Nortel Multimedia Communication Server 5100

System Manager Fundamentals

ATTENTION

Clicking on a PDF hyperlink takes you to the appropriate page. If necessary, scroll up or down the page to see the beginning of the referenced section.

NN42020-109

Document status: Standard
Document version: 01.01
Document date: 29 January 2007

Sourced in Canada

Revision history

January 2007
Standard 01.01. This document is issued to support Multimedia Communication Server 5100 Release 4.0. This document contains information previously contained in the following legacy document, now retired: *Management Module Basics* (NN10268-111).

November 2005
Standard 3.0. This document is up-issued for MCS 5100 Release 3.5.

November 2005
Standard 2.0. This document is up-issued for MCS 5100 Release 3.5.

October 2005
Standard 1.0. This document is up-issued for MCS 5100 Release 3.5.

Contents

New in this release

The following sections describe what is new in this document for Multimedia Communications Server (MCS) 5100 Release 4.0.

Features

The following new features affect this document:

The following sections describe how the features affect this release.

Base OAMP supportability

The Base Operations, Administration, Maintenance, and Provisioning (OAMP) supportability feature enhances the support and hardware configuration of the Multimedia Communications Server (MCS) 5100 product. The feature includes the following benefits:

- shared network data
- consolidated configuration data
- consolidated software to reduce memory requirements
- ability to configure additional Accounting Managers (AM), and Fault and Performance Managers (FPM)

Consequently, the System Management Console GUI layout is different. The application area replaces the general information area (GIA). The system tree pane is replaced by the navigation view pane.

OAM framework enhancements

The Operations, Accounting and Maintenance (OAM) framework enhancements feature is closely related to the Base OAMP supportability feature. This feature introduces multiple Fault Performance Managers (FPM) and Accounting Managers (AM) for improved scalability. This feature also reorganizes the operational measurements groups.

Complete re-IP support

With the Complete re-IP support feature, you do not need to reinstall the server software after you change various server identification parameters, such as country, time zone, and IP address. For more information, see *Routine Maintenance* (NN42020-502).

IBM core hardware introduction

This feature introduces the IBM eSeries x306m hardware for all the core MCS servers. The Sun Fire V100, V210, and Netra 240 servers are not supported in Release 4.0.

Linux support

With the Linux support feature, the MCS 5100 software can operate in the Linux Operating System. The core MCS system, including the Wireless Client Manager (WiCM), operates in Linux.

WARNING

Do ***not*** contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

Other changes

The following technical changes have been made to the document:

- The H.323 Gatekeeper is not supported in Release 4.0; references to it have been removed.
- Note added that an alarm is raised when the System Manager service address is changed.
- The Re-IP procedures appendix is moved to *Routine Maintenance* (NN42020-502).
- Unnecessary graphics are removed from this document.
- This document is renamed and renumbered from *Management Module Basics* (NN10268-111) to *System Manager Fundamentals* (NN42020-109).

How to get help

This chapter explains how to get help for Nortel products and services.

Finding the latest updates on the Nortel web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation for Multimedia Communication Server (MCS) 5100, go to www.nortel.com and navigate to the Technical Documentation page for MCS 5100.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support web site and the Nortel Knowledge Base for answers to technical issues
- arrange for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the telephone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Regulatory and license information

This chapter contains regulatory and license information.

WARNING
Do ***not*** contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

Red Hat Software

Passthrough End User License Agreement

This section governs the use of the Red Hat Software and any updates to the Red Hat Software, regardless of the delivery mechanism and is governed by the laws of the state of New York in the U.S.A. The Red Hat Software is a collective work under U.S. Copyright Law. Subject to the following terms, Red Hat, Inc. ("Red Hat") grants to the user ("Customer") a license to this collective work pursuant to the GNU General Public License. Red Hat Enterprise Linux (the "Red Hat Software") is a modular operating system consisting of hundreds of software components. The end user license agreement for each component is located in the component's source code. With the exception of certain image files identified below, the license terms for the components permit Customer to copy, modify, and redistribute the component, in both source code and binary code forms. This agreement does not limit Customer's rights under, or grant Customer rights that supersede, the license terms of any particular component. The Red Hat Software and each of its components, including the source code, documentation, appearance, structure and organization are owned by Red Hat and others and are protected under copyright and other laws. Title to the Red Hat Software and any component, or to any copy, modification, or merged portion shall remain with the aforementioned, subject to the applicable license. The "Red Hat" trademark and the "Shadowman" logo are registered trademarks of Red Hat in the U.S. and other countries. This agreement does not permit Customer to distribute the Red Hat Software using Red Hat's trademarks. If Customer makes a commercial redistribution of the Red Hat Software, unless a separate agreement with Red Hat is

executed or other permission granted, then Customer must modify any files identified as "REDHAT-LOGOS" and "anaconda-images" to remove all images containing the "Red Hat" trademark or the "Shadowman" logo. As required by U.S. law, Customer represents and warrants that it: (a) understands that the Software is subject to export controls under the U.S. Commerce Department's Export Administration Regulations ("EAR"); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria); (c) will not export, re-export, or transfer the Software to any prohibited destination, entity, or individual without the necessary export license(s) or authorizations(s) from the U.S. Government; (d) will not use or transfer the Red Hat Software for use in any sensitive nuclear, chemical or biological weapons, or missile technology end-uses unless authorized by the U.S. Government by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Software to eligible end users, it will, as required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department's Bureau of Industry & Security (BIS), which include the name and address (including country) of each transferee; and (f) understands that countries other than the United States may restrict the import, use, or export of encryption products and that it shall be solely responsible for compliance with any such import, use, or export restrictions. Red Hat may distribute third party software programs with the Red Hat Software that are not part of the Red Hat Software. These third party programs are subject to their own license terms. The license terms either accompany the programs or can be viewed at www.redhat.com/licenses/. If Customer does not agree to abide by the applicable license terms for such programs, then Customer may not install them. If Customer wishes to install the programs on more than one system or transfer the programs to another party, then Customer must contact the licensor of the programs. If any provision of this agreement is held to be unenforceable, that shall not affect the enforceability of the remaining provisions.

"Red Hat" and the Red Hat "Shadowman" logo are registered trademarks of Red Hat, Inc.
"Linux" is a registered trademark of Linus Torvalds.
All other trademarks are the property of their respective owners.

Safety information

This section contains important safety information.

⚠ Warning

Please be careful of the following while installing the equipment:

- Please only use the Connecting cables, power cord, AC adaptors shipped with the equipment or specified by Nortel to be used with the equipment. If you use any other equipment, it may cause “failures, malfunctioning or fire”.
- Power cords shipped with this equipment must not be used with any other equipment. In case the above guidelines are not followed, it may lead to death or severe injury

⚠ 警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

- 接続ケーブル、電源コード、ACアダプタなどの部品は、必ず製品に同梱されております添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となることがあります。
- 同梱されております付属の電源コードを他の機器には使用しないでください。

上記注意事項を守らないと、死亡や大怪我など人身事故の原因となることがあります。

Introduction

WARNING
Do ***not*** contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

The System Manager is a core component of the Multimedia Communication Server (MCS) 5100 infrastructure. It supports the services used to communicate with and manage the network elements and servers.

The topics in this chapter include:

How this guide is organized

This guide is organized as follows:

This chapter describes the performance management strategy of the System Manager software and hosting servers.

- "Security and administration" (page 49)

  This chapter describes the security issues and administrative tasks related to the operations of System Manager services.

- Re-IP procedures

  This appendix includes re-IP procedures for servers and components.

System Manager functions and services

The System Manager network element provides the services that support communication amongst the Multimedia Communication Server network elements and management requests issued from the System Management Console. In conjunction with the System Management Console, the System Manager supports the following functionality:

- system operations administration
- system software management
  - — software inventory, a list of available software loads
  - — software updates
  - — deployment, start, and monitoring
- system configuration
  - — add, modify, delete
- system maintenance
  - — start, stop, kill, and restart network element services
  - — IPCM device diagnostics and firmware upgrades
- fault monitoring
  - — logs
  - — alarms
  - — archival of logs (which includes fault events)
- system performance monitoring
  - — operational measurements
  - — configurable collection period and archival of operational measurements
- network management interfaces

— SOAP (Simple Object Access Protocol) over HTTPS

— System Management Console

System Manager interfaces

In the MCS system communications scheme, the System Manager sits between the MCS network elements and the System Management Console.

The following are the interfaces of the System Manager:

- Transmission Control Protocol/Internet Protocol (TCP/IP) interface
- Structured query language (SQL) interface
- Simple Object Access Protocol (SOAP) interface
- Simple network management protocol version 2 (SNMPv2) interface
- Secure File Transfer Protocol (SFTP) interface

Transmission Control Protocol/Internet Protocol (TCP/IP)

The System Manager uses TCP/IP to communicate management and configuration data to each of the managed network elements. The managed network elements use TCP/IP to communicate performance data, logs, and alarms upwards to the System Manager or Fault Performance Manager

Structured query language (SQL)

The system uses SQL over a Java Database Connection (JDBC) to store and retrieve system configuration data between the System Manager and the Database Manager.

Simple Object Access Protocol (SOAP)

SOAP is an XML-based lightweight protocol for the exchange of information in a decentralized, distributed environment. SOAP is used to communicate requests to the System Manager.

Simple Network Management Protocol version 2c (SNMPv2c)

The system uses SNMPv2c to poll the System Manager for alarm events. The system can also use SNMPv2c polling to report MCS alarms to an existing network management system.

Secure File Transfer Protocol (SFTP)

The system uses SFTP to transfer data from the System Manager to a northbound management system for logs and operational measurements (OMs).

Server hardware

The System Manager runs on an IBM eSeries x306m server. The number of servers and the network elements sharing a server depend on the specific deployment scenario. For more information, see *MCS 5100 Overview* (NN42020-143).

Fault tolerance

In redundant network architectures, the System Manager resides on two servers. One server hosts the active System Manager and the standby Accounting Manager. A second server hosts the active Accounting Manager and the cold standby System Manager. This arrangement ensures the availability of these two fundamental network elements. If the active System Manager or its hosting server fails, an administrator can perform the failover procedure to transfer the System Manager operations to the cold standby server. Likewise, if the active Accounting Manager or its hosting server fails, an administrator can transfer the Accounting Manager operations to the cold standby server. For additional information, see "Fault management" (page 23).

Upgrades

Maintenance Releases (MR) for major components of the MCS system are available on CDs or by electronic distribution. Documentation that outlines steps required for the upgrade is included with the distribution.

As a prerequisite to upgrades, the MCS system must be properly configured and functioning. Before upgrading the system, the technician must transfer MR upgrade files from the CD to the appropriate servers. Additionally, the technician must extract files from any compressed archives included with the MR release.

For more information, see the MR release notes that are included in the MR distribution and *MCS Upgrades - Maintenance Releases* (NN42020-303).

Fault management

The topics in this chapter include:

Overview

The System Manager software includes all the functionality of a Fault Performance Manager (FPM). Two additional FPMs can be deployed in the MCS network to collect alarm, log, and operational measurement information from network elements.

Alarms and logs are the primary fault management information. The System Manager services collect and archive the alarms and logs generated by subsystems on the System Manager and any network elements that use the System Manager for fault and performance management. Administrators can view collected fault information by using the System Management Console on the management PC.

Use the following System Management Console tools to view and work with alarms and logs that are collected by the System Manager:

- alarm summary

  The alarm summary area of the System Management Console provides the total number of alarms, the number of critical, major, minor, or warning alarms, and the number of acknowledged alarms for each severity. The entire alarm summary area is color coded so that it is the

color of the most severe alarm. For information about specific alarms and how to clear them, see *Alarm and Log Reference*, (NN42020-703).

- Logical View and Physical View windows

  You can open these windows from the System Management Console toolbar to obtain immediate visual identification of alarmed network elements. After selecting an alarmed network element, you can open the alarm browser.

- alarm browser

  Administrators use the alarm browser to view active alarms. View alarms for the System Manager (SM) by selecting the SM network element from the navigation pane and clicking the alarm browser icon, or by selecting SM_0 or SM_1 from the Logical View window and clicking on the alarm browser icon.

- log browser

  Administrators use the System Management Console log browser to view operational event information related to the services of the System Manager software and the status of the System Manager hardware. The System Management Console log browser provides 50 log reports in a circular buffer, and therefore does not review or display old log reports. To view historical log reports, configure an FTP transfer of the log reports to another host and use an Operation Support System (OSS) tool to view them.

For information about using the System Management Console tools, see *System Management Console User Guide* (NN42020-110).

For alarm descriptions and log information, see *Alarm and Log Reference* (NN42020-703).

If a fault causes a failure on the active System Manager or its hosting server and the System Manager uses a redundant architecture, administrators can perform the manual failover procedure to activate the standby System Manager.

SNMP information

The following information about how the System Manager uses Simple Network Management Protocol (SNMP) is useful for integrating the MCS with an OSS system such as the Nortel Integrated Element Management System (IEMS).

To forward traps northbound perform the procedure Configuring an SNMP Manager with the OSS host as the destination host and associate that SNMP Manager profile with the SM and the FPMs in the MCS network.

Ensure that the SNMP agent on the destination host has SNMPv2c available for communication. To perform this procedure, you require the SNMP port and community string for the SNMP daemon on the destination host.

For networks that prefer to poll the System Manager and FPMs for data, the System Manager and each FPM offer an SNMP port. Determine the open port number by adding 17 to the base port of the network element. For the System Manager, the base port is 12100, so the open port is 12117. For FPMs, select Network Elements > Fault Performance Managers and view the base port for the configured FPMs. When you configure SNMP parameters for the host that collects the data, the community string the client uses is the same as the community string for a configured SNMP Manager.

Local storage

Log, alarm, and operational measurement (OM) data is recorded to disk on the System Manager or FPM that a network element is configured to use. Those records are stored as follows:

- System Manager

  /var/mcp/oss/om/MCP_9.0/SM_0/

- Fault Performance Manager

  /var/mcp/oss/om/MCP_9.0/<fpm_name>_0/

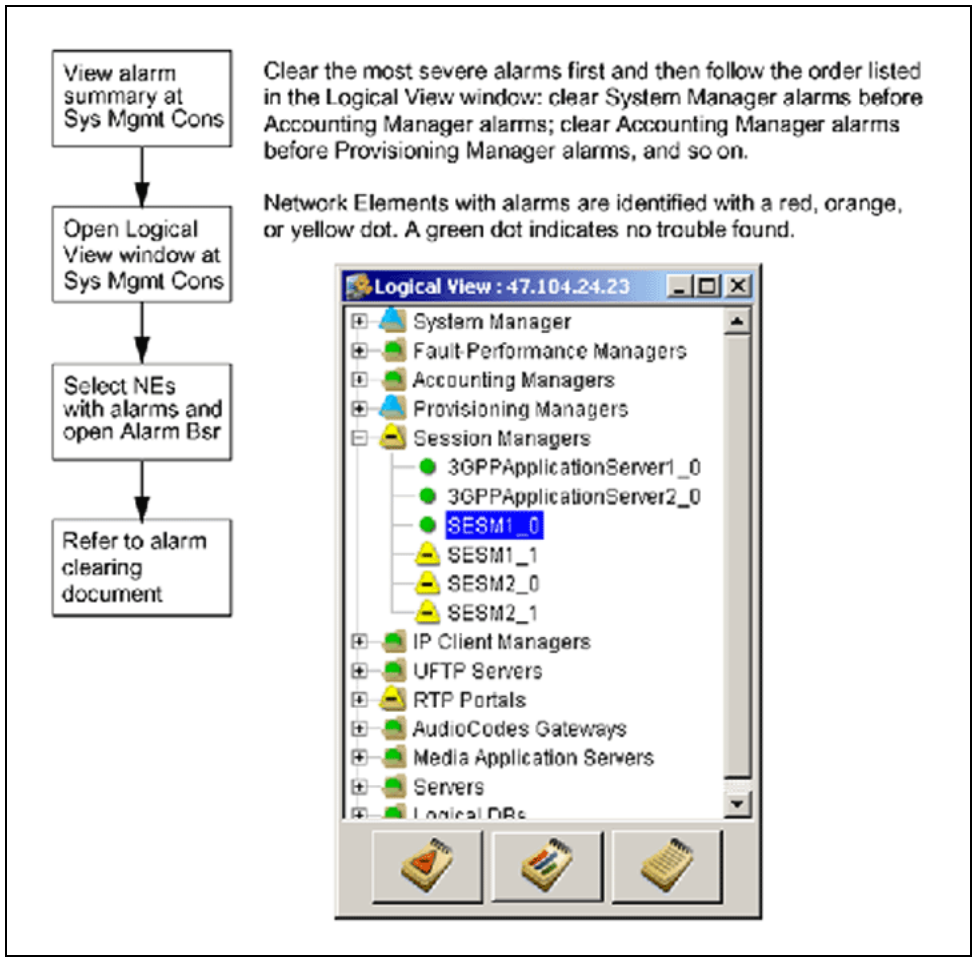
  The name of the Fault Performance Manager is typically a value like FPM1, which becomes FPM1_0 in the file system.

Below these directories, a directory is created for each network element instance that reports data to the System Manager or FPM.

Fault management taskflow

Use the following flowchart to assist with clearing trouble conditions.

Figure 1
Fault management taskflow



Hosting server backup and restore

You can back up and recover MCS server software. With backups, you can recover the software and server configuration after minor server failures, or after catastrophic server failures.

Nortel recommends that you back up the System Manager so that you can restore the software and the server configuration after a catastrophic failure.

ATTENTION

Back up servers according to a schedule. However, Nortel recommends that you manually back up an MCS server

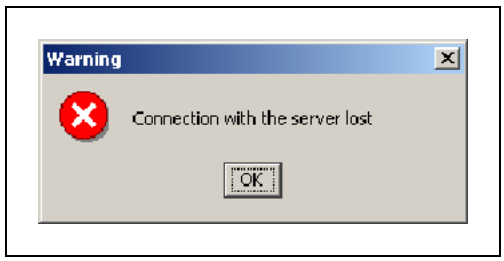
- after you update the operating system
- after you deploy an MCS software maintenance release for the System Manager

For details regarding backup procedures, see *Routine Maintenance*, (NN42020-502).

Lost System Management Console connection

When the connection between the System Manager and System Management Console is lost, the following dialog box appears on the administrator's workstation screen followed by a log on prompt.

Figure 2
Warning dialog box

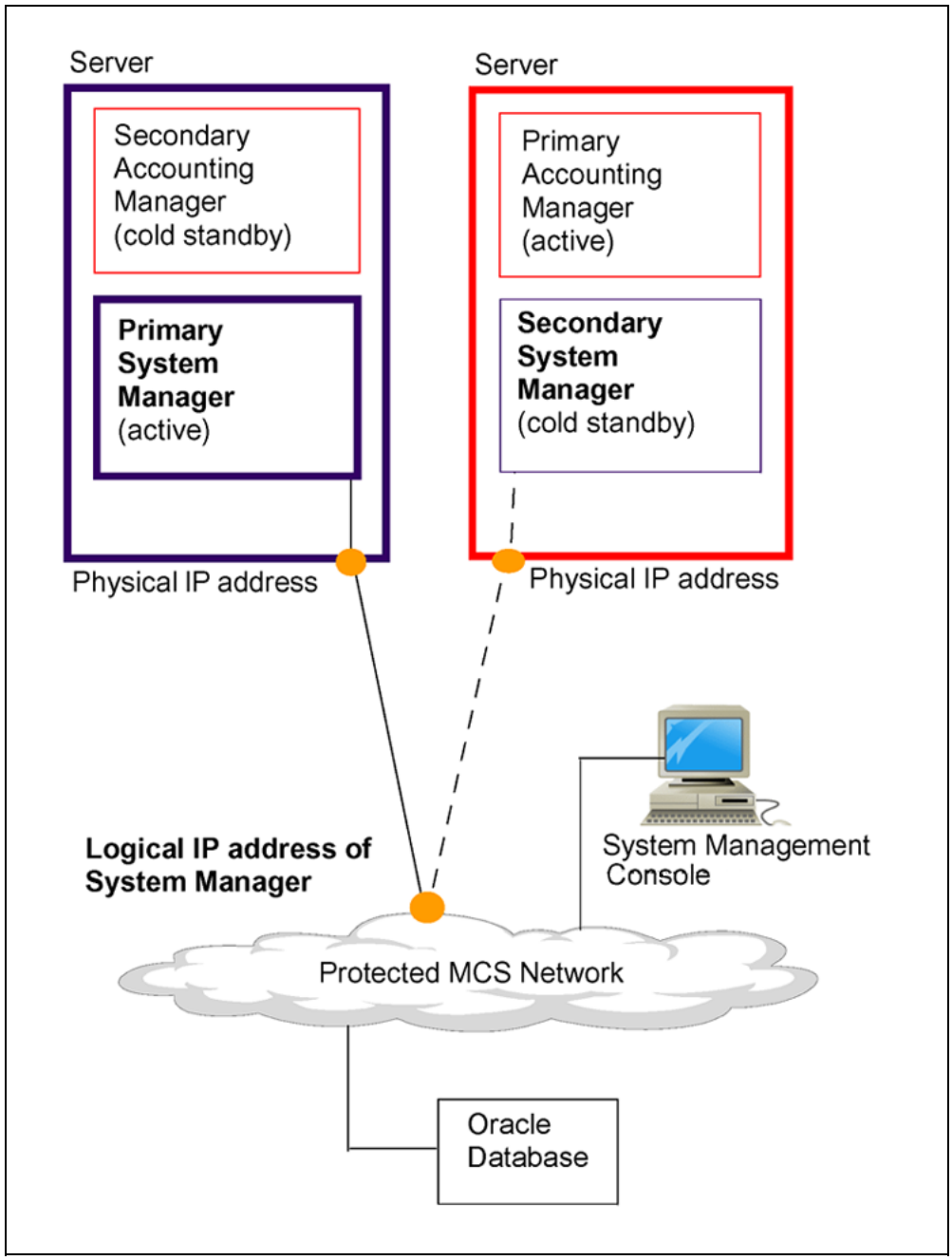


The lost connection can be an indication that the System Manager application on the System Manager or its hosting server has failed. If an attempt to log on after a lost connection fails, administrators must perform basic connectivity troubleshooting to ensure the fault is not a network or other problem.

Manual failover in a redundant configuration

In a redundant architecture, two servers host the System Manager software. One server hosts the active System Manager and another hosts the cold standby System Manager. If the active System Manager or hosting server fails, a manual failover allows the transfer of the management operations to the cold standby System Manager. The active System Manager component owns the logical IP address used to connect with the System Management Console. In addition, all the network elements use the logical IP address to send logs, alarms, and OMs to the System Manager. The following figure shows a logical view of this configuration.

Figure 3
Redundancy of System Manager - logical view



When the active System Manager fails, the System Management Console loses its connection. In addition, logs and alarms from the managed network elements that use the System Manager for fault and performance management are spooled on each network element instance and are not reported until the active System Manager is recovered or until an administrator performs a failover to the cold standby System Manager.

The manual failover process involves stopping the System Manager processes, releasing the service IP address from the System Manager server, and starting the processes on the server hosting the secondary System Manager. All actions require the use of a UNIX log on account.

The Oracle database stores the system application and configuration data. The secondary System Manager retrieves the latest configuration data from the database when it becomes active. However, information stored on the management server's local disk is not transferred during a manual failover. This information includes archived logs and holding OMs.

To facilitate this procedure, Nortel recommends that you have a log book with the information (physical and service IP addresses, log on information) required to perform the failover.

Physical IP addresses of the System Manager servers

To perform an manual failover, you must know the physical IP addresses of the servers hosting the primary and secondary System Manager network elements. Use the following procedure to view the physical IP addresses of the active and cold standby System Manager.

Procedure 1

Viewing the physical IP addresses of the System Manager servers

Step	Action
1	In the System Management Console, from the configuration view pane, select **Network Data and Mtc > Addresses**. The Addresses window appears in the work area.
2	If the office is configured according to the Nortel-recommended naming convention, the two System Manager server interfaces are deployed with logical names of **EMServer1Addr** and **EMServer2Addr**. In this event, scroll to the two entries and record the IP addresses for these two servers.
3	If the office is not configured according to the Nortel recommended naming convention, select **Network Elements > System Manager > System Manager > Instance**. The System Manager Instance window appears in the work area.
4	Determine the name of the servers on which the System Managers are deployed.
5	After recording the server names, close the System Manager Instance window.

6 From the configuration view pane, select the **Servers**.

The Servers window appears in the work area.

7 Determine the logical name of the address provisioned as Interface 1 for each server.

8 After recording the logical name of the addresses, close the Servers window.

9 From the configuration view pane, in the **Network Data and Mtc** section, select **Addresses** .

The Addresses window appears in the work area.

10 Determine the IP address provisioned for each logical name.

—End—

Manual failover in a redundant configuration

When the System Manager application or active System Manager server fails, its associated processes and ownership of the logical IP address must be stopped. Because the connection to the System Management Console is lost, administrators must log on remotely to the standby System Manager server with a secure shell connection.

To log on to the servers, the you must use the limited access account created for this procedure. Use the following procedure to perform a manual failover in a redundant configuration.

Procedure 2
Performing a manual failover in a redundant configuration

Step	Action
1	At the management PC, using the UNIX account, log on to the server that hosts the primary System Manager.
2	Run the smStop.pl script.
3	At the management PC, using the UNIX account, log on to the server that hosts the secondary System Manager.
4	Run the smStart.pl script.

—End—

For more information, see the following topics:

- "System Manager processes" (page 31)
- "Cold standby System Manager" (page 31)
- "After you restore the primary System Manager" (page 32)
- "Failover impacts and recovery" (page 33)

System Manager processes

Stop the primary System Manager if possible. If the hosting server is down, or in an isolated state, you cannot stop the primary System Manager. See Procedure 4 "Starting the cold standby System Manager" (page 32).

Use the following procedure to stop the primary System Manager.

Procedure 3

Stopping the primary System Manager

Step	Action
1	At the management PC, use secure shell to log on to the server running the active System Manager instance as **nortel**. `ssh nortel@<phys_ip_address>` **<physical address of server>** is the physical IP address of the server.
2	If this is the first secure connection to the server from this computer and you receive a prompt to exchange keys, respond with **yes**.
3	To stop System Manager processes and release the logical IP address, run the smStop.pl script by typing **/var/mcp/<site>/smStop.pl**. When the shutdown is complete, the name and path of the log file associated with this event appear on screen.

—End—

Cold standby System Manager

When you start the cold standby System Manager instance, the System Manager logical IP address becomes associated with the newly active System Manager. Once the logical IP address is associate, you can reestablish the System Management Console connection.

Use the following procedure to start the cold standby System Manager.

Procedure 4
Starting the cold standby System Manager

Step	Action
1	At the management PC, use secure shell to log on to the server running the active System Manager instance as **nortel**. `ssh nortel@<phys_ip_address>` **<physical address of server>** is the physical IP address of the server.
2	If this is the first secure connection to the server from this computer and you receive a prompt to exchange keys, respond with **yes**.
3	Run the smStart.pl script to start the System Manager processes and take ownership of the logical IP address: `/var/mcp/<site>/smStart.pl` When the startup is complete, the name and path of the log file associated with this event appear on screen.

—End—

After you restore the primary System Manager

The procedure to revert to the primary System Manager is the reverse of the failover to the secondary System Manager. Use the following procedure to revert to the primary System Manager.

Procedure 5
Reverting to the primary System Manager

Step	Action
1	At the management PC, close the System Management Console.
2	Use secure shell to log on to the server hosting the active secondary System Manager instance.
3	Execute the smStop.pl script to stop System Manager processes and release the logical IP address: `/var/mcp/<site>/smStop.pl`
4	Use secure shell to log on to the server hosting the preferred System Manager instance.
5	Execute the smStart.pl script to start System Manager processes and take ownership of the logical IP address:

```
/var/mcp/<site>/smStart.pl
```

6 Reestablish the System Management Console connection.

—End—

Failover impacts and recovery

Administrators must be aware of the following system impacts of a System Manager failure and recovery:

- You may be unable to stop the primary System Manager, due to network isolation of the System Manager server.

  Impact:
  A remote logon session may not be possible if the server is in a network isolated state. You can start the secondary System Manager and take ownership of logical IP address. However, if the primary System Manager comes back online while the secondary System Manager is running, conflicts occur between the two active components.
  Recovery:
  You must promptly shut down one of the two active components. If possible, try to connect to the management server through the terminal server and execute the smStop.pl script. In the event that the two instances compete for the active role, log into the secondary server and execute the smStop.pl script as soon as possible. As a last resort, physically cycle down the power on the server until the backup System Manager stops.

- Running the secondary System Manager uses the resources of its hosting server.

  Impact:
  The secondary System Manager is hosted on the accounting server. When the secondary System Manager is active, it shares the server resources with the active Accounting Manager. This can result in degraded capacity of both the management and accounting processes.
  Recovery:
  You must switch the management processes back to the primary System Manager server as soon as it becomes available.

Nonredundant System Manager

In a nonredundant configuration, the single server of the System Manager hosts one or more active MCS network elements.

If software on the System Manager fails, watchdog processes attempt to restart the software application 3 times. If this does not work, software on the server waits 5 minutes and then tries to restart the software application an additional 3 times. If the software application still does not run, manual action is necessary.

The preferred method of restarting the System Manager is to log on to the server and start the System Manager instance. This method does not affect the other applications also running on the server. Use the following procedure to restart a nonredundant System Manager.

Procedure 6
Restarting a System Manager in a nonredundant configuration

Step	Action
1	At the management PC, log on to the server hosting the System Manager application: `ssh nortel@<sys_man_phys_ip_address>`
2	If this is the first secure connection to the server from this computer, you receive a prompt to exchange keys. Respond with Yes.
3	If the network interface to the server is unavailable, you must log on through a terminal server.
4	Run the smStop.pl script: `/var/mcp/<site>/smStop.pl` If an error occurs while stopping the processes, the script output states "Error occurred stopping System Manager" and includes the command that failed. Contact your next level of support.
5	Run the smStart.pl script: `./smStart.pl` If an error occurs while stopping the processes, the script output states "Error occurred stopping System Manager" and includes the command that failed. Contact your next level of support.

—End—

Configuration management

The topics in this chapter include:

Overview

Deployment personnel perform the physical installation and initial configuration of the System Manager. Only after the System Manager is installed and operational can administrators interact with the network elements using the System Management Console.

All the service properties of the System Manager are preconfigured with default values. The operational parameters for the System Manager are separated into two groups: Configuration parameters and Engineering parameters. Configuration parameters typically depend on network element type and traffic expectations for the network element. Administrators can change these parameters as the network evolves. Engineering parameters are associated for a particular network element instance and are related to network element type and server configuration. Modify engineering parameters only in an emergency. Modifications are lost after an upgrade.

Optional configuration tasks

Log and operational measurement (OM) file rotation parameters are typically configured at the system level. However, administrators can configure file rotation parameters with values for either a specific server or network element. For information about configuring the rotation parameters, see *System Management Console User Guide* (NN42020-110).

The SNMP community string value for a server can be changed from the default value of public to some other value, for network security reasons. After you configure the SNMP community string value for a server, it

applies this value to SNMP message traffic of the hosted components. For information about configuring the community string, see *System Management Console User Guide* (NN42020-110).

System Manager Configuration parameters

Use this procedure to alter configuration parameters for the System Manager. Changing these values does not require a restart. If the System Manager is in a redundant configuration, the change is made immediately on both network element instances.

Use the following procedure to configure the configuration parameters. To perform this procedure, you must have WRITE permission for the ConfigParmService.

Procedure 7

Configuring System Manager configuration parameters

Step	Action
1	In the System Management Console, from the configuration view pane, select **Network Elements > System Manager > System Manager > Configuration Parameters**.
2	From the System Manager **Config Parms** window, select a Parm Group.
3	Click **Edit**.
4	In the Edit System Manager **Config Parms** window, enter a new value.
5	Click **Apply**.

—End—

Additional information

The following configuration parameters are available on the System Manager.

Table 1
Configuration parameters

Parm Group	Parameter	Description
OM	OfficeTransferPeriod	This parameter controls the Fault Performance Manager polling period in minutes. Valid values are 5, 15, 30, and 60. The default value is 15.
Security	DisableMtcLogs	If set to true, SEC801 log reports are not generated for successful maintenance requests such as opening the log browser. The default is false.
	DisableReadLogs	If set to true, SEC801 log reports are not generated for successful read requests such as viewing values in the Network Data section of the System Management Console. The default is true.
	DisableWriteLogs	If set to true, SEC801 log reports are not generated for successful data change requests such as changing Configuration Parameters. The default is false.

FTP Push stream configuration

Administrators can configure the System Manager and any Fault Performance Managers to send log and operational measurement data northbound to an OSS server.

If the server hosting the System Manager or Fault Performance Manager is configured with a management interface at the System Management Console, the system transfer data that interface. If a second interface is not provisioned, the system transfer data over the first interface. This data transfer can compete with call processing traffic.

Use the following procedure to configure an FTP Push stream. Before performing this procedure, ensure that the destination host is online and that connectivity is established between the System Manager and the destination host.

Procedure 8
Configuring an FTP Push stream

Step	Action
1	In the System Management Console, from the configuration view pane, select **Network Data > Addresses** to add the IP address of the destination host.
2	In the Addresses window, click **Add**.
3	In the Add Addresses dialog box, enter a logical name for the destination host and the IP address of the destination host.
4	Click **Apply**.
5	From the configuration view pane, select **Network Data > OAM Profiles > OSS Server** to associate the logical name with an OSS server entry.
6	In the OSS Server window, click **Add**.
7	In the Add OSS Server dialog box, enter a name for the destination host and use the drop-down list to locate the IP address logical name.
8	Click **Apply**.
9	Optionally, configure a format path for the information. Use the Record Format, File Type, and Format Path areas at the System Management Console. For more information, see *System Management Console User Guide* (NN42020-110).
10	From the configuration view pane, select **Network Data > OAM Profiles > FTP Push** to add an FTP Push profile.
11	In the FTP Push window, click **Add**.
12	In the Add FTP Push Profile dialog box, enter the configuration data.

For more information, see Table 2 "Configuration data" (page 39).

Table 2
Configuration data

Field	Value	Description
Name	string	This value identifies the FTP Push profile and is used when associating the FTP Push stream at the System Manager or Fault Performance Manager.
Server	drop-down list	Use the drop-down list to select the name associated with the OSS server.
Root Directory	string	Enter the fully qualified directory path on the OSS server, in which to place the files. The directory path must exist before activating the FTP Push.
User ID	string	Enter a user account that is active on the destination host.
Password	string	Enter the password for the user ID.
Confirm Password	string	Enter the password for the user ID again.

13 Click **Apply**.

14 From the configuration view pane, expand **Network Elements > System Manager > <any supported Network Element >** (for example, System Manager, FPM, or AM).

15 Click **FTP Push Log Stream** or **FTP Push OM Stream**.

16 In the window that appears in the work area, click **Add**.

17 In the dialog box, use the drop-down lists to select the Format Path and FTP Push Profile.

18 Click **Apply**.

—End—

SNMP Manager configuration

Use this procedure to configure a destination host to which the System Manager and Fault Performance Manager forward alarm traps.

If the destination host is already configured with an SNMP port and community string, you require this information to perform this procedure. If the destination host is not already configured, you must use the values for the SNMP port and community string that you enter during this procedure to configure the SNMP agent on the destination host.

Procedure 9

Configuring an SNMP Manager

Step	Action
1	From the navigation pane, select **Network Data > Addresses**.
2	In the Addresses window, click **Add** to create an address for the destination host.
3	In the Add Addresses dialog box, enter a logical name such as OSSSrvr1Addr, and the IP address of the destination host.
4	Click **Apply**.
5	From the navigation pane, select **Network Data > OAM Profiles > OSS Server**.
6	In the OSS Server window, click **Add** .
7	In the Add OSS Server dialog box, enter a name for the OSS Server, such as OSSSrvr1.
8	From the drop-down list, select the address of the destination host.
9	Click **Apply**.
10	From the navigation pane, select **Network Data > OAM Profiles > SNMP Manager**.
11	In the SNMP Manager window, click **Add**. The Add SNMP Manager dialog box appears.
12	In the Add SNMP Manager dialog box, enter the configuration data.

For more information, see Table 3 "Configuration data" (page 41).

Table 3
Configuration data

Field	Value	Description
Name	string	This value identifies the SNMP Manager. It is used later in this procedure to associate this SNMP Manager with the System Manager or a Fault Performance Manager.
Community	string	Enter the SNMP community string that the SNMP agent on the OSS server is configured to accept.
Server	drop-down list	Use the drop-down list to select the OSS server.
Trap Port	integer	Enter the port number that the SNMP agent on the OSS server is configured to listen on. A typical value is 162.

13 Click **Apply**.

14 From the navigation pane, select **Network Elements > System Manager > System Manager > SNMP Manager**.

The SM SNMP Manager window appears in the work area.

15 In the SM SNMP Manager window, from the drop-down list, select the destination host.

16 Click **Apply**.

17 If the network includes Fault Performance Managers, select **Network Elements > Fault Performance Managers > FPM > SNMP Managers** and assign the SNMP Manager.

—End—

Accounting management

System Manager configuration and operations have no impact or involvement in accounting functions.

For information about accounting management, including configuration and operations, see *Accounting Manager Fundamentals* (NN42020-144).

Performance management

The topics in this chapter include:

Overview

Administrators use the System Management Console to monitor performance metrics of the System Manager and its hosting server. The Logical View and Physical View windows of the System Management Console provide an indication of the System Manager and server operational state. For each server, the system monitors CPU, memory, disk, and network interface usage. Operational measurements (OM) for the System Manager processes, consist of counters and gauges. Use the OM browsers of the System Management Console to view these OMs..

For information about using the System Management Console, see *System Management Console User Guide* (NN42020-110).

Server monitoring

Use the System Management Console to view the performance of a server that hosts the System Manager. Use the following procedure to monitor the System Manager server.

Procedure 10
Monitoring the System Manager server

Step	Action
1	From the configuration view pane, select **Servers > SESMServer1 > Monitor**. The Monitor window appears in the work area and displays statistics for CPU, Memory, Disk, and Interface usage.

2 If the Monitor window does not display data, and the status bar at the bottom of the Monitor window indicates `The server monitor is not running`, click the **Start Monitor** button.

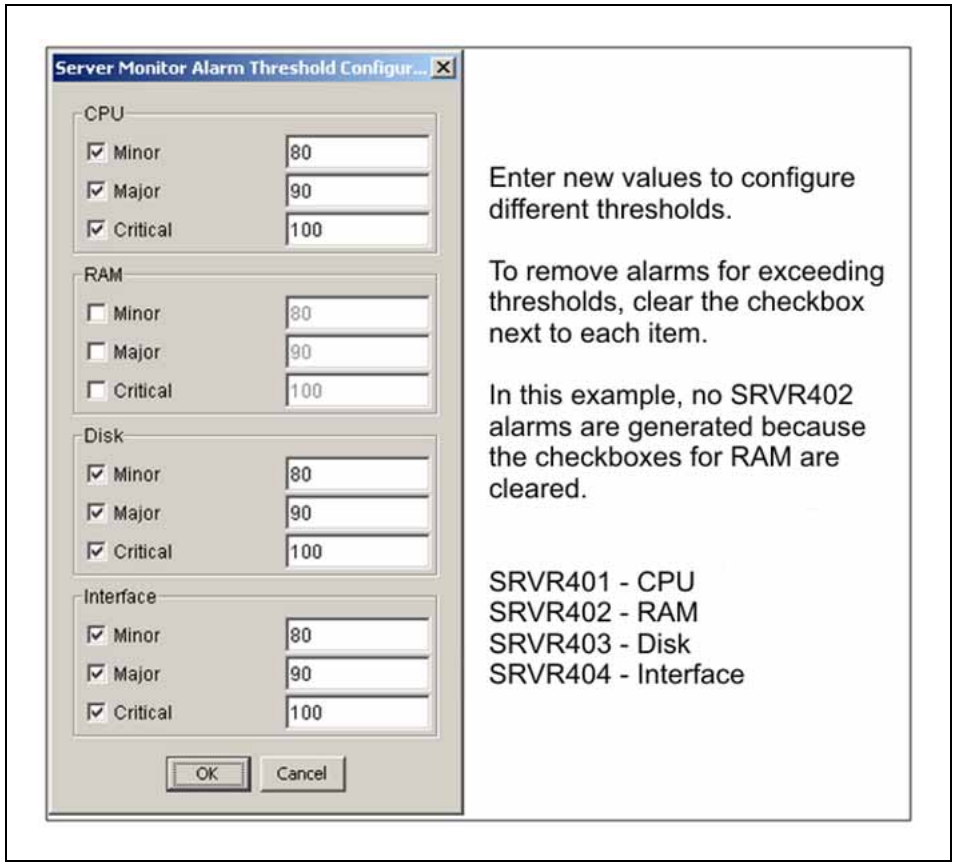
—End—

Additional information

While the server monitor runs, the system records server operational measurements to disk on the active instance of the System Manager. To see these operational measurements, use the OM browser in the System Management Console.

Configure thresholds for CPU, memory, disk, and interface usage from the Monitor window by clicking the Configure Thresholds button. To alter thresholds, you must have WRITE privileges for ServerMonitorConfigService.

Figure 4
Threshold configuration dialog box



Operational measurements

Operational measurements (OM) consist of counters and gauges that monitor the activity of the System Manager processes. For more information about viewing System Manager operational measurements, see *System Management Console User Guide* (NN42020-110).

Operational measurements are tallied in memory and recorded in an active file stored in the /var/mcp/spool directory on the network element that is generating the OMs. After the interval provisioned in the OfficeTransferPeriod configuration parameter expires, the data is flushed to the active file, the file is closed, and then the file is transferred to the System Manager or Fault Performance Manager that the network element uses. The System Manager and Fault Performance Manager record the data to the /var/mcp/oss directory as a holding file. This file is closed after it reaches the size or interval configured in the OM Format Path.

Use the System Management Console OM browser to view OMs that are generated by the System Manager. By default, the active OMs are displayed. These OMs have not been recorded to disk and represent the events that occurred since the last OfficeTransferPeriod interval expired. To display the most recent holding OMs, select Holding from the Type list. These OMs were stored to disk when the last OfficeTransferPeriod interval expired. To view older OMs, configure an FTP Push job to an OSS server and view the historic information there.

The OM file retention period is configured at the system level. For more information about the procedure for configuring the retention period, see *System Management Console User Guide* (NN42020-110).

Use the System Management Console and the following procedure to view OMs.

Procedure 11
Viewing OMs

Step	Action
1	Select **Network Elements > System Manager > SM** to make the OM browser button active.
2	On the icon toolbar, click the OM browser button.

Figure 5
OM browser button

—End—

For more information about available operational measurements, see *Operational Measurements Reference* (NN42020-704).

Local storage of operational measurements

The system records Operational measurement (OM) data to disk on the System Manager or FPM that a network element is configured to use. These records are stored as follows:

- System Manager

  /var/mcp/oss/om/MCP_9.0/SM_0/

- Fault Performance Manager

  /var/mcp/oss/om/MCP_9.0/<fpm_name>_0/

  The name of the FPM is typically a value like FPM1, which becomes FPM1_0 in the file system because there is only a single instance of an FPM as indicated by the underscore and zero.

Below these directories, a directory exists for each network element instance that reports data to the System Manager or FPM.

Security and administration

The topics in this chapter include:

Security

The System Manager operates within the private MCS network, isolated from public network security risks. System access is the primary security risk to the System Manager and hosting servers, so access is password protected. Access must be limited to trusted administrative personnel.

Administrators may need to log on to the servers hosting the System Manager software to perform a manual failover procedure. The log on requires use of the nortel user account and the physical IP address of the server.

To prevent nontrusted employees from logging on to the servers, Nortel recommends that both the password and server IP addresses remain confidential. After initial provisioning, The system administrator can create an administrative role without IPAddressService privileges and assign administrators with maintenance responsibilities to this role. Administrators with this role cannot view IP addresses, add servers to the network, or perform most configuration tasks. This role is appropriate for an alarm and log monitoring-only administrative account.

You can change SNMP community string values for a server from the default value (public) to some other value for network security reasons. After the SNMP community string value is configured for a server, it is applied to the SNMP message traffic of the hosted components. For more information about configuring an SNMP Profile to use the new the community string, see *System Management Console User Guide* (NN42020-110).

Administration

The System Manager uses software loads to determine the versions of software that are available for use. Software loads are added onto the server hosting the System Manager through zip files. When an administrator performs an add or update task from the System Management Console, the System Manager accesses the installed software loads and generates the load list displayed in the System Management Console.

To free up disk space on the server, administrators with the appropriate privileges can remove old and unused software versions by removing the associated directory and zip file from the server hosting the System Manager. For more information about removing a software load, see the procedure Removing software loads.

Server backups

Use MCS server backups to recover from a catastrophic hardware failure where a complete restore of the server software (both third-party and MCS software) is required. Nortel recommends backup of the System Manager hosting servers after third-party software updates, such as an applied operating system patch.

For details regarding backup procedures for MCS servers, see *Routine Maintenance* (NN42020-502).

Removal of software loads

In a network with redundant instances of the System Manager, the software pools are present on both servers that host the System Manager. You must remove the software loads from both servers to fully remove the older versions.

Before performing the following procedure, use the System Management Console to review the software loads that are used by all instances of all network elements to ensure that the load that you want to remove is not used by a network element. Use the following procedure to remove software loads from the server that hosts the System Manager.

ATTENTION

Contact your next level of support if you must perform this procedure and you do not have the required server access.

Procedure 12

Removing software loads

Step	Action
1	At the management PC, log on to the server hosting the System Manager.

2 Change directory to the location of the software loads:

```
cd /var/mcp/loads
```

3 List the software loads:

```
ls
```

4 From the list of available software loads, determine the loads that are not in use and can be safely removed.

CAUTION
The following steps delete all the files from the directory where you execute the rm -rf command. Ensure you are in the correct directory before executing the command.

5 Delete the files of the software load from the file system:

```
/bin/rm -rf <load_name>
/bin/rm <load_name>.zip
```

The zip file may not be present in the file system if the zip file was deleted after installing the software load.

Example
To delete the MCP_9.0.0_2005-10-10-2335 software load, the commands are as follows:

```
/bin/rm -rf MCP_9.0.0_2005-10-10-2335
/bin/rm MCP_9.0.0_2005-10-10-2335.zip
```

The files and directory with the software are removed. The deleted software load is no longer available for provisioning against a network element instance at the System Management Console.

6 If there is a redundant unit, repeat this procedure on the other unit. In addition, ensure that the remaining software loads reside on both units.

—End—

System Management Console message of the day

You can configure a message of the day file by using the System Manager. The contents of this file appear at the System Management Console interface after a successful log on. If the message of the day file does not exist, no message of the day window appears.

Limitations

The message of the day file does not persist after software upgrades or updates. During the System Manager software upgrade or update, the directory that holds the message of the day file is overwritten and the file is destroyed.

In redundant configurations, the message of the day file is not automatically created or updated on the second System Manager instance. Transfer the file to or create a second version of the file on the second System Manager instance.

Use the following procedure to configure the message of the day.

Procedure 13
Configuring the message of the day

Step	Action
1	At the management PC, log into the System Manager server as the nortel user.
2	Change directory: `cd /var/mcp/run/MCP_9.0/SM_x/data`
3	Create a file named **`motd.txt`** by using an editor, such as vi.
4	In the motd.txt file, enter the message that you want to display.
5	Save the motd.txt file. At the next successful log on from the System Management Console, the message appears.

—End—

Nortel Multimedia Communication Server 5100

System Manager Fundamentals

Publication: NN42020-109
Document status: Standard
Document version: 01.01
Document date: 29 January 2007

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

Sourced in Canada