- listing a user

Additionally, an administrator may perform the following tasks:

- accessing/starting an element
- configuration tasks, such as
 - deploying, monitoring, modifying, and restarting the element manager
 - changing system behavior
- performance monitoring tasks, such as
 - monitoring disk space usage
 - checking operational measurements
 - setting thresholds
 - checking alarms
- provisioning tasks, such as
 - Gateway routing changes
 - domain/subscribers information
 - device information
 - voice mail information
 - service packages
 - IP Client Manager
 - administrators
- managing access control (user IDs and passwords)

Note: Only users configured as “system administrators” of the System Management Console are allowed to add/delete/modify

user information. This capability can be further extended to domain information administration.

- backing up and restoring system and database includes
 - manually backing up and restoring the operating system, database, and MCS 5100 software
 - saving data to a remote external device using shell scripting (This method is used because the Vega 100 platform does not contain SCSI or DAT drive.)

Administration tasks for the Provisioning Client

Administrators can create, or define, all the necessary provisioning roles to support their system. They can allow or restrict provisioning roles to carry out specific actions. [Table 6](#) provides examples of several administrator provisioning roles and the “rights based” restrictions associated with various provisioning tasks.

Table 6 Examples of roles and rights of administrators

Provisioning role example	Rights given	Allowed tasks
User administrator	<ul style="list-style-type: none">• User management with read, write, and delete access• Domain management with read access only	Can view domain details, and add, delete, or modify users. Does not have access to other parts of the system, for example voicemail, service packages, and so forth.
Device administrator	<ul style="list-style-type: none">• Domain management with read access• Device management with read, write, and delete access	Cannot add or modify users. Can add, modify or delete devices.
System administrator	Full domain access	Can see all domains, regardless of who created the domain, or the list of domains provisioned against the administrator.

Diagnostic tools

Use the following diagnostic tools to debug system problems:

- Unix commands such as “netstat -r,” “ping,” and traceroute
- Monitoring logs, alarms, operational measurements, and syslog
- Audits such as the Long Call Duration
- Loopback IP address testing on all physical ports provided by Sun Microsystems
- snoop (sniffer) or port mirroring on Ethernet switch, with sniffer connected to mirrored port, for monitoring messages
- Sun IP Multipathing for signals to switch physical interfaces upon detection of loss of the link



Appendix A: Downgrade procedures



CAUTION

It is recommended that you perform downgrade procedures only in the **rare case** that the upgrade to the maintenance release software fails. Do not perform these procedures at any other time.

The update operation on the System Management Console allows administrators to either upgrade the network components to future maintenance releases, or downgrade the network components to a previous maintenance release. Rollbacks or downgrades of the Database Module is only successful when downgrading to a previously running maintenance release.

If a failure occurs during the upgrade process for any component, an automatic rollback is usually performed. An indication of this automatic rollback is displayed on the System Management Console. However, when an upgrade failure for network components occurs in a non-redundant architecture, an automatic rollback of the Database module is not performed.

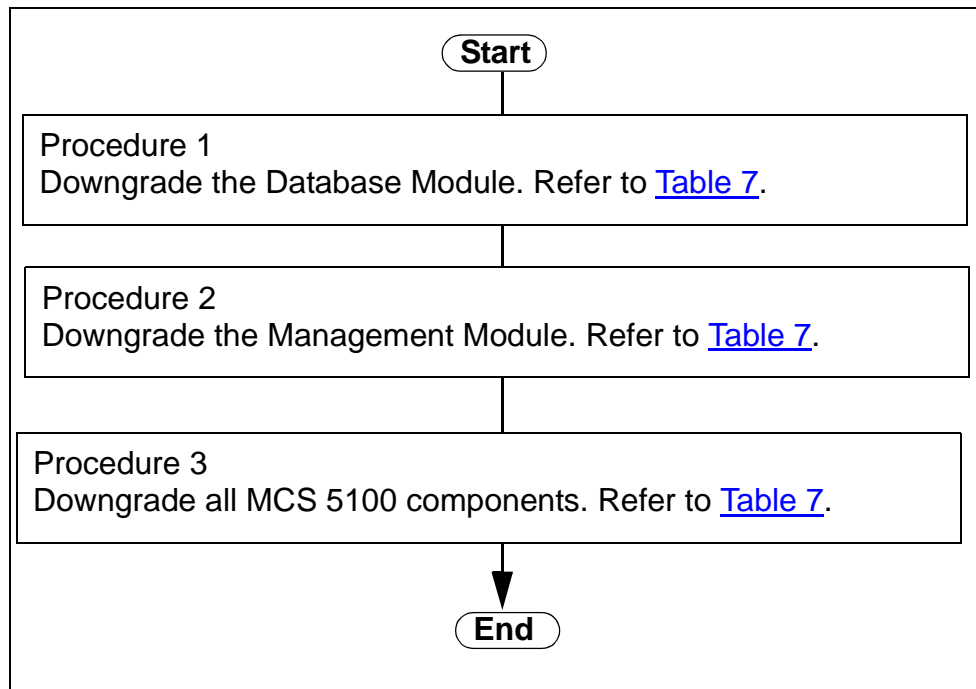
The following sections describe the sequence of tasks that must be manually performed to rollback or downgrade the system for the following procedures:

- How to downgrade a non-redundant system with a single database
- How to downgrade a redundant system

How to downgrade a non-redundant system with a single database

[Figure 1](#) shows the work flow for downgrading a non-redundant system that is configured with a single database. The table following the figure shows the tasks the user must follow for downgrading a non-redundant system with a single database.

Figure 1 Work flow for downgrading a non-redundant system with a single database



[Table 7](#) shows the task sequence that the user must follow for downgrading a non-redundant system with a single database. The table also provides references to the procedures titles from applicable component documents.

Table 7 Downgrading a non-redundant system with a single database

Procedure	Task	Procedure title	Document reference
1. Downgrade the Database Module.			
1a	Stop all components from the System Management Console.	Stopping the Management Module processes	<i>MCS 5100 Management Module Basics</i>
1b	Shut down the management module.	Stopping the Management Module processes	<i>MCS 5100 Management Module Basics</i>
1c	Downgrade the Database Module.	Updating the Database Module component	<i>MCS 5100 Database Module Basics</i>

Table 7 Downgrading a non-redundant system with a single database

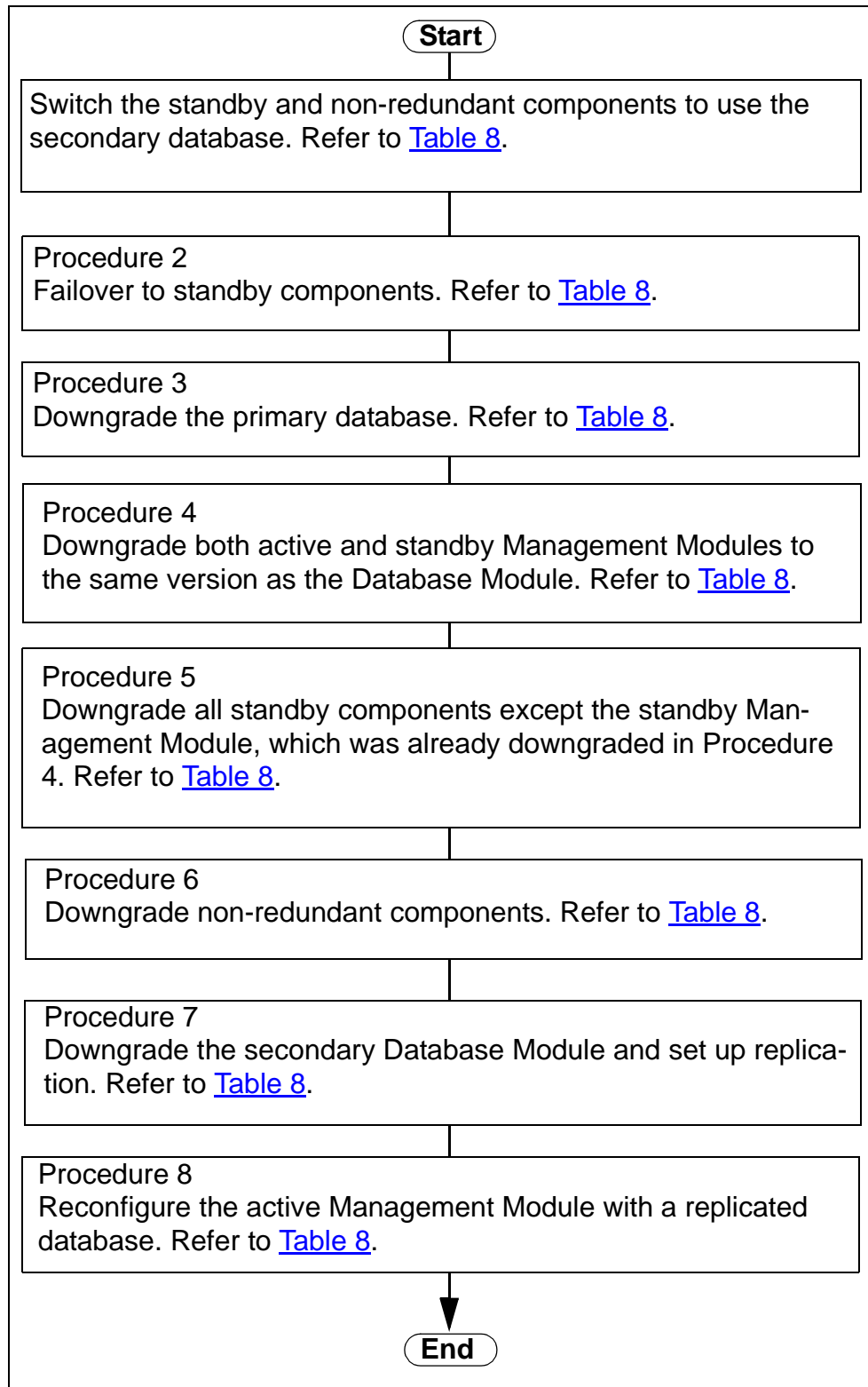
Procedure	Task	Procedure title	Document reference
2. Downgrade the Management Module.			
2a	Downgrade and start the Management load.	Updating the Management Module software	<i>MCS 5100 Management Module Basics</i>
2b	Downgrade the System Management Console, refer to procedure in the document.	Installing the System Management Console	<i>MCS 5100 System Management Console Basics</i>
3. Downgrade all MCS 5100 components.			
3a	Downgrade all MCS 5100 components.	Component software updates	<i>MCS 5100 System Management Console Basics</i>

How to downgrade a redundant system

Attention

Before starting the downgrade procedure for a redundant system, compose a list of all component names and their IP addresses (including the redundant applications). As you downgrade each component, mark them off of the list. Checking components off from the list will be especially helpful as each component is switched from preferred to standby and back again.

[Figure 2](#) shows the work flow for downgrading a redundant system. The table following the figure shows the tasks the user must follow for downgrading a redundant system.

Figure 2 Work flow for downgrading a redundant system

[Table 8](#) shows the task sequence that the user must follow for downgrading a redundant system. The table also provides references to the procedures titles from applicable component documents.

Table 8 Downgrading a redundant system

Procedure	Task	Procedure title	Document reference
1. Switch the standby and non-redundant components to use the secondary database.			
1a	Stop the Oracle Monitor.	Using the System Management Console for Operational Tasks	<i>MCS 5100 System Management Console Basics</i>
1b	Modify the properties of the Database Base for standby and redundant components.	Component Database Base Configuration <i>table</i>	<i>MCS 5100 Database Module Basics</i>
2. Failing over to standby components except the standby Management Module.			
2a	Stop all running components except the Accounting Module and Management Module from the System Management Console.	Using the System Management Console for Operational Tasks	<i>MCS 5100 System Management Console Basics</i>
2b	Failover to the cold standby Accounting Module.	Failover to the cold standby Accounting Module	<i>MCS 5100 Accounting Module Basics</i>
3. Downgrade the primary Database.			
3a	Downgrade the primary Database.	Downgrade the primary Database	<i>MCS 5100 Database Module Basics</i>
4. Downgrade both active and standby Management Modules to the same version as the Database Module.			
4a	Downgrade and restart the active Management Module.	Updating the Management Module software	<i>MCS 5100 Management Module Basics</i>

Table 8 Downgrading a redundant system

Procedure	Task	Procedure title	Document reference
4b	Downgrade the standby Management Module.	Updating the Management Module software	<i>MCS 5100 Management Module Basics</i>
4c	Install and log into the downgraded version of the System Management Console.	Installing the System Management Console	<i>MCS 5100 System Management Console Basics</i>
5. Downgrade all standby components except the standby Management Module, which was already downgraded in Procedure 4.			
5a	Downgrade all standby components including the Accounting Module from the System Management Console.	Component Software Updates	<i>MCS 5100 System Management Console Basics</i>
5b	Stop the active components so that standby components become active components from the System Management Console.	Using the System Management Console for Operational Tasks	<i>MCS 5100 System Management Console Basics</i>
5c	Failover back to the preferred Accounting Module.	Failover to the preferred Accounting Module	<i>MCS 5100 Accounting Module Basics</i>
5d	Stop all other components from the system hierarchy tree on the System Management Console.	Using the System Management Console for Operational Tasks	<i>MCS 5100 System Management Console Basics</i>
5e	Downgrade the remaining components including the Accounting Module.	Component software updates	<i>MCS 5100 System Management Console Basics</i>

Table 8 Downgrading a redundant system

Procedure	Task	Procedure title	Document reference
6. Downgrade non-redundant components.			
6a	Downgrade non-redundant components.	Component software updates	<i>MCS 5100 System Management Console Basics</i>
7. Downgrade the secondary Database Module and set up replication.			
7a	Downgrade the secondary Database Module and set up replication.	Downgrade the secondary Database Module and setting up replication	<i>MCS 5100 Database Module Basics</i>
8. Reconfigure the active Management Module with a replicated database.			
8a	Reconfigure the active Management Module with a replicated database.	Updating the Management Module software	<i>MCS 5100 Management Module Basics</i>



List of acronyms

AC	alternating current
AC	application contexts
ACD	automatic call distribution
ADSL	asynchronous digital subscriber line
ATM	asynchronous transfer mode
BBUA	back-to-back user agent
BPS 2000	Business Policy Switch 2000
BPT	bulk provisioning tool
CAM	central accounting manager
CAS	channel-associated signaling
CD	compact disc
CDP	coordinated dialing plan

CDS	converged desktop services
CGI	common gateway interface
CLI	command line interface
CODEC	coder/decoder
CoS	class of service
CPE	customer premise equipment
CPL	call processing language
CRM	customer's records management
CS 2000	Communication Server 2000
CSE 1000	Communication Server for Enterprise 1000
CSE 2000	Communication Server for Enterprise 2000
CSV	comma separated value
DC	direct current
DHCP	dynamic host configuration protocol
DIGMAN	digit manipulation
DiffServ	differentiated service

DLCMI	data link control management interface
DLL	dynamic link library
DMS-100	Digital Multiplex System-100
DNS	domain name server
DP	Developer Program
DSL	digital subscriber line
DSM	distributed software manager
DTMF	dual tone multi frequency
EBIP	enhanced breaker interface panel
EBN	Enterprise Business Networks
ERC	express routing code
ESD	electronic software delivery
FoIP	Fax over IP
FRU	field replaceable unit
FTP	file transfer protocol
GMT	Greenwich Mean Time

GUI	graphical user interface
HDLC	high-level data link control
HSC	hot swap controller
HTTP	Hyper-text Transfer Protocol
HTTPS	Hyper-text Transfer Protocol Secure
IETF	Internet Engineering Task Force
IM	instant messaging
I/O	input/output
IP	Internet Protocol
IPCM	Internet Protocol Client Manager
IPDR	Internet Protocol Data Records
IPMP	Internet Protocol Multi-pathing
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
IVR	interactive voice response
JDBC	Java database connectivity

JPEG	joint photographic experts groupPNG (portable network graphic)
KVM	keyboard/ video/ mouse
LAM	Local Accounting Manager
LAN	local area network
LCD	liquid crystal display
LI	Legal Intercept (also Lawful Intercept)
MAC	media access control
MAddr	media access control address
MAS	Media Application Server
MCP	Multimedia Communications Portfolio
ME	managed element
MGCP	Media Gateway Control Protocol
MGCP+	Media Gateway Control Protocol with Extensions
MIB	management information base
MMC	Microsoft Management Console
MO	managed object

MOH	Music on hold
MOP	methods of procedure
Meridian SL-100	Meridian SuperNode Logic-100
MS	Microsoft
MSD	most significant digit
MWI	message waiting indication
NAT	network address translator
NAPT	network address port translation
NIC	network interface controller
NMS	network management system
OAM	operations, administration, and maintenance
OCM	originating call model
OAM&P	operations, administration, maintenance, and provisioning
OCM	originating call model
OEM	Oracle Enterprise Manager
OM	operational measurement

ONMS	Optivity Network Management System
OPI	open provisioning interface
OSN	on-site Notification
OSS	operations support system
OUFCAPS	Overview, Upgrades, Fault, Configuration, Accounting, Performance, and Security and Administration
PA	Personal Agent
PBX	private branch exchange
PC	personal computer
PCMA	Pulse Code Modulated (aLaw encoding)
PCMU	Pulse Code Modulated (μLaw encoding)
PDIL	partial dial
PM	performance measurement
PNG	portable network graphic
Pos	provisionable objects
PRACK	persistent acknowledge messages

PRI	primary rate interface
PSAP	Public Safety Answering Point
PSEIZ	permanent seizure
PSTN	public switched telephone network
QFE	quad fast ethernet
QoS	quality of service
RFC	Request for Comment
RMAN	Recovery Manager
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
RU	recording units
SA	system administrator
SAM16	Service Application Module-16
SC	service consumer
SCTP	Signaling transport control point
SDP	Session Description Protocol

SE	service element
SIP	Session Initiation Protocol
SimRing	Simultaneous Ring
SLEE	service level execution environment
SMDI	simple message desk interface
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SQL	structured query language
SS	service session
SS7	Signaling System 7
SSL	Secure Socket Layer
STD format	standard format
TCM	terminating call model
TDM	Time Division Multiplexer
TCP	Transmission Control Protocol
ToS	Type of service

TSAC	terminal services advanced client
UAS	Universal Audio Server
UDP	Universal Datagram Protocol
UE	usage entry
UFTP	UNISlim File Transfer Protocol
UM	unified messaging
UNISlim	Unified Network Internet Protocol Stimulus Protocol
URI	universal resource indicator
URL	uniform resource locator
USB	universal serial bus
VMS	voice mail server
VPN	virtual private network
VoIP	Voice over Internet Protocol
WAN	wide area network
WCSCP	Web Client Session Control Protocol
WSDL	web service definition language

XML

EXtensible Markup Language

Multimedia Communication Portfolio

Multimedia Communication Server 5100

FCAPS Summary

Copyright © 2004 Nortel Networks,

All Rights Reserved

NORTEL NETWORKS CONFIDENTIAL: The information contained in this document is the property of Nortel Networks. Except as specifically authorized in writing by Nortel Networks, the holder of this document shall keep the information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to third parties and use same for evaluation, operation, and maintenance purposes only. Changes or modifications to the MCS 5100/5200 network elements and software without the express consent of Nortel Networks may void its warranty and void the user's authority to operate the equipment.

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

*Nortel Networks, the Nortel Networks logo, the Globemark, and Nortel are trademarks of Nortel Networks.

*Sun Fire is a trademark of Sun Microsystems, Inc.

*Oracle is a trademark of Oracle Corporation.

Publication number: NN10422-109

Product release: MCS 5100 3.0

Document version: Standard 03.02

Date: July 2004

