NN10369-111

Carrier Voice over IP

Communication Server 2000

System Manager Basics

(I)SN08 Preliminary 03.01 March 2005

NORTEL

Overview

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

Topics in this chapter

How this guide is organized

This guide contains the following information:

- Upgrades on page 9

  Describes the upgrade strategy of the System Manager software.
- Fault management on page 25

  Describes the fault management strategy and manual failover of the System Manager.
- Configuration management on page 41

  Describes the configuration strategy and the property fields of the System Manager component services.
- Accounting management on page 75

  Describes the accounting activities of the System Manager.

- Performance management on page 77

  Describes the performance management strategy of the System Manager software and hosting servers.

- Security and administration on page 83

  Describes the security issues and administrative tasks related to the operations of System Manager services.

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 or the Open Managemant Interface (OMI). 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, and restart network element services
  - IPCM device diagnostics (e.g. i2004) and firmware upgrades
  - H.323 Endpoint diagnostics
- 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 CVoIP 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 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. Likewise, 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)

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

Simple Network Management Protocol version 2c (SNMPv2c)

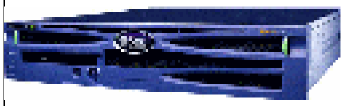
SNMPv2c is used to poll the System Manager for alarm events. The SNMPv2c polling can be used to report MCS alarms to an existing network management system.

Secure File Transfer Protocol (SFTP)

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

Server hardware

The number of servers and the network elements sharing a server depend on the specific deployment scenario. For the limited availability MCS 5200 4.0 release, only the Sun Microsystem Netra* 240 hardware has been verified.

Hardware	Details
Netra 240 	The server has the following hardware features: • AC or DC power • 2 x 1.28 GHz UltraSPARC IIIi processors • 1 MB integrated L2 cache • 4 GB RAM • 2 x 73 GB SCSI hard drives, 15 000 RPM • 4 x 10/100/1000 Base-T Ethernet ports operating at 100 Mbps • 1 x 10 Mbps Ethernet port for LOM • 2 X USB ports • 1 x TIA/EIA-232F RJ45 serial ports • 1 x TIA/EIA-232-F asynchronous (DB9) serial port • 1 x DVD-ROM drive

Hardware	Details
Sun Fire* V100 	The server has the following hardware features: • AC power only • 1 x 550 MHz UltraSPARC IIi processor • 512 KB internal cache • 1 GB RAM • 2 x 80 GB IDE hard drives, 7 200 RPM • 2 x 10/100 Base-T Ethernet ports operating at 100 Mbps • 2 x USB ports • 2 x RS-232C/RS-423 RJ45 serial ports • 1 x 24X CD-ROM Drive
Netra t 1400/05 ***Note:*** This hardware is not available for new installations. It is supported in this release and is available for exapansion of existing sites.	The server has the following hardware features: • AC or DC power • 4 x 440 MHz UltraSPARC II processors • 4 MB internal cache • 4 GB RAM • 36 GB SCSI hard drives, 10 000 RPM — 2 drives when deployed for Session Manager — 4 drives when deployed for System Manager, Accounting Manager, or Database Manager • 1 x PCI Quad Fast-Ethernet controller providing 4 x 100 Base-T Ethernet ports • 1 x 12 GB 4 mm DDS-4 internal tape drive when deployed for a System Manager, Accounting Manager, or Database Manager • 2 x RS-232C/RS-423 DB-25 serial ports • 1 x 10X DVD-ROM Drive

Fault tolerance

In redundant network architectures, the System Manager is hosted 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 high availability of these two fundamental network elements. If the active System Manager or its hosting server fails, a manual failover allows the transfer of the System Manager operations to the cold standby server. Likewise, if the active Accounting Manager or its hosting server fails, an administrator can failover the Accounting Manager operations to the cold standby server. See Fault management on page 25 for additional information.

Upgrades

Full upgrades to the System Manager software should only be performed with involvement from your next level of support. An example of an upgrade scenario is upgrading from the 3.0 release to the 4.0 release.

For updates, system administrators use a script that automates the manual deployment of a new System Manager version, and the undeployment of the existing version. The script must be executed as the nortel user. In most instances, this requires the involvement of your next level of support. An example of an update is MCP_4.0.0_2005-01-13-2335 to MCP_4.0.0_2005-01-20-2335.

When there are primary and secondary System Manager servers, the standby can be updated without interruption of System Manager services or the loss of the System Management Console connection. When updating the primary server, the System Manager processes are stopped and the System Management Console connection is lost.

Topics in this chapter

Updating the System Manager

Updating the System Manager version is performed using a script. The script is run on the server hosting the System Manager and must be run as the nortel user. This may require involvement from your next level of support.

Required information

System administrators require the following information when performing the procedure, editing the installprops.txt file, and running the software update script.

- Physical IP address of the server hosting the System Manager being updated
- MCP software load (zip file)
- Whether or not the database is replicated
- Primary database logical IP address
- Secondary database logical IP address if the database is replicated
- System Manager logical IP address

Action

At a workstation

1 FTP or secure copy the software load zip file to the System Manager server being updated. The suggested location to put the load is `/var/mcp/loads`.

2 Log in to the server hosting the System Manager being updated using the physical IP address of the server.

3 Change directory to the location of the software load zip file and unzip it:

```
cd /var/mcp/loads
unzip MCP_4.0.0_2004-10-10-2335.zip
```

Note: The actual zip file name will vary.

A new directory is created in /var/mcp/loads and is named similar to the zip file name, without the .zip suffix. The software load update is in this new directory.

4 Identify the directory in /var/mcp that holds the existing installprops.txt file. It may be /var/mcp/lab, but is site specific and is identified as /var/mcp/<site> for the remainder of this procedure.

5 Copy the install files from the data and bin directories to the new directory:

```
cd /var/mcp/loads/<MCP_load>/install_scripts

cp data/* /var/mcp/<site>
cp bin/* /var/mcp/<site>
```

A listing of the /va/mcp/<site> directory should resemble the following:

```
$ ls /var/mcp/<site>
Staging2Server.tags    Upgrade.xml            mcpInstall.pl
Staging2Server.xml     dbInstall.pl           mcpUpgrade.pl
Staging4Server.tags    dbUninstall.pl         smDeploy.pl
Staging4Server.xml     installUtils.pm        smInstall.pl
Staging8Server.tags    installprops.txt       smUndeploy.pl
Staging8Server.xml     mcp3.0To4.0Upgrade.pl  smUpgrade.pl
$
```

6 Edit the installprops.txt file and update it with the required parameters. An example of the installprops.txt file is located at the end of this procedure.

```
cd /var/mcp/<site>
vi installprops.txt
```

The installprops.txt file is opened in the terminal window. Enter the required parameters, save the file, and close it. Optionally copy the file to the /admin directory so the file is backed up at the next scheduled backup.

> ***Note:*** *Set field db.backup to Y so that a database dump is made and is available in case rollback is needed. Enabling this option does slow the update though.*

7 Run the **mcpUpgrade.pl** script:

```
./mcpUpgrade.pl -p installprops.txt
```

> ***Note:*** The username must be 'nortel' to run this script.

A log file is opened in /var/mcp/install/logs and is named mcpUpgrade.log.HH_MM_SS where HH_MM_SS is the hour, minute, and second that the script was started.

The variables provisioned in the installprops.txt file are validated and printed to the terminal.

```
-----------------------------------
Management (SM) Information:
  Host:             47.47.47.47 (local host)
  Port:             12100
  NE Name:          SM
  Instance:         0
  Load:             MCP_4.0.0_2004-10-10-2335
  Config:           V100_Standard

Database Information:
  Host:             47.47.47.48
  NE Name:          mcpdb
  Username:         mcpuser
  Password:         password
  Type:             Single
  Perform Backups: Y

Operation being performed: UPGRADE

Continue with these settings?(Y/N)[N]:
```

8 Enter **Y** to confirm the prompt.

The upgrade continues. The database is updated first. A backup of the database is performed and requires approximately 10 minutes. An update may change the database schema, if so, these changes require approximately 10 minutes. If the database is replicated, the replication begins and may require a prolonged time.

After the database is updated, the System Manager software is updated. The currently running load is stopped and undeployed. The updated load is deployed and the System Manager is started with it.

9 Determine the next action:

If	Do
this is the only System Manager server	This procedure is complete.
there is a second System Manager server to update	Proceed to step 10.

10 FTP the zip file and the installprops.txt file to the second unit. Place the zip file in /var/mcp/loads.

11 Login to the second unit as user nortel and prepare the software load:

```
cd /var/mcp/loads
unzip MCP_4.0.0_2004-10-10-2335.zip
```

12 Ensure that the /var/mcp/lab or <site> directory exists similar to step 4.

13 Copy the install files from the data and bin directories to the new directory:

```
cd /var/mcp/loads/<MCP_load>/install_scripts

cp data/* /var/mcp/<site>
cp bin/* /var/mcp/<site>
```

14 Edit the installprops.txt file. The following changes are required:

- ne.mgmt.ip — this identfies the physical IP address of this server
- ne.instance.id — change this value to 1 to indicate this is the SM_1 instance.

At the System Management Console

15 Select **Network Elements > System Manager > SM > Instance** from the config view.

The SM Instance window opens in the work area.

16 Select the second instance fro mthe SM Instance window and click **Edit**.

The Edit SMInstance dialog box opens.

17 Use the pull down menu to select the load from field Load. Click **Apply**.

The Edit SMInstance dialog box closes.

18 Select **NE Maintenance** from the config view.

The SM Maintenance window opens in the work area.

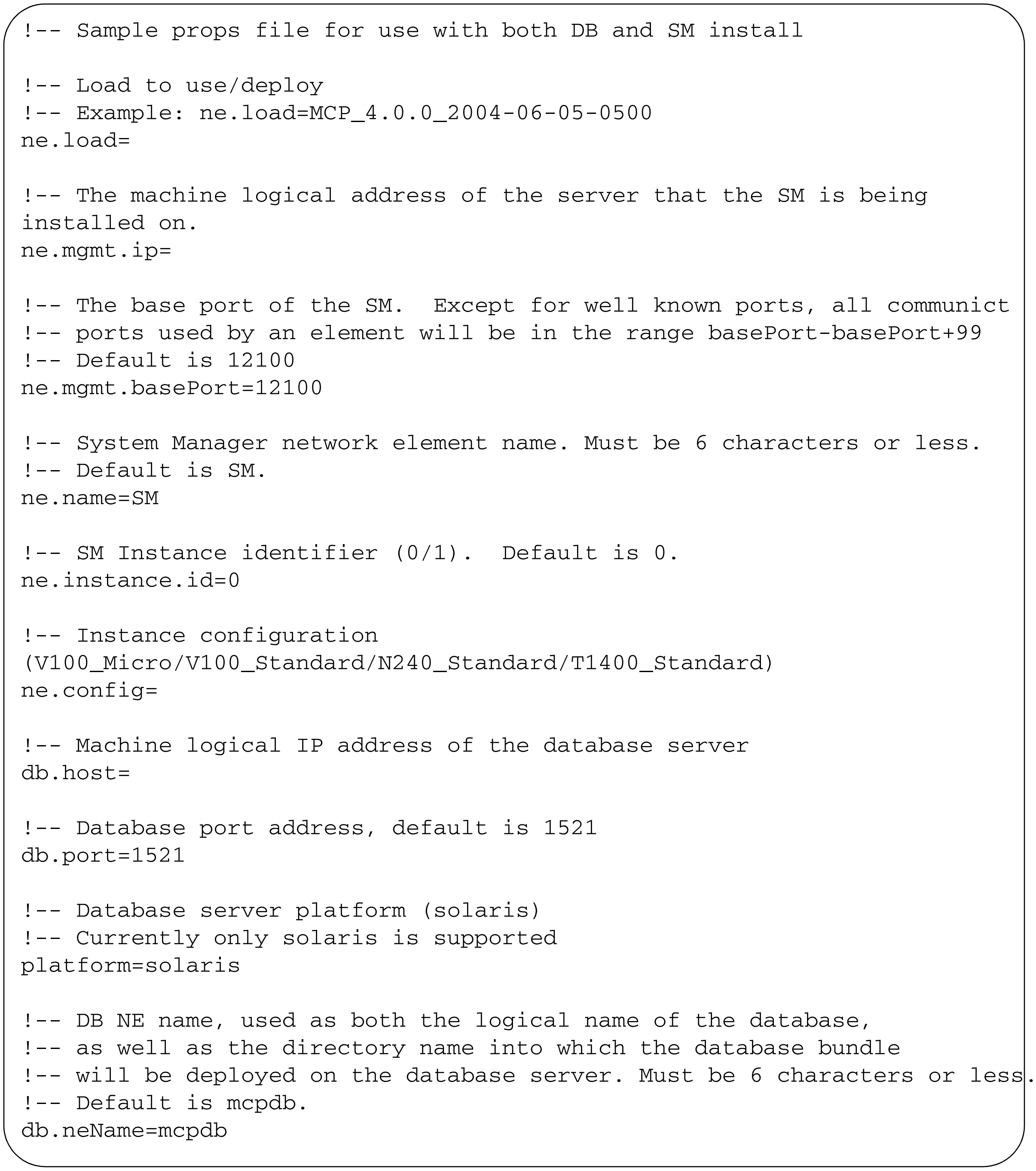
19 Select the CONFIGURED instance and click **Deploy**.

The software load is installed on the second System Manager server. The instance transitions to OFFLINE. The software is not started, but is available to be started if the first unit fails.

20 This procedure is complete.

Additional information

The following figure shows an example of an empty installprops.txt file.



```
!-- Sample props file for use with both DB and SM install

!-- Load to use/deploy
!-- Example: ne.load=MCP_4.0.0_2004-06-05-0500
ne.load=

!-- The machine logical address of the server that the SM is being
installed on.
ne.mgmt.ip=

!-- The base port of the SM.  Except for well known ports, all communict
!-- ports used by an element will be in the range basePort-basePort+99
!-- Default is 12100
ne.mgmt.basePort=12100

!-- System Manager network element name. Must be 6 characters or less.
!-- Default is SM.
ne.name=SM

!-- SM Instance identifier (0/1).  Default is 0.
ne.instance.id=0

!-- Instance configuration
(V100_Micro/V100_Standard/N240_Standard/T1400_Standard)
ne.config=

!-- Machine logical IP address of the database server
db.host=

!-- Database port address, default is 1521
db.port=1521

!-- Database server platform (solaris)
!-- Currently only solaris is supported
platform=solaris

!-- DB NE name, used as both the logical name of the database,
!-- as well as the directory name into which the database bundle
!-- will be deployed on the database server. Must be 6 characters or less.
!-- Default is mcpdb.
db.neName=mcpdb
```

```
!-- Database username.  Default is mcpuser
db.user=mcpuser

!-- Database password.  Default is mcpuser2001
db.password=mcpuser2001

!-- DB type (Single or Replicated)
!-- Default is Single
db.type=Single

!-- If type set to Replicated (above), then provide
!-- valid machine logical IP address for the Secondary database (ignored
!-- instance is set to Single)
db.secHost=

!-- Should database be backed up on upgrades, default is Y
db.backup=Y

!-- Device to perform backups to (DISK or TAPE), default = DISK
db.device=DISK
```

Rolling back an update

CAUTION
Possible service interruption
Read and understand this procedure entirely before beginning the rollback.

Understand that rolling back some system configurations causes an interruption of service.

The following system configurations are covered in this procedure:

- redundant system (Session Managers are in a 1+1 configuration and the database is replicated)
- non-redundant system with a replicated database
- non-redundant system with a single database

Required information

System administrators require the following information:

- A list of all the network element application names, such as SESM1, SESM2, RTP1, and a the IP addresses of the network elements. Use this list to mark off each network element as it is rolled back.
- Physical IP address of the server hosting the System Manager being updated
- MCP software load (zip file)
- Whether or not the database is replicated
- Primary database logical IP address
- Secondary database logical IP address if the database is replicated
- System Manager logical IP address

Limitations

Rollback has the following limitations:

- Rollback is only supported from a release 4.0 load to a release 4.0 software load that was already deployed and running in the past. Rollback from release 4.0 to release 3.0 is not covered in this procedure.
- An attempt to rollback to a software version that was not deployed in the past fails. Refer to Rollback scenarios for more information.

- The version of the software that is rolled back to must exist in directory /var/mcp/loads on the System Manager server.
- Registrations written to the secondary database during the rollback are lost.

Rollback scenarios

The database can only be downgraded to a version which had been successfully deployed in the past. The reason for this is a downgrade restores the database back to a previous version using a backup that was taken right before the database was upgraded from that version. For example, consider the following series of database deployments:

1. MCP_4.0.0_2005-01-13-2335 — *mcpInstall.pl performed the initial deployment of the database load*
2. MCP_4.0.0_2005-01-20-2335 — *mcpUpgrade.pl created a backup of the MCP_4.0.0_2005-01-13-2335 database with its current contents*
3. MCP_4.0.0_2005-01-27-2335 — *mcpUpgrade.pl created a backup of the MCP_4.0.0_2005-01-20-2335 database with its current contents*

At this point in time, the system can rollback to either of the following:

- MCP_4.0.0_2005-01-13-2335 — *rollback would restore the database using the backup taken when the database was upgraded to the MCP_4.0.0_2005-01-20-2335 load*
- MCP_4.0.0_2005-01-20-2335 — *rollback would restore the database using the backup taken when the database was upgraded to MCP_4.0.0_2005-01-27-2335*

An attempt to downgrade to any other version fails because there is no backup of the databse to restore.

Action

At a workstation

1 Log in with the oracle account to the primary Database Manager.

2 Remove database replication:

```
$ cd /var/mcp/run/MCP_4.0/mcpdb_0/bin/
$ ./cleanupReplication.sh <dbUser> <dbPasswd>
```

Downgrade the primary database

In simplex database environments, this stage downgrades the only database instance. Understand that in simplex database environments, once the database is downgraded, call processing becomes unpredictable because network elements that have been upgraded and require database access to perform call processing are not able to connect to the database.

At a workstation

3 Log in with the nortel account to the primary System Manager.

4 Change directory to the installprops.txt file:

```
$ cd /var/mcp/<site>
```

5 Edit the installprops.txt file to use the old software load for field ne.load.

6 Deploy the old database software load with the files only option. This step does not restore the database contents, that is done after this step.

```
$ cd /var/mcp/<site>
$ ./dbInstall.pl -p installprops.txt -fo
```

When asked "Deploy Files Only" operation to Secondary DB also (Y/N)? Answer **Y**.

7 Log in with the oracle account to the primary Database Manager.

8

> **CAUTION**
>
> **Possible service interrption**
>
> If the database is not redundant, then call processing results are unpredictable since network elements that may require database access to complete calls are not able to access the necessary data. This unpredictable situation remains until all network elements are downgraded.
>
> If the database is redundant, call processing is not disrupted.

Retore the database backup to the primary database with the dbRestore.sh command:

```
$ cd /var/mcp/run/MCP_4.0/mcpdb_0/bin
$ ./dbRestore.sh <dbUser> <dbPasswd>
<backupName> DISK
```

Note: Parameter <backupName> is a value like 4.0.0_2005-02-13-2335 and indicates a dump file that must be located in /var/mcp/backup/orabackup.

The data is loaded into the primary database. The database must be restarted, so a prompt for the root password is presented. Enter the root password.

At this point the primary database is downgraded. Note that if the database is redundant, then network elements running with the new load will only connect to the secondary database because the secondary database is still running the new load. In a redundant database configuration, call processing is not disrupted.

Downgrade the primary System Manager

In a simplex System Manager configuration, this stage downgrades the only System Manager instance. Understand that OAM communication is lost briefly for simplex System Manager configurations. Additionally, even if the System Manager is redundant, operators may choose to accept the brief loss of OAM communication and skip the failover process.

At a workstation

9 Log in with the nortel account to the primary System Manager.

10 Determine the next action.

If the System Manager	Do
is not redundant	Follow steps 11, 15, 16 and 20. Note that OAM communication is lost until step 20 is complete.
is redundant, but loss of OAM communication for approximately 3 minutes is acceptable	Follow steps 11, 15, 16 and 20. Note that OAM communication is lost until step 20 is complete.
is redundant and operators are willing to failover the System Manager to retain OAM communication	Proceed with the following steps in order.

11 Stop the System Manager application:

```
$ cd /var/mcp/run/MCP_4.0/SM_x/bin
$ ./neStop.pl
```

Replace SM_x in the above path with SM_0 or SM_1, depending on which is the active and primary System Manager. Most likely, SM_0 is the right choice.

After the neStop.pl command is entered, the System Manager application stops running and the System Management Console connection closes.

12 Log in with the nortel account to the secondary System Manager.

13 Start the System Manager application to complete the failover:

```
$ cd /var/mcp/run/MCP_4.0/SM_y/bin
$ ./neStart.pl
```

Note that the path to the command is not the same on this server. Once the neStart.pl command is entered, the System Manager application starts and network elements begin communicating with this instance of the System Manager.

Start the System Management Console again to monitor network elements.

14 Log in with the nortel account to the primary System Manager.

15 Edit the installprops.txt file to reference the load old in field ne.load if this wasn't done in step 5.

16 Deploy the old load to the primary System Manager:

```
$ cd /var/mcp/<site>
$ ./smUpgrade.pl -p installprops.txt
```

The old software load is deployed on the currently stopped System Manager.

17 Log in with the nortel account to the secondary System Manager.

18 Stop this instance of the System Manager to begin the failover back to the primary System Manager:

```
$ cd /var/mcp/run/MCP_4.0/SM_y/bin
$ ./neStop.pl
```

> ***Note:*** This command is performed from the same directory as the command in step 13.

The System Management Console connect closes.

19 Log in with the nortel account to the primary System Manager:

20 Start the downgraded System Manager software:

```
$ cd /var/mcp/run/MCP_4.0/SM_x/bin
$ ./neStart.pl
```

The failover to the primary System Manager is complete. At this point the primary System Manager is downgraded. The downgraded System Manager connects to the primary database, since they are running the same software version. If the System Manager is redundant, the secondary instance is still *running the new software load and is downgraded later in this procedure. Relaunch the System Management Console to monitor the network elements.*

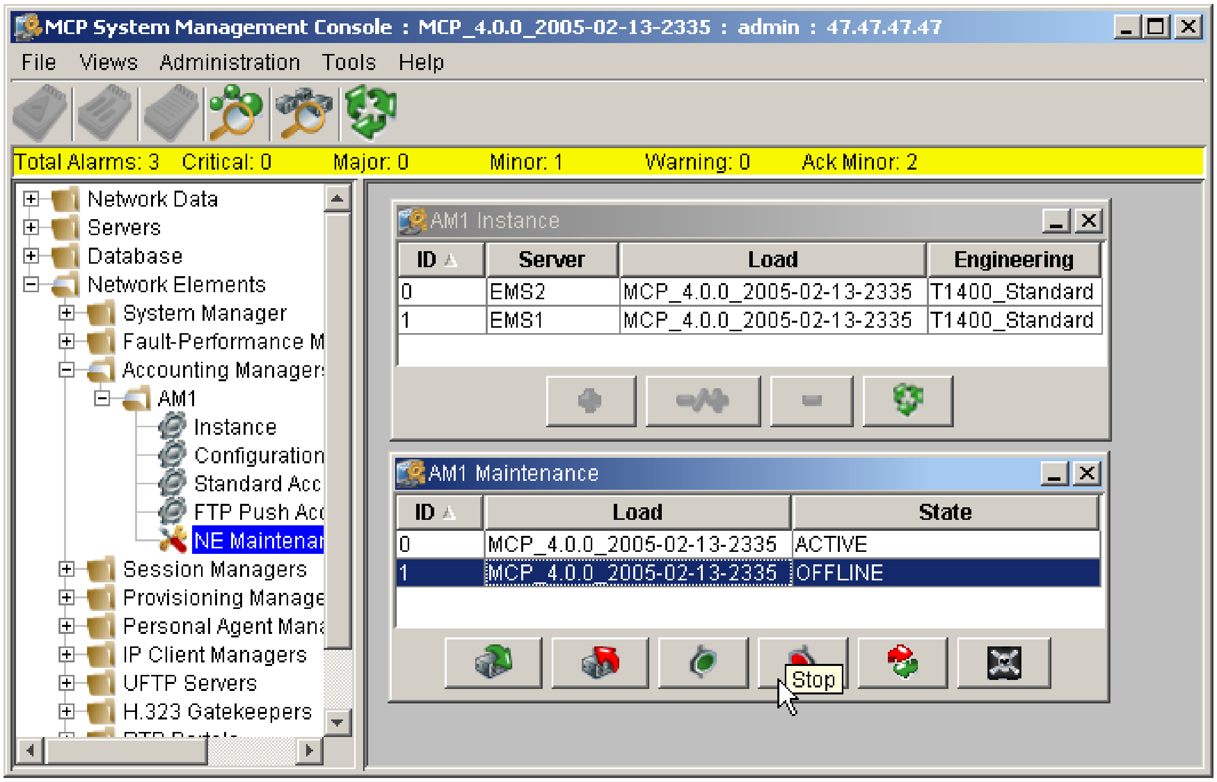
Note that all other network elements are still connected to the secondary database if the database is redundanr. If the database is not redundant, call processing remains unpredictable.

Downgrade all other network elements

Use the System Management Console to downgrade all other network elements, starting with the Accounting Manager and then traversing the config view downward. Note that the decision in step 26 is based on the fact that redundant Accounting Managers require a manual failover process of stopping the running instance and starting the previously stopped instance.

At the System Management Console

21 Open the **Instance** and **NE Maintenance** windows for a single network element such as AM1. The display should be similar to the following figure.



AM1 Instance

ID	Server	Load	Engineering
0	EMS2	MCP_4.0.0_2005-02-13-2335	T1400_Standard
1	EMS1	MCP_4.0.0_2005-02-13-2335	T1400_Standard

AM1 Maintenance

ID	Load	State
0	MCP_4.0.0_2005-02-13-2335	ACTIVE
1	MCP_4.0.0_2005-02-13-2335	OFFLINE

22 On the NE Maintenance window select the OFFLINE or WARM STANDBY instance. If the network element is not redundant, select the only instance.

Click **Stop**.

23 On the Instance window select the same numbered instance and click **Edit**.

An Edit Instance dialog box opens.

24 On the Edit Instance dialog box, use the pull down menu to select the old software load in field Load. Click **Apply**.

> ***Note:*** Perform the the actions described in this step even if the previous software load version is shown in field Load.

25 On the NE Maintenance window, select the same instance (it should be CONFIGURED) and click **Deploy**.

26 How to proceed with starting the downgraded software depends on redundancy and if the network element is an Accounting Manager. Determine the next action.

If the network element	Do
is not redundant	Select the only instance (should be OFFLINE) and click **Start**.
is a redundant Accounting Manager	Select the ACTIVE instance and click **Stop**. Select the other instance and click **Start**.
is any other redundant network element type	Select the OFFLINE instance, click **Start**, and wait for it to become WARM STANDBY. Then select the ACTIVE instance and click **Stop**. The currently ACTIVE instance becomes OFFLINE and the previously WARM STANDY instance becomes ACTIVE.

27 If the network element is redundant, repeat the actions in steps 23 through 25 to downgrade the software on the second instance of the network element. For redundant network elements, if the currently active instance is not the preferred active instance, repeat step 26.

28 Repeat the network element downgrade steps from step 21 to step 27 until all the remaining network elements are downgraded. One caution is to avoid starting more than one application at a time on Sun Microsystems v 100 servers. For example, do not start an IPCM instance and a UFTP instance at the same time. Wait for one to complete before starting the other.

At this point, only the secondary System Manager is running the newer software load and all other network element instances are rolled back to the old software load. In simplex database configurations, call processing returns to normal.

Downgrade the secondary System Manager

Ignore this section if the System Manager is not redundant.

At the System Management Console

29 Select **Network Elements > System Manager > SM > Instance** from the config view.

The SM Instance window opens in the work area. Consider opening the NE Maintenance window to confirm the OFFLINE instance.

30 Select the inactive instance (the instance labeled OFFLINE at the NE Maintenance window), and click **Edit**.

The Edit Instance dialog box opens.

31 Use the pull down menu to select the old software load from the Load field. Click **Apply**.

The dialog box closes and the instance transitions from OFFLINE to CONFIGURED on the NE Maintenance window.

32 On the NE Maintenance window, select the CONFIGURED instance and click **Deploy**.

The old software load is transferred to the secondary System Manager server.

At this point, all instances of all network elements are downgraded and all network elements are connected to the primary database.

Resynchronize the database

Ignore this section if the Database Manager is not redundant. The full resynchronization procedure is described in procedure "Resynchronization (only in a redundant architecture)" from the *CVoIP Database Manager Basics*. The key actions are repeated here for convenience.

Log in to the primary Database Manager server with the oracle account and start resynchronization with the Resync.pl command:

```
$ /var/mcp/run/MCP_4.0/mcpdb_0/bin/util/Resync.pl
```

Log in to the **secondary** Database Manager and then truncate non-replicated tables by executing the following command.

```
$ cd /var/mcp/run/MCP_4.0/mcpdb_0/bin/util
$ ./truncateNonRepdTables.sh <dbUser> <dbPasswd>
```

Use the Oracle Enterprise Manager to reenter the backup jobs. Refer to the *CVoIP Database Manager Basics*.

Downgrade complete

After the secondary database resynchronizes to the primary database, the downgrade is complete.

Fault management

The System Manager software includes all the functionalifty 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.

The primary fault management information used by administrators are alarms and logs. 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. Once collected, administrators can view the fault information using the System Management Console.

The following System Management Console tools are used for viewing and working with alarms and logs collected by 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 the alarm summary area is the color of the most severe alarm.

- Logical View and Physical View windows

  These two windows are launched from the System Management Console toolbar and provide immediate visual identification of alarmed network elements. After selecting an alarmed network element, the Alarm Browser can be opened.

- Alarm Browser

  Administrators use the alarm browser to view active alarms. The alarms for the System Manager are viewed by selecting the SM network element from the system tree and clicking on 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 browsers

  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 approximately 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 OSS tool for viewing them.

For information on using the System Management Console tools, refer to the *CVoIP System Management Console User Guide*.

For alarm descriptions and log information, refer to the guide *CVoIP Fault Management: Alarm and Log reference*.

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

SNMP information

The following informaton about how the System Manager uses SNMP is useful for integrating the MCS with an OSS system such as the Nortel Integrated EMS.

To forward traps northbound, perform procedure Configuring an SNMP Manager on page 48 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. The SNMP port and community string for the SNMP daemon on the destination host are needed to perform this procedure.

For networks that prefer to poll the System Manager and FPMs for data, the System Manager and each FPM offer an open 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 at 12117. For FPMs, select **Network Elements > Fault-Performance Managers** and view the Base Port for the configured FPMs. To configure SNMP parameters for the host that will fetch 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_4.0/SM_0/*
  ```

- Fault-Performance Manager

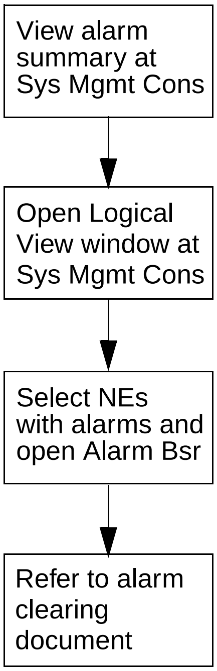
  ```
  /var/mcp/oss/om/MCP_4.0/<fpm_name>_0/*
  ```

  > ***Note:*** The name of the Fault-Performance Manager 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 is created for each network element instance that reports data to the System Manager or FPM.

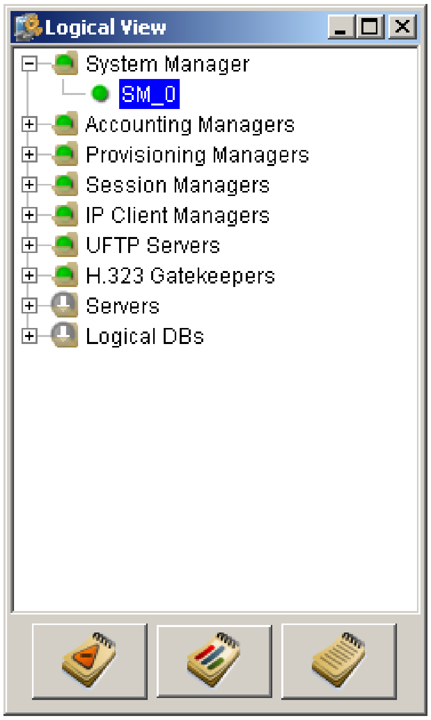
Fault management taskflow

Use the following flowchart to assist with clearing trouble conditions.


View alarm summary at Sys Mgmt Cons
Open Logical View window at Sys Mgmt Cons
Select NEs with alarms and open Alarm Bsr
Refer to alarm clearing document

Clear the most severe alarms first and then follow the order listed in the Logical View window: clear System Manager alarms before Accounting Manager alarms; clear Accounting Manager alarms before Provisioning Manager alarms, and so on.

Network Elements with alarms are identified with a red, orange, or yellow dot. A green dot indicates no trouble found.



Hosting server backup and restore

There are capabilities to back up and recover MCS server software and hardware as a result of specific hardware failures. These capabilities range from the ability to recover the hardware and software after minor server failures to the recovery of hardware and software after catastrophic server failures.

Backup of System Manager is recommended so that a restore of software and the server configuration can be completed after a catastrophic failure.

ATTENTION
Servers should be backed up according to a schedule. However, manual backup of an MCS server is recommended:

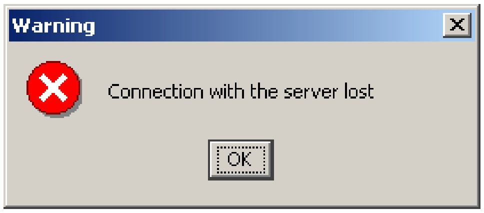
— after the Solaris Operating System is updated

— after an MCS software maintenance release for the System Manager is deployed

Please refer to the *MCS Backup and Recovery Guide* for details regarding backup and recovery procedures.

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 login prompt.



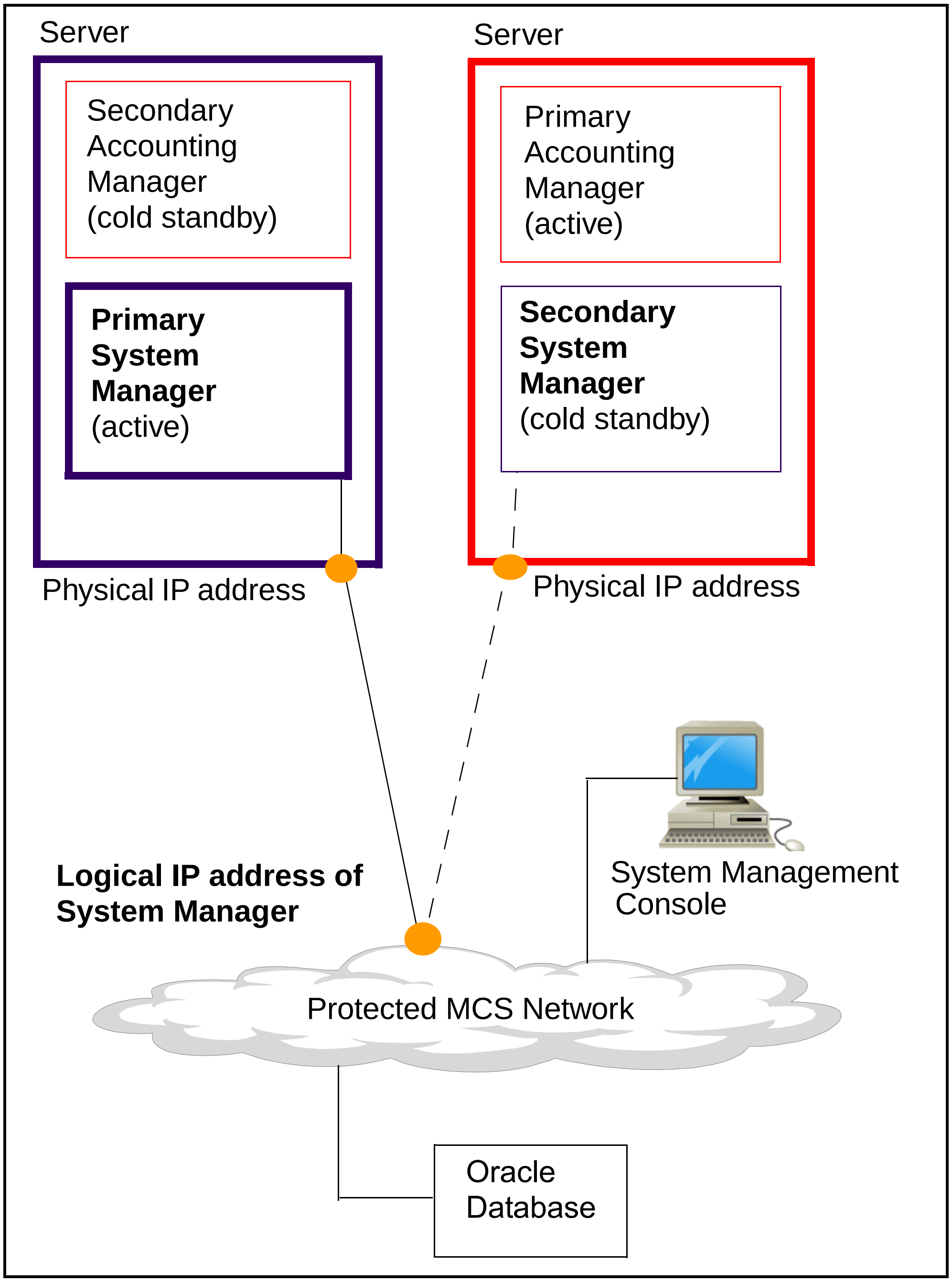
Connection with the server lost

The lost connection may or may not be an indication that the System Manager application on the System Manager or its hosting server has failed. If an attempt to login after a lost connection fails, administrators need to 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. A logical view of this configuration is shown in the following figure.

Figure 1 Redundancy of System Manager - logical view



Server
Secondary Accounting Manager (cold standby)
Primary System Manager (active)
Physical IP address
Server
Primary Accounting Manager (active)
Secondary System Manager (cold standby)
Physical IP address
Logical IP address of System Manager
System Management Console
Protected MCS Network
Oracle Database

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 a failover to the cold standby System Manager is initiated by an administrator.

The manual failover process involves stopping the System Manager processes and releasing the logical IP address from the System Manager server, and starting the processes on the server hosting the secondary System Manager. Both actions require the use of a UNIX login 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, we recommend that administrators have a log book with the information (physical and logical IP addresses, login information) required to perform the failover.

Physical IP addresses of the System Manager servers

Administrators need to know the physical IP addresses of the servers hosting the primary and secondary System Manager network elements before performing a manual failover. The physical IP addresses of the active and cold standby System Manager are displayed in the work area of the System Management Console.

At the System Management Console

1 Select **Network Data** > **Addresses** in the config view.

The Addresses window opens in the work area.

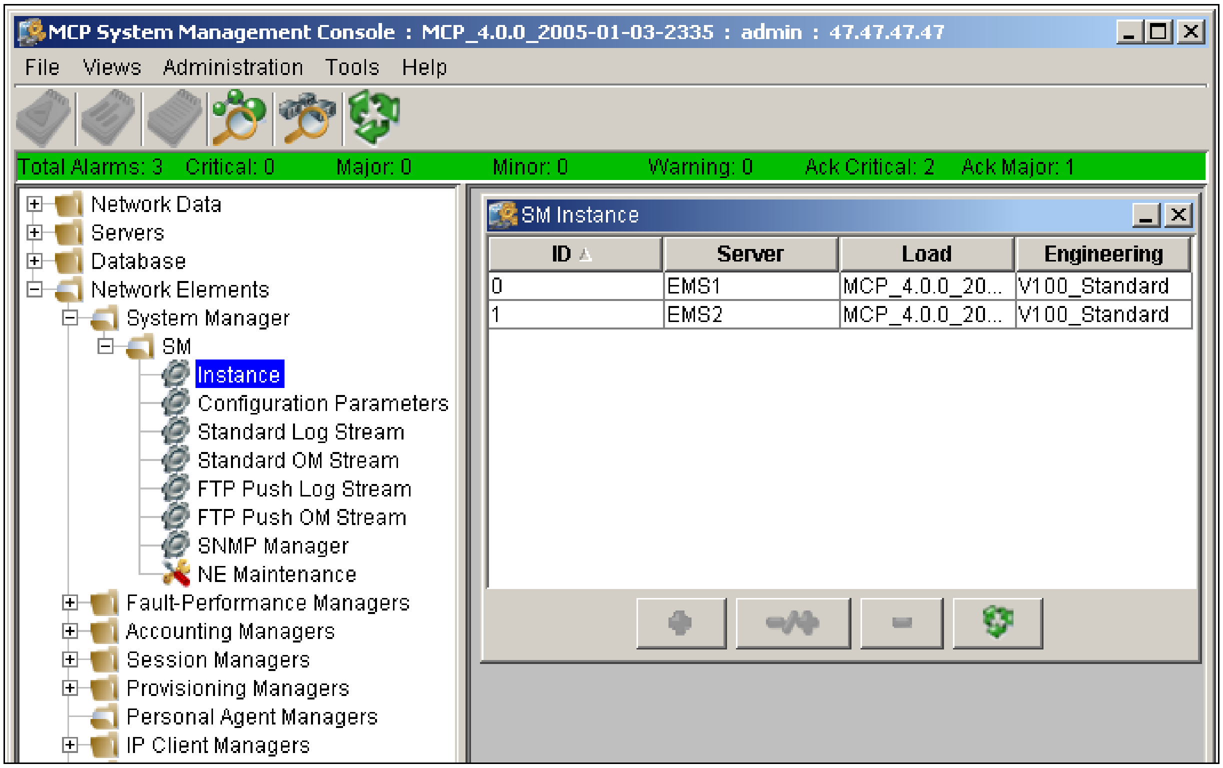
2 If the office is configured according to the Nortel recommended naming convention, the two System Manager server interfaces are deployed with Logical Names of **EMServer1Addr** and **EMServer2Addr**.

In this event, scroll to the two entries and record the IP addreses for these two servers.

3 If the office is not configured according to the Nortel recommended naming convention, select **Network Elements** > **System Manager** > **SM** > **Instance**.

The SM Instance window opens in the work area.

4 Determine the name of the Servers that the System Managers are deployed on.



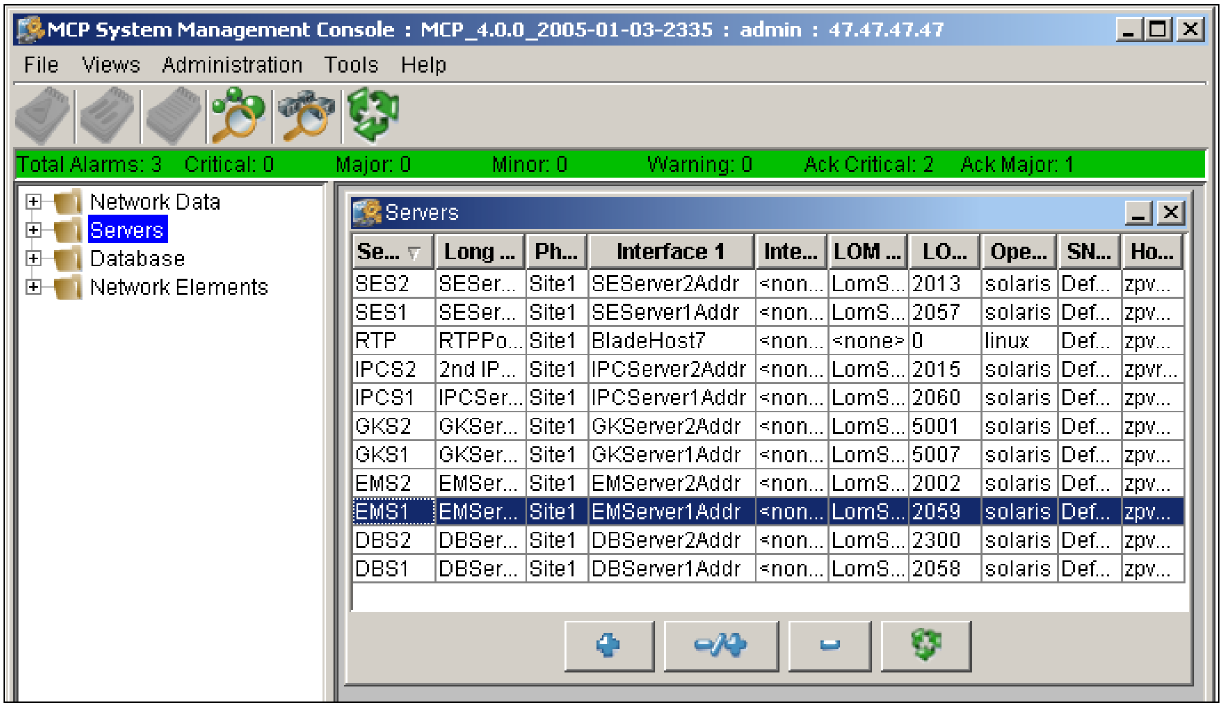
ID	Server	Load	Engineering
0	EMS1	MCP_4.0.0_20...	V100_Standard
1	EMS2	MCP_4.0.0_20...	V100_Standard

In this example, the two servers are EMS1 and EMS2. Close the SM Instance window after recording the server names.

5 Select the **Servers** folder in the config view.

The Servers window opens in the work area.

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



Se...	Long ...	Ph...	Interface 1	Inte...	LOM ...	LO...	Ope...	SN...	Ho...
SES2	SESer...	Site1	SEServer2Addr	<non...	LomS...	2013	solaris	Def...	zpv...
SES1	SESer...	Site1	SEServer1Addr	<non...	LomS...	2057	solaris	Def...	zpv...
RTP	RTPPo...	Site1	BladeHost7	<non...	<none>	0	linux	Def...	zpv...
IPCS2	2nd IP...	Site1	IPCServer2Addr	<non...	LomS...	2015	solaris	Def...	zpvr...
IPCS1	IPCSer...	Site1	IPCServer1Addr	<non...	LomS...	2060	solaris	Def...	zpv...
GKS2	GKSer...	Site1	GKServer2Addr	<non...	LomS...	5001	solaris	Def...	zpv...
GKS1	GKSer...	Site1	GKServer1Addr	<non...	LomS...	5007	solaris	Def...	zpv...
EMS2	EMSer...	Site1	EMServer2Addr	<non...	LomS...	2002	solaris	Def...	zpv...
EMS1	EMSer...	Site1	EMServer1Addr	<non...	LomS...	2059	solaris	Def...	zpv...
DBS2	DBSer...	Site1	DBServer2Addr	<non...	LomS...	2300	solaris	Def...	zpv...
DBS1	DBSer...	Site1	DBServer1Addr	<non...	LomS...	2058	solaris	Def...	zpv...

In this example, EMServer1Addr is the logical name of the address provisioned for server EMS1. Close the Servers window after recording the logical name of the addresses.

7 Select **Addresses** in the Network Data section of the config view.

The Addresses window opens in the work area.

8 Determine the IP address provisioned for each Logical Name.

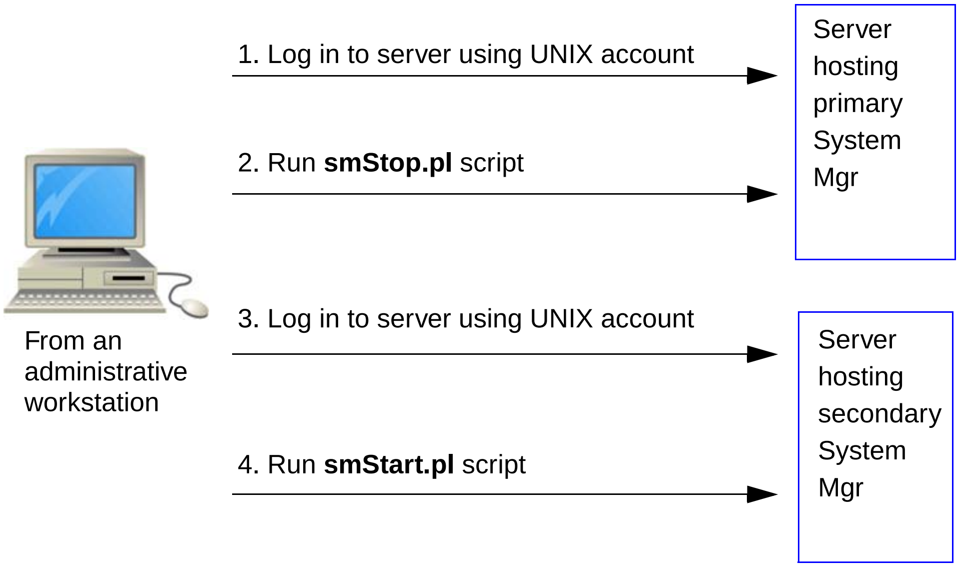
9 This procedure is complete.

Performing a 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 need to be stopped. Since the connection to the System Management Console is lost, administrators need to log on remotely to the standby System Manager server with a secure shell connection.

To log on to the servers, the administrators need to use the limited access account created for this procedure. The following figure shows the sequence of actions performed during the failover procedure.

Steps in performing a manual failover


1. Log in to server using UNIX account
2. Run **smStop.pl** script
Server hosting primary System Mgr
From an administrative workstation
3. Log in to server using UNIX account
4. Run **smStart.pl** script
Server hosting secondary System Mgr

See the following for the manual failover procedures:

- Stopping the System Manager processes
- Starting the cold standby System Manager
- Reverting back to the primary System Manager
- Failover impacts and recovery

Stopping the System Manager processes

Stop the primary System Manager if possible. If the hosting server is down, or in an isolated state, this will not be possible and administrators should proceed to the next step: Starting the cold standby System Manager.

At a workstation

1 Log in to the server running the active System Manager instance. Use secure shell.

IP Address : <physical address of server>

Login ID : **nortel**

```
ssh nortel@<phys_ip_address>
```

If this is the first time a secure connection has been made to the server from this workstation, you will be prompted to exchange keys. Respond with yes.

2 Execute the smStop.pl script to stop System Manager processes and release the logical IP address:

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

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

Starting the cold standby System Manager

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

At a workstation

1 Log in to the server running the cold standy System Manager instance. Use secure shell.

IP Address : <physical address of server>

Login ID : **nortel**

```
ssh nortel@<phys_ip_address>
```

If this is the first time a secure connection has been made to the server from this workstation, you will be prompted to exchange keys. Respond with yes.

2 Execute 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 finished, the screen will display the name and path of the log file associated with this event.

Reverting back to the primary System Manager

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

At a workstation

1 Close the System Management Console.

2 Log in 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 Log in 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.

Failover impacts and recovery

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

- Stopping the primary System Manager may not be possible due to network isolation of the System Manager server.

  Impact:

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

  Recovery:

  Administrators need to promptly shutdown one of the two active components. If possible, the administrator should try to connect to the management server through the terminal server and execute the smStop.pl script. In the event that two instances compete for the active role, log in to 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 is stopped.

- 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 may result in degraded capacity of both the management and accounting processes.

  Recovery:

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

Restarting a non-redundant System Manager

In a non-redundant 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 three times. If this doesn't work, software on the server waits five minutes and then tries to restart the software application an additional three times. If the software application still does not run, manual action is necessary.

The preferred method of restarting the System Manager is to log in to the server and start the System Manager instance. This method will not affect the other applications also running on the server.

At a workstation

1 Log in to the server hosting the System Manager application:

```
ssh nortel@<sys_man_phys_ip_address>
```

If this is the first time ssh has been used to log in from this workstation, there is a prompt to exchange keys. Respond to the prompt with yes.

If the network interface to the server is unavailable, a log in connection through a terminal server is necessary.

2 Issue the smStop.pl command:

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

The following output is generated for a successful stop.

```
$ /var/mcp/<site>/smStop.pl

Stopping System Manager

$
```

In the event of an error while stopping the processes, the script outputs `Error occurred stopping System Manager` *and then prints the command that failed.*

3 Execute the smStart.pl command:

```
./smStart.pl
```

The following output is generated for a successful start.

```
$ ./smStart.pl

Starting the System Manager
```

In the event of an error, the message `Error occurred starting System Manager` *is printed, and the command that failed is printed.*

4 This procedure is complete.

Configuration management

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 pre-configured with default values. The operational parameters for the System Manager are seperated into two groups, Configuration Parameters, and Engineering Parameters. Configuration parameters typically depend on network element type and traffic expectations for the network element. These parameters are changed as the network evolution requires. Engineering parameters are associated for a particular network element instance and are related to network element type and server configuration. Engineering parameters should only be modified in an emergency and modifications are lost after an upgrade.

Topics in this chapter

Optional configuration tasks

Log and operational measurement (OM) file rotation parameters are typically configured at the system level. However, they can also be configured with values for either a specific server or network element. Information on configuring the rotation parameters is documented in the *CVoIP System Management Console User Guide*.

SNMP community string values for a server can be changed from the default ‘public’ to some other value for network security reasons. Once configured for a server, it applies this community string value to SNMP message traffic of the hosted components. Information on configuring the community string is documented in the *CVoIP System Management Console User Guide*.

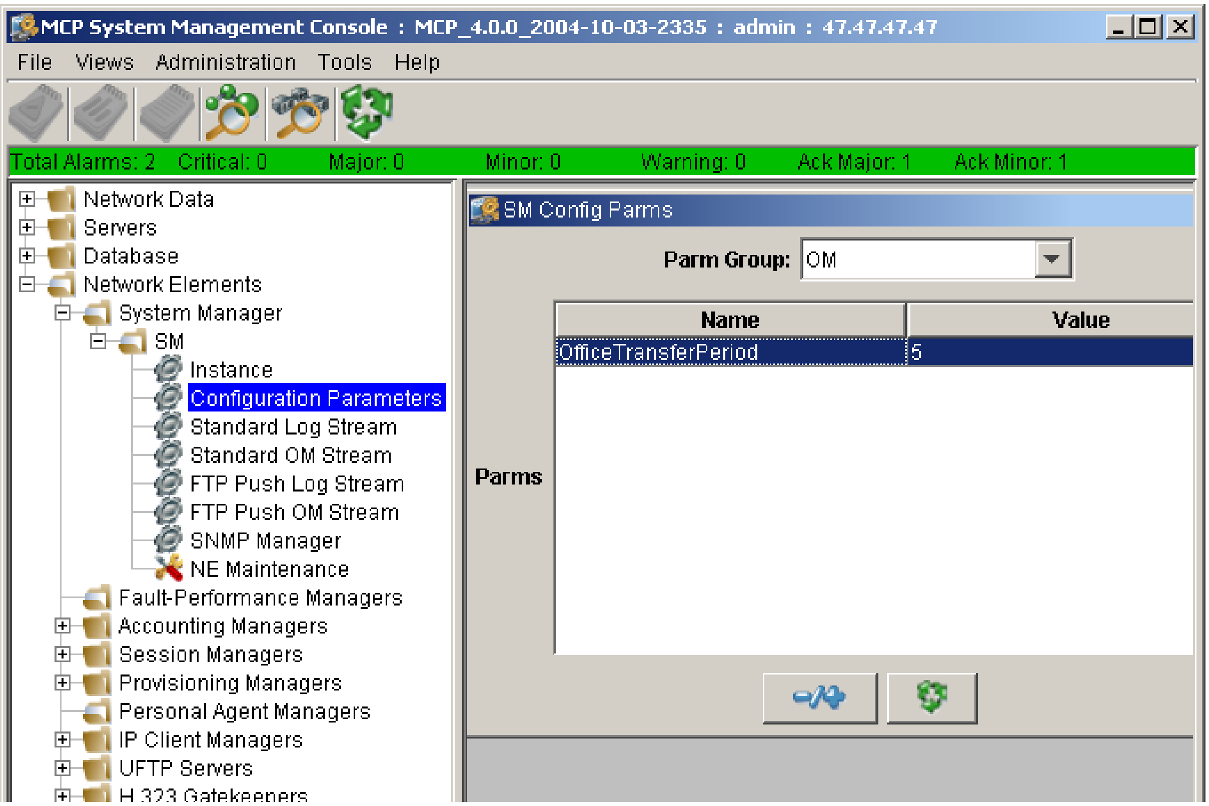
Configuring Configuration Parameters

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

This procedure requires an administrative role with WRITE permission for the ConfigParmService.

At the System Management Console

1 Select **Network Elements** > **System Manager** > **SM** > **Configuration Parameters** fom the config view:



MCP System Management Console : MCP_4.0.0_2004-10-03-2335 : admin : 47.47.47.47

Total Alarms: 2 Critical: 0 Major: 0 Minor: 0 Warning: 0 Ack Major: 1 Ack Minor: 1

SM Config Parms

Parm Group: OM

Parms

Name	Value
OfficeTransferPeriod	5

The SM Config Parms window opens in the work area.

2 Select a Parm Group from the SM Config Parms window and click **Edit**.

The Edit SM Config Parm window opens.

3 Enter a new value and click **Apply**.

The Edit SM Config Parm window closes and the data change is sent to all System Manager instances.

4 This procedure is complete.

Additional information

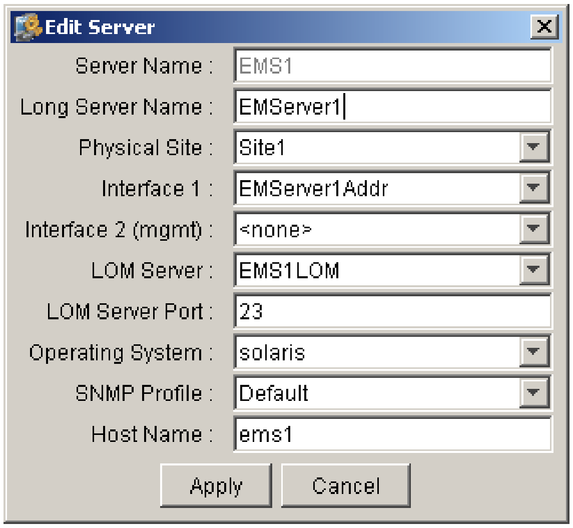
The following Configuration Parameters are available on the System Manager.

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.

Configuring an FTP Push Stream

The System Manager and any Fault-Performance Managers can be configured 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 managment interface at the System Management Console, then the data is transferred over that interface. If a second interface is not provisioned, the data is transferred over the first interface and may compete with call processing traffic. The following figure shows a server without a management interface configured.



Server Name : EMS1
Long Server Name : EMServer1
Physical Site : Site1
Interface 1 : EMServer1Addr
Interface 2 (mgmt) : <none>
LOM Server : EMS1LOM
LOM Server Port : 23
Operating System : solaris
SNMP Profile : Default
Host Name : ems1

Field Interface 2 (mgmt) is used to configure a management interface for a server.

Prerequisites

Before performing this procedure, ensure that the destination host is online and that connectivity is established between the System Manager and the destination host.

Action

Perform the following steps.

Add the IP address of the destination host

At the System Management Console

1 Select **Network Data > Addresses** from the config view to add the IP address of the destination host:

The Addresses window opens in the work area.

2 Click Add on the Addresses window.

The Add Addresses dialog box opens.

3 Enter a logical name for the destination host and the IP address of the destination host. Click **Apply**.

Add an OSS server

At the System Management Console

4 Select **Network Data > Profiles > OSS Server** from the config view to associate the logical name with an OSS server entry.

The OSS Server window opens in the work area.

5 Click Add on the OSS Server window.

The Add OSS Server dialog box opens.

6 Enter a name for the destination host and use the pull down menu to locate the IP address logical name. Click **Apply**.

Configure a format path

At the System Management Console

7 Optionally configure a format path for the information. This is done with the Record Format, File Type, and Format Path areas at the System Management Console. Refer to the *System Management Console User Guide* for information.

Add an FTP Push profile

At the System Management Console

8 Select **Network Data > Profiles > FTP Push** from the config view.

The FTP Push window opens in the work area.

9 Click Add on the FTP Push window.

The Add FTP Push Profile dialog box opens.

10 Enter the 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	pull down menu	Use the pull down menu to select the name associated with the OSS Server.
Root Directory	string	Enter the fully qualified directory path on the OSS Server to place the files. Note that the directory path must exist before activating the FTP Push.
User ID	string	Enter a user account that is active on the destination host.
Passsword	string	Enter the password for the User ID.
Confirm Password	string	Enter the password for the User ID again.

Click **Apply**.

Configure the System Manager and Fault-Performance Managers to use the FTP Push Profile

At the System Management Console

11 Expand **Network Elements > System Manager > SM** or **Network Elements > Fault-Performance Managers > FPMx** from the config view.

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

13 On the window that opens in the work area, click **Add**.

A dialog box opens.

14 Use the pull down menus to select the Format Path and FTP Push Profile. Click **Apply**.

15 This procedure is complete.

Configuring an SNMP Manager

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

If the destination host is already configured with an SNMP port and community string, this information is needed to perform this procedure. If the destination host is not already configured, then the values for SNMP port and community string entered during this procedure must be used to configure the SNMP agent on the destination host.

At the System Management Console

1 Select **Network Data > Addresses** from the system tree.

The Addresses window opens in the work area.

2 Click **Add** on the Addresses window to create an address for the destination host.

The Add Addresses dialog box opens.

3 Enter a Logical Name such as OSSSrvr1Addr, and the IP address of the destination host. Click **Apply**.

4 Select **Network Data > Profiles > OSS Server** from the system tree.

The OSS Server window opens in the work area.

5 Click **Add** on the OSS Server window.

The Add OSS Server dialog box opens.

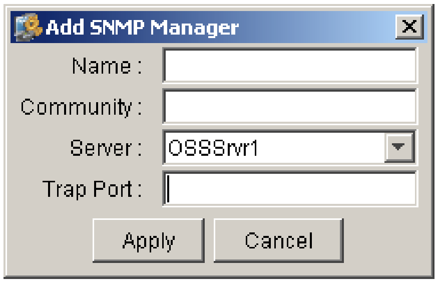
6 Enter a name for the OSS Server such as OSSSrvr1, and then use the pull down to select the Address of the destination host. Click **Apply**.

7 Select **Network Data > Profiles > SNMP Manager** from the system tree.

The SNMP Manager window opens in the work area.

8 Click **Add** on the SNMP Manager window.

The Add SNMP Manager dialog box opens.



Server : OSSSrvr1

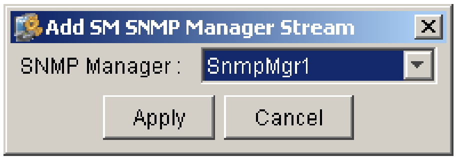
9 Enter the configuration data.

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	pull down menu	Use the pull down menu 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 yypical value is 162.

Click **Apply**.

10 Select **Network Elements > System Manager > SM > SNMP Manager** from the system tree.

The SM SNMP Manager window opens in the work area.



SNMP Manager : SnmpMgr1

11 Use the pull down menu to select the destination host and click **Apply**.

12 If the network has Fault-Performance Managers deployed, select **Network Elements > Fault-Performance Managers > FPMx > SNMP Managers** and assign the SNMP Manager.

13 This procedure is complete.

Configuring Internet Protocol Security

Perform this procedure to enable Internet Protocol Security (IPSec) communication between the System Manager and Database Manager network elements.

After performing this procedure, proceed to Configuring the initiator poking mechanism on page 72 to ensure that IPSec resumes after a power outage or other disruption of service.

Prerequisites

Meet the following prequisites before beginning this procedure:

- The System Manager and Database Manager must be deployed and running.
- The MCP IPSec utility package, ipsec.zip, must be available on each instance of the System Manager and Database Manager servers.
- root user privilege is required on the System Manager and Database Manager servers.

Limitations

This procedure must be repeated if any of the servers have their IP addresses changed.

Procedure Installing MCP IPSec utilities on page 52 must be repeated after any restoration of a back up, and after any upgrade.

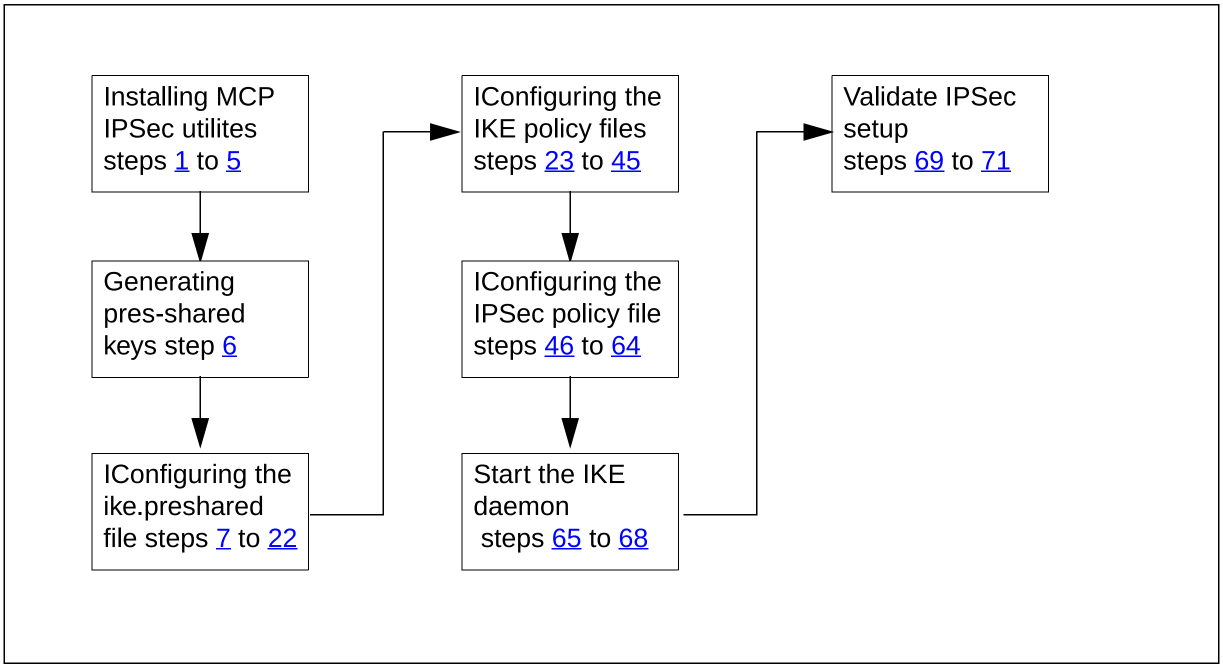
Required information

Before beginning this procedure, determine the IP addresses and valid log in information for the System Manager and Database Manager servers.

Discuss with security personnel whether to use a single pre-shared key value on the servers, or if separate pre-shared keys should be generated and configured on the server pairs. More information is provided under Generating pre-shared keys on page 53.

Action

Review the following flowchart for an overview of the process:


Installing MCP IPSec utilites steps 1 to 5
Generating pres-shared keys step 6
IConfiguring the ike.preshared file steps 7 to 22
IConfiguring the IKE policy files steps 23 to 45
IConfiguring the IPSec policy file steps 46 to 64
Start the IKE daemon steps 65 to 68
Validate IPSec setup steps 69 to 71

Installing MCP IPSec utilities

At each instance of the System Manager and Database Manager

1 Log in to the server and gain root privilege.

2 Copy the ipsec.zip file to /tmp:

```
# cp /opt/mcp/ipsec/ipsec.zip /tmp
```

3 Change directory to /tmp and unzip the utilities.

```
# cd /tmp
# unzip ipsec.zip
```

The archive is unzipped into the current directory.

```
# unzip ipsec.zip
Archive: ipsec.zip
  inflating: IPSecBR.pl
  inflating: IPSecInstall.pl
  inflating: PokeInitiator.pl
  inflating: SetupInitiatorInfo.pl
  inflating: StartPoking
  inflating: StartIKE.pl
#
```

4 Run the IPSecInstall.pl script:

```
# ./IPSecInstall.pl
```

This script installs the IPSec utilities in the filesystem.

5 Verify the utilities have be installed in the correct locations and with the correct permissions as shown:

```
# ls -l /usr/local/bin/SetupInitiatorInfo.pl
-rwxr-xr-x   1  root   other   8273  Aug 26 11:05
/usr/local/bin/SetupInitiatorInfo.pl

# ls -l /usr/local/bin/PokeInitiator.pl
-rwxr-xr-x   1  root   other   3941  Aug 26 11:05
/usr/local/bin/PokeInitiator.pl

# ls -l /usr/local/bin/IPSecBR.pl
-rwxr-xr-x   1  root   other   4082  Aug 26 11:05 /usr/local/bin/IPSecBR.pl

# ls -l /usr/local/bin/StartIKE.pl
-rwx------   1  root   other     97  Aug 26 11:05 /usr/local/bin/StartIKE.pl

# ls -l /etc/init.d/StartPoking
-rwxr-xr-x   1  root   other    172  Aug 26 11:05 /etc/init.d/StartPoking

# ls -asl /etc/rc2.d/S99zping
lrwxrwxrwx   1  root   other     23  Aug 26 11:05 /etc/rc2.d/S99zping ->
/etc/init.d/StartPoking

#
```

Generating pre-shared keys

At at terminal

6 Generate a 128 bit pre-shared key:

```
# od -X -A n /dev/random | head -1
```

Thirty two hexidecimal digits are returned. This value, without the spaces, is used as a pre-shared key.

```
3a5f47e6 64505e3a 35de52ae eb6bf0a5
```

Administrators can use a single key value on all servers, System Manager, Database Manager, and RTP Media Portals, or administrators can repaet this step to generate a unique pre-shared key for each server pair:

- System Manager to primary Database Manager
- System Manager to secondary Database Manager

  This key is not needed for simplex environments.
- RTP Media Portal to System Manager

  One key is needed for each RTP Media Portal to secure communication with the Service IP address of the System Manager. In redundant environments, this key is placed on both System Manager instances.
- RTP Media Portal to primary Database Manager

  One key is needed for each RTP Media Portal
- RTP Media Portal to secondary Database Manager

  This key is not needed for simplex environments.. In redundant environments, one of these keys is needed for each RTP Media Portal.

Configuring the ike.preshared file

After a pre-shared key for the entire MCS system or each server pair is generated, the pre-shared key must be installed on each server.

For the remiander of this procedure the following configuration data is assumed:

Sample configuration data for examples

Network element	IP address
System Manager Service IP address	47.47.47.47
Primary Database Manager	47.47.47.48
Secondary Database Manager	47.47.47.49
RTP Media Portal	47.47.47.160

Configuring the System Manager

At a terminal

7 Login to the System Manager server and gain root privilege.

8 Delete the `/etc/inet/secret/ike.preshared` file if it exists:

```
# rm /etc/inet/secret/ike.preshared
```

9 Open a text editor such as vi or emacs and create a new `/etc/inet/secret/ike.shared` file with the following data to enable IPSec between the System Manager and the Database Manager:

```
{
# SysMgr to Pri DB
    localidtype   IP
    localid       47.47.47.47
    remoteidtype  IP
    remoteid      47.47.47.48
    key 3a5f47e664505e3a35de52aeeb6bf0a5
}
```

Note: The System Manager Service IP Address is used for localid.

10 If there is a secondary Database Manager, add the following lines for IPSec between the System Manager and secondary Database Manager:

```
{
# SysMgr to Sec DB
    localidtype   IP
    localid       47.47.47.47
    remoteidtype  IP
    remoteid      47.47.47.49
    key 28891ca5ef592e96a09831283d8f74e4
}
```

Note: The System Manager Service IP Address is used for localid and the key in this example changed. This example shows separater keys for each server pair. If administrators decide to use a single key for the entire MCS system instead, then the key value would be the same as the first example.

11 Add the following lines for IPSec between the System Manager and the RTP Media Portal:

```
{
# SysMgr to RTP MP
    localidtype   IP
    localid       47.47.47.47
    remoteidtype  IP
    remoteid      47.47.47.160
    key 1abc4760b34b99a21b3ac9acfe6cf69b
}
```

> ***Note:*** This step is repeated for each RTP Media portal that needs an IPSec connection to the System Manager.

12 Save the file and quit the editor.

If there is a redundant System Manager instance, log in to that server and repeat steps 7 through 12. Enter the configuration data identically since other network elements communicate with a single Service IP address to the System Manager rather than the physical IP address of each server.

Configuring the primary Database Manager

Configure IPSec on the primary Database Manager.

At a terminal

13 Log in to the primary Database Manager and gain root privilege.

14 Delete the `/etc/inet/secret/ike.preshared` file if it exists:

```
# rm /etc/inet/secret/ike.preshared
```

15 Open a text editor such as vi or emacs and create a new `/etc/inet/secret/ike.shared` file with the following data to enable IPSec between the primary Database Manager and the System Manager:

```
{
# Pri DB to SysMgr
    localidtype   IP
    localid       47.47.47.48
    remoteidtype  IP
    remoteid      47.47.47.47
    key 3a5f47e664505e3a35de52aeeb6bf0a5
}
```

> ***Note:*** The System Manager Service IP Address is used for remote id and the key is the same value as specified in step 9.

16 Add the following lines for IPSec between the primary Database Manager and the RTP Media Portal:

```
{
# Pri DB to RTP MP
    localidtype   IP
    localid       47.47.47.48
    remoteidtype  IP
    remoteid      47.47.47.160
    key d54e464e5288767f035d5a16c4ef0143
}
```

Note: This step is repeated for each RTP Media portal that needs an IPSec connection to the System Manager.

17 Save the file and quit the editor.

Configuring the secondary Database Manager

Perform the following substeps only if there is a secondary Database Manager.

At a terminal

18 Log in to the secondary Database Manager and gain root privilege.

19 Delete the `/etc/inet/secret/ike.preshared` file if it exists:

```
# rm /etc/inet/secret/ike.preshared
```

20 Open a text editor such as vi or emacs and create a new `/etc/inet/secret/ike.shared` file with the following data to enable IPSec between the secondary Database Manager and the System Manager:

```
{
# Sec DB to SysMgr
    localidtype   IP
    localid       47.47.47.49
    remoteidtype  IP
    remoteid      47.47.47.47
    key 28891ca5ef592e96a09831283d8f74e4
}
```

Note: The System Manager Service IP Address is used for remote id and the key is the same value as specified in step 10.

21 Add the following lines for IPSec between the secondary Database Manager and the RTP Media Portal:

```
{
# Sec DB to RTP MP
    localidtype   IP
    localid       47.47.47.49
    remoteidtype  IP
    remoteid      47.47.47.160
    key 98fb044a32042b0b23c0c2df64674e5a
}
```

Note: This step is repeated for each RTP Media portal that needs an IPSec connection to the System Manager.

22 Save the file and quit the editor.

Configuring IKE policy configuration files

The /etc/inet/ike/config file on the System Manager and Database servers must be configured to contain rules for matching inbound and outgoing internet key exchange requests.

Configuring the System Manager policy file

At a terminal

23 Log in to the System Manager server and gain root access.

24 Delete the `/etc/inet/ike/config` file if it exists:

```
# rm /etc/inet/ike/config
```

25 Open a new /etc/inet/ike/config file in an editor such as vi or emacs.

26 Insert the following global parameter specifications into the file:

```
p1_lifetime_secs 60
p1_nonce_len 16
p2_nonce_len 16
```

27 Insert the following IKE rule for rule for communication between the System Manager and the primary Database Manager:

```
{
    label "SysMgr-PriDB"
    local_addr 47.47.47.47
    remote_addr 47.47.47.48
    p1_xform
      { auth_method preshared   oakley_group 1
        auth_alg sha   encr_alg 3des }
    p2_lifetime_secs 86400
}
```

Note: The value for parameter label can be any string of the administrators choice. The Service IP address of the System Manager is used for parameter local_addr. The value for parameter p2_lifetime_secs is set to 86 400 (24 hours) in this example. If this parameter is not specified, the default value of 28 800 (8 hours) is used.

28 If there is a secondary Database Manager, insert the following IKE rule for communication between the System Manager and the secondary Database Manager:

```
{
    label "SysMgr-SecDB"
    local_addr 47.47.47.47
    remote_addr 47.47.47.49
    p1_xform
      { auth_method preshared   oakley_group 1
        auth_alg sha   encr_alg 3des }
    p2_lifetime_secs 86400
}
```

Note: The Service IP address of the System Manager is used for parameter local_addr.

29 Insert the following IKE rule for communication between the System Manager and the RTP Media Portal:

```
{
    label "SysMgr-RTPMP"
    local_addr 47.47.47.47
    remote_addr 47.47.47.160
    p1_xform
      { auth_method preshared   oakley_group 1
        auth_alg sha   encr_alg 3des }
    p2_lifetime_secs 86400
}
```

Note: The Service IP address of the System Manager is used for parameter local_addr. An entry like this must be entered for each additional RTP Media Portal.

30 Save the file and quit the editor.

Validate the syntax of the config file:

```
# in.iked -c
```

Ensure the response indicates:

```
File /etc/inet/ike/config syntactically checks
out.
```

31 If there is a redundant instance of the System Manager, log in to that server and repeat steps 23 through 30.

Configuring the primary Database Manager policy

At a terminal

32 Log in to the primary Database Manager server and gain root access.

33 Delete the `/etc/inet/ike/config` file if it exists:

```
# rm /etc/inet/ike/config
```

34 Open a new /etc/inet/ike/config file in an editor such as vi or emacs.

35 Insert the following global parameter specifications into the file:

```
p1_lifetime_secs 60
p1_nonce_len 16
p2_nonce_len 16
```

36 Insert the following IKE rule for rule for communication between the primary Database Manager and the System Manager:

```
{
    label "PriDB-SysMgr"
    local_addr 47.47.47.48
    remote_addr 47.47.47.47
    p1_xform
      { auth_method preshared   oakley_group 1
        auth_alg sha   encr_alg 3des }
    p2_lifetime_secs 86400
}
```

Note: Even if the System Manager is redundant, only one entry is needed since the primary Database Manager communicates with the Service IP of the System Manager. The Service IP address of the System Manager is used for parameter remote_addr.

37 Insert the following IKE rule for communication between the primary Database Manager and the RTP Media Portal:

```
{
    label "PriDB-RTPMP"
    local_addr 47.47.47.48
    remote_addr 47.47.47.160
    p1_xform
      { auth_method preshared   oakley_group 1
        auth_alg sha   encr_alg 3des }
    p2_lifetime_secs 86400
}
```

Note: An entry like this must be entered for each additional RTP Media Portal.

38 Save the file and quit the editor.

Validate the syntax of the config file:

```
# in.iked -c
```

Ensure the response indicates:

```
File /etc/inet/ike/config syntactically checks
out.
```

Configuring the secondary Database Manager policy

Only perform this procedure if a secondary Database Manager is deployed.

At a terminal

39 Log in to the secondary Database Manager server and gain root access.

40 Delete the `/etc/inet/ike/config` file if it exists:

```
 # rm /etc/inet/ike/config
```

41 Open a new /etc/inet/ike/config file in an editor such as vi or emacs.

42 Insert the following global parameter specifications into the file:

```
p1_lifetime_secs 60
p1_nonce_len 16
p2_nonce_len 16
```

43 Insert the following IKE rule for rule for communication between the secondary Database Manager and the System Manager:

```
{
    label "SecDB-SysMgr"
    local_addr 47.47.47.49
    remote_addr 47.47.47.47
    p1_xform
      { auth_method preshared   oakley_group 1
        auth_alg sha   encr_alg 3des }
    p2_lifetime_secs 86400
}
```

Note: The Service IP address of the System Manager is used for parameter remote_addr.

44 Insert the following IKE rule for communication between the secondary Database Manager and the RTP Media Portal:

```
{
    label "SecDB-RTPMP"
    local_addr 47.47.47.49
    remote_addr 47.47.47.160
    p1_xform
      { auth_method preshared   oakley_group 1
        auth_alg sha   encr_alg 3des }
    p2_lifetime_secs 86400
}
```

Note: An entry like this must be entered for each additional RTP Media Portal.

45 Save the file and quit the editor.

Validate the syntax of the config file:

```
# in.iked -c
```

Ensure the response indicates:

```
File /etc/inet/ike/config syntactically checks
out.
```

Configuring IPSec policy configuration files

The /etc/inet/ipsecinit.conf files must be configured to secure internet traffice between hosts.

Configuring the System Manager ipsecinit.conf file

At a terminal

46 Log in to the System Manager server and gain root access.

47 Delete the `/etc/inet/ipsecinit.conf` file if it exists:

```
# rm /etc/inet/ipsecinit.conf
```

48 Open a new /etc/inet/ipsecinit.conf file in an editor such as vi or emacs.

49 Insert the following IPSec policy for communication between the System Manager and the primary Database Manager:

```
{laddr 47.47.47.47 raddr 47.47.47.48} ipsec
{auth_algs sha  encr_algs 3des sa shared}
```

Note: The Service IP address of the System Manager is used for parameter laddr.

50 If there is a secondary Database Manager, insert the following IPSec policy for communication between the System Manager and the secondary Database Manager:

```
{laddr 47.47.47.47 raddr 47.47.47.49} ipsec
{auth_algs sha  encr_alg 3des sa shared}
```

> ***Note:*** The Service IP address of the System Manager is used for parameter laddr.

51 Insert the following IPSec policy for communication between the System Manager and the RTP Media Portal:

```
{laddr 47.47.47.47 raddr 47.47.47.160} ipsec
{encr_algs null  encr_auth_algs sha sa shared}
```

> ***Note:*** The Service IP address of the System Manager is used for parameter laddr and that null encryption is used in phase two security associations between the RTP Media Portal and other network elements. An entry like this must be entered for each additional RTP Media Portal.

52 Save the file and quit the editor.

If there is a redundant instance of the System Manager, log in to that server and repeat steps 46 through 52.

Configuring the primary Database Manager IPSec policy file

At a terminal

53 Log in to the primary Database Manager server and gain root access.

54 Delete the `/etc/inet/ipsecinit.conf` file if it exists:

```
# rm /etc/inet/ipsecinit.conf
```

55 Open a new /etc/inet/ipsecinit.conf file in an editor such as vi or emacs.

56 Insert the following IPSec policy for communication between the primary Database Manager and the System Manager:

```
{laddr 47.47.47.48 raddr 47.47.47.47} ipsec
{auth_algs sha  encr_algs 3des sa shared}
```

> ***Note:*** The Service IP address of the System Manager is used for parameter raddr.

57 Insert the following IPSec policy for communication between the primary Database Manager and the RTP Media Portal:

```
{laddr 47.47.47.48 raddr 47.47.47.160} ipsec
{encr_algs null  encr_auth_algs sha sa shared}
```

Note: Null encryption is used in phase two security associations between the RTP Media Portal and other network elements. An entry like this must be entered for each additional RTP Media Portal.

58 Save the file and quit the editor.

Configuring the primary Database Manager IPSec policy file

Perform the following steps if a redundant Database Manager is deployed.

At a terminal

59 Log in to the secondary Database Manager server and gain root access.

60 Delete the `/etc/inet/ipsecinit.conf` file if it exists:

```
# rm /etc/inet/ipsecinit.conf
```

61 Open a new /etc/inet/ipsecinit.conf file in an editor such as vi or emacs.

62 Insert the following IPSec policy for communication between the secondary Database Manager and the System Manager:

```
{laddr 47.47.47.49 raddr 47.47.47.47} ipsec
{auth_algs sha  encr_algs 3des sa shared}
```

Note: The Service IP address of the System Manager is used for parameter raddr.

63 Insert the following IPSec policy for communication between the secondary Database Manager and the RTP Media Portal:

```
{laddr 47.47.47.49 raddr 47.47.47.160} ipsec
{encr_algs null  encr_auth_algs sha sa shared}
```

Note: Null encryption is used in phase two security associations between the RTP Media Portal and other network elements. An entry like this must be entered for each additional RTP Media Portal.

64 Save the file and quit the editor.

Start the IKE daemon

Perform the following steps on each server that was configured to activate the IPSec setup. This procedure is only performed after configuration. The IKE daemon is started automatically at boot up after installation.

At a terminal

65 Log in to one of the servers and gain root access.

66 Change directory:

```
# cd /usr/local/bin
./StartIKE.pl
```

Verify that the script attempts to start the daemon:

```
Complete IKE daemon startup.
```

67 Verify that the IKE daemon is running with the **ps** command:

```
# ps -ef | grep iked
```

Ensure that a line with in.iked is returned:

```
# ps -ef | grep iked
    root  320  96  0  09:17:19   pts/1  0:00   grep iked
    root   432  96  0  09:17:05   pts/1  0:00   /usr/lib/net/in.iked
#
```

***Note:** If the in.iked line is not returned, then something is misconfigured in one of the configuration files.*

68 List the /admin/ipsec directory to verify that the StartIKE.pl script backed up the configuration files:

```
# ls -l /admin/ipsec
```

Ensure that the date field indicates the current date or the time of the last reboot:

```
# ls -l /admin/ipsec
-rw-------    1  root   other    614   Aug 26  14:21  config
-rw-------    1  root   other    563   Aug 26  14:21  ike.preshared
-rw-------    1  root   other    180   Aug 26  14:21  ipsecinit.conf
```

Validate IPSec setup

One method of validating IPSec communication is to log in to two of the servers and snoop for Encapsulating Security Payload (ESP) traffic.

At a terminal on one server

69 Gain root access and start the **snoop** command with a filter of ESP:

```
# snoop | grep ESP
```

The command indicates that it is using device /dev/qfe in promiscuous mode.

At a terminal on the second server

70 Ping the first host to generate traffic:

```
$ ping <srvr_one_addr>
```

The response indicates that the remote host is alive.

At the terminal for the first server

71 Verify that the snoop command generates output similar to the following:

```
# snoop | grep ESP
Using device /dev/qfe (promiscuous mode)
47.47.47.49 -> <hostname>       ESP SPI=0xf76a8a63 Replay=268
  <hostname> -> 47.47.47.49     ESP SPI=0x31eeb426 Replay=162
```

> ***Note:*** Validation will fail to and from the RTP Media Portal until IPSec has been configured for the RTP Media Portal by running the **MPIPSec.pl** script on the RTP Media Portal.

Proceed to Configuring the initiator poking mechanism on page 72 to ensure that IPSec resumes after a power outage or disruption of service.

Sample configuration files

The following figures show sample configuration files with the configuration data from the previous procedures.

Sample ike.preshared file for System Manager

```
#
#ident  "@(#)ike.preshared      1.1     01/09/28 SMI"
#
# Copyright (c) 2001 by Sun Microsystems, Inc.
# All rights reserved.
#

# ike.preshared - Pre-shared secrets for IKE authentication.
#
# Entries are of the form:
#
# {
#       <attribute> <value>
#       ...
# }
#
# Consult the man page for ike.preshared(4) for details.

{
# SysMgr to Pri DB
    localidtype   IP
    localid       47.47.47.47
    remoteidtype  IP
    remoteid      47.47.47.48
    key 3a5f47e664505e3a35de52aeeb6bf0a5
}
```

This section is created during step 9.

```
{
# SysMgr to Sec DB
    localidtype   IP
    localid       47.47.47.47
    remoteidtype  IP
    remoteid      47.47.47.49
    key 28891ca5ef592e96a09831283d8f74e4
}
```

This section is created during step 10.

```
{
# SysMgr to RTP MP
    localidtype   IP
    localid       47.47.47.47
    remoteidtype  IP
    remoteid      47.47.47.160
    key 1abc4760b34b99a21b3ac9acfe6cf69b
}
```

This section is created during step 11.

Note: This file is duplicated, with the same values on a second System Manager server, if the System Manager is redundant.

Sample ike.preshared file for primary Database Manager

```
#
#ident  "@(#)ike.preshared      1.1     01/09/28 SMI"
#
# Copyright (c) 2001 by Sun Microsystems, Inc.
# All rights reserved.
#

# ike.preshared - Pre-shared secrets for IKE authentication.
#
# Entries are of the form:
#
# {
#       <attribute> <value>
#       ...
# }
#
# Consult the man page for ike.preshared(4) for details.

{
# Pri DB to SysMgr
    localidtype   IP
    localid       47.47.47.48
    remoteidtype  IP
    remoteid      47.47.47.47
    key 3a5f47e664505e3a35de52aeeb6bf0a5
}
```

This section is created during step 15.

```
{
# Pri DB to RTP MP
    localidtype   IP
    localid       47.47.47.48
    remoteidtype  IP
    remoteid      47.47.47.160
    key d54e464e5288767f035d5a16c4ef0143
}
```

This section is created during step 16.

Note: An example for the secondary Database Manager is not provided but the configuration data is the same except parameter `localid` is the IP address of the secondary Database Manager.

Sample IKE Policy configuration file for System Manager

```
### ike/config file 47.47.47.47

## Global parameters
p1_lifetime_secs 60
p1_nonce_len 16
p2_nonce_len 16

## The rule to communicate with  47.47.47.48
{
    label "SysMgr-PriDB"
    local_addr 47.47.47.47
    remote_addr 47.47.47.48
    p1_xform
      { auth_method preshared  oakley_group 1
        auth_alg sha encr_alg 3des }
    p2_lifetime_secs 86400
}
```

This section is created during step 27.

```
## The rule to communicate with 47.47.47.49
{
    label "SysMgr-SecDB"
    local_addr 47.47.47.47
    remote_addr 47.47.47.49
    p1_xform
      { auth_method preshared  oakley_group 1
        auth_alg sha   encr_alg 3des }
    p2_lifetime_secs 86400
}
```

This section is created during step 28.

```
## The rule to communicate with 47.47.47.160
{
    label "SysMgr-RTPMP"
    local_addr 47.47.47.47
    remote_addr 47.47.47.160
    p1_xform
      { auth_method preshared  oakley_group 1
        auth_alg sha   encr_alg 3des }
    p2_lifetime_secs 86400
}
```

This section is created during step 29.

Sample IKE Policy configuration file for primary Database Manager

```
### ike/config file 47.47.47.48

## Global parameters
p1_lifetime_secs 60
p1_nonce_len 16
p2_nonce_len 16

## The rule to communicate with  47.47.47.47
{
    label "PriDB-SysMgr"
    local_addr 47.47.47.48
    remote_addr 47.47.47.47
    p1_xform
      { auth_method preshared   oakley_group 1
       auth_alg sha   encr_alg 3des }
    p2_lifetime_secs 86400
}
```

This section is created during step 36.

```
## The rule to communicate with 47.47.47.160
{
    label "PriDB-RTPMP"
    local_addr 47.47.47.48
    remote_addr 47.47.47.160
    p1_xform
      { auth_method preshared   oakley_group 1
       auth_alg sha   encr_alg 3des }
    p2_lifetime_secs 86400
}
```

This section is created during step 37.

Note: An example for the secondary Database Manager is not provided but the configuration data is the same except parameter `local_addr` is the IP address of the secondary Database Manager.

Sample ipsecinit.conf configuration file for the System Manager

```
### /etc/inet/ipsecinit.conf file 47.47.47.47

{laddr 47.47.47.47 raddr 47.47.47.48} ipsec
{auth_algs sha  encr_algs 3des sa shared}
```

This section is created during step 49.

```
{laddr 47.47.47.47 raddr 47.47.47.49} ipsec
{auth_algs sha  encr_alg 3des sa shared}
```

This section is created during step 50.

```
{laddr 47.47.47.47 raddr 47.47.47.160} ipsec
{encr_algs null  encr_auth_algs sha sa shared}
```

This section is created during step 51.

Sample ipsecinit.conf configuration file for the primary Database Manager

```
### /etc/inet/ipsecinit.conf file 47.47.47.48

{laddr 47.47.47.48 raddr 47.47.47.47} ipsec
{auth_algs sha  encr_algs 3des sa shared}
```

This section is created during step 56.

```
{laddr 47.47.47.48 raddr 47.47.47.160} ipsec
{encr_algs null  encr_auth_algs sha sa shared}
```

This section is created during step 57.

Note: An example for the secondary Database Manager is not provided but the configuration data is the same except parameter `laddr` is the IP address of the secondary Database Manager.

Configuring the initiator poking mechanism

This procedure configures the an initiator poking mechanism on servers that have IPSec already configured. Performing this procedure ensures that the servers resume IPSec communication after an extreme condition such as a power outage.

Prerequisites

Complete procedure Configuring Internet Protocol Security on page 51 and also configure IPsec on the RTP Media Portal with the **/usr/loca/bin/MPIPSec** script.

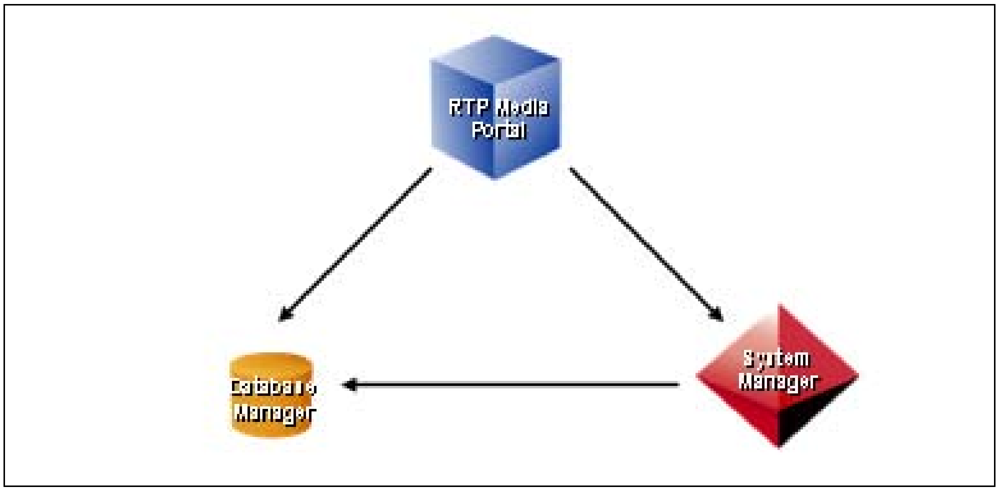
Limitations

This procedure must be repeated if the IP addresses of any of the servers are changed.

Initiator and responder concept

Amongst the RTP Media Portal, Database Manager, and System Manager, there are relationships of initiating communication and responding to communication. The following figure shows the path of communication initiation: the RTP Media Portal initiates communication with the Database Manager and the System Manager; the System Manager initiates communication with the Database Manager.

Path of initiating communication



As indicated in the figure, the System Manager must be configured with the RTP Media Portal as an initiator and the Database Manager must be configured with the RTP Media Portal and the System Manager as initiators.

Action

At a terminal

1 Log in to the server and gain root privilege.

2 Change directory to /usr/local/bin and execute the **SetupInitiatorInfo.pl** script.

```
# cd /usr/local/bin
# ./SetupInitiatorInfo.pl
```

A menu is printed to the screen and a prompt is presented.

```
# cd /usr/local/bin
# ./SetupInitiatorInfo.pl

  Select an operation:

    [1]  List all existing initiator IP addresses
    [2]  Add a new initiator IP address
    [3]  Delete an existing initiator IP address
    [4]  Done

  Your choice (1 - 4): 2
```

3 Enter 2 at the prompt to enter an initiator IP address. Repeat this step for each initiator IP address to add.

Follow the configuration data in the following table depending upon which responder host you are logged into.

Responder host logged into	Initiator IP addresses to add
primary System Manager server	RTP Media Portal
secondary System Manager server (if present)	RTP Media Portal
primary Database Manager	RTP Media Portal and System Manager Service IP address
secondary Database Manager (if present)	RTP Media Portal and System Manager Service IP address

4 This procedure is complete.

Accounting management

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

Performance management

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. Each server is monitored for CPU, memory, disk, and network interface usage. Operational measurements for the System Manager processes, consisting of counters and gauges, are viewed in the OM browsers of the System Management Console.

For information on using the System Management Console, refer to the *CVoIP System Management Console User Guide*.

Topics in this chapter

Local storage of operational measurements

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_4.0/SM_0/*
  ```

- Fault-Performance Manager

  ```
  /var/mcp/oss/om/MCP_4.0/<fpm_name>_0/*
  ```

> ***Note:*** The name of the Fault-Performance Manager 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.

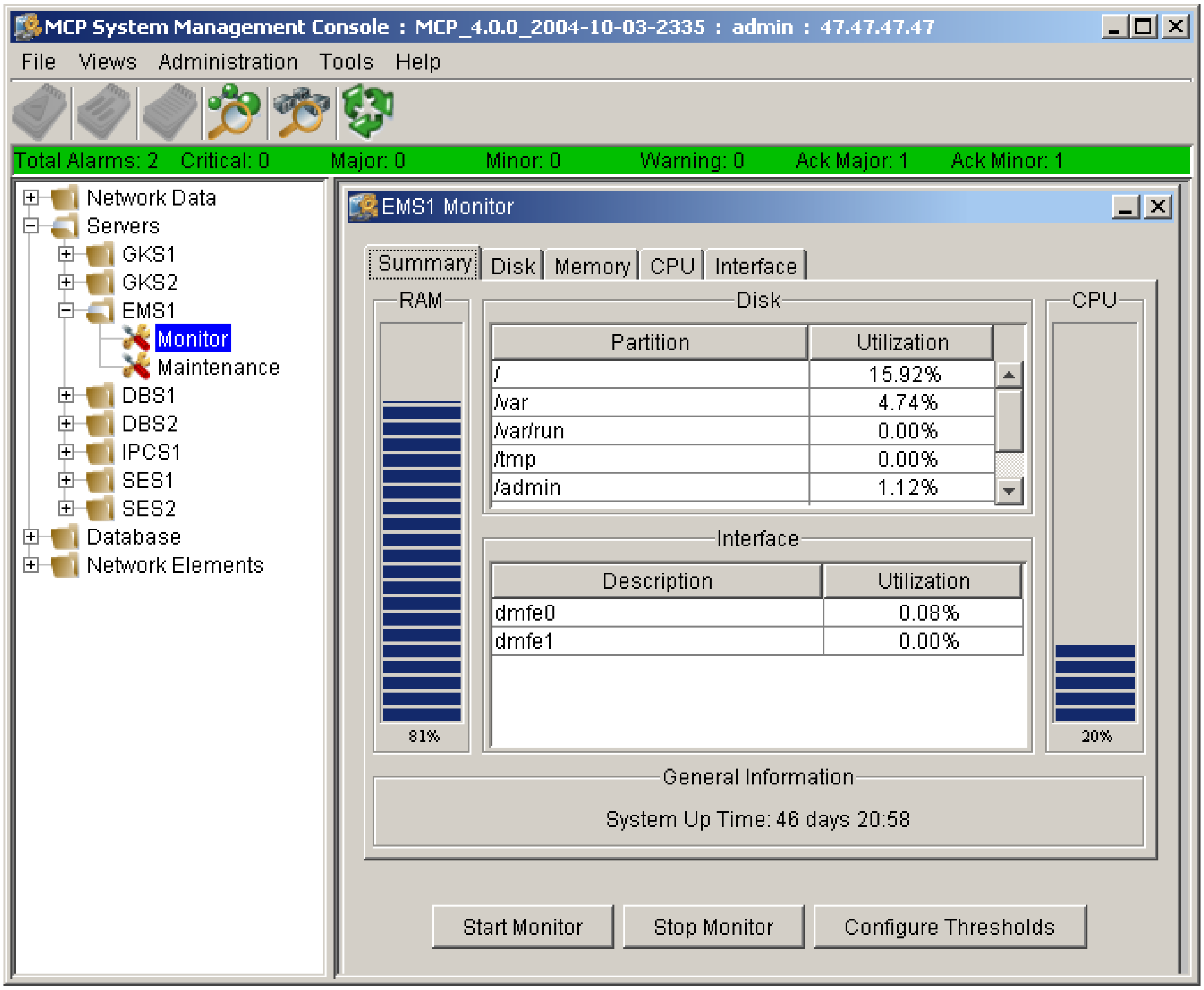
Below these directories, a directory is created for each network element instance that reports data to the System Manager or FPM.

Monitoring servers

Use this procedure to view the performance of the System Manager servers that host the System Manager.

At the System Management Console

1 Select **Servers** > **EMSx** > **Monitor** from the config view:



Total Alarms: 2 Critical: 0 Major: 0 Minor: 0 Warning: 0 Ack Major: 1 Ack Minor: 1

Disk

Partition	Utilization
/	15.92%
/var	4.74%
/var/run	0.00%
/tmp	0.00%
/admin	1.12%

Interface

Description	Utilization
dmfe0	0.08%
dmfe1	0.00%

General Information

System Up Time: 46 days 20:58

The Monitor window opens the work area and displays statistics for CPU, Memory, Disk, and Interface usage.

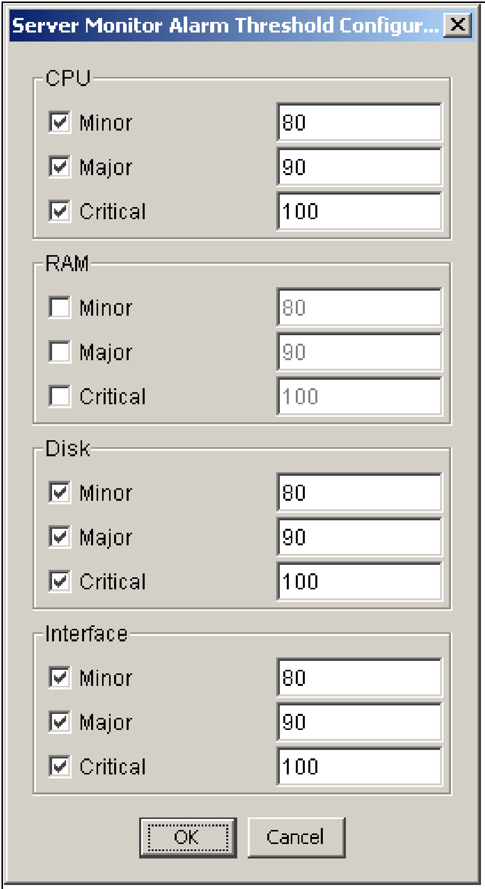
2 If the Monitor window does not display data and the status bar at the bottom of the Monitor window indicates `The server monitor is not running`, click the Start Monitor button.

3 This procedure is complete.

Additional information

While the server monitor is running, server operational measurements are recorded to disk on the active instance of the System Manager. These operational measurements are not viewable from the System Management Console. To view these operational measurements, use the System Management Console to provision an FTP Push job to an OSS server, and then assign an FTP Push OM Stream to use the FTP Push job.

Thresholds for CPU, memory, disk, and interface usage are set from the Monitor window by clicking the Configure Thresholds button.



Server Monitor Alarm Threshold Configur...

CPU
☑ Minor 80
☑ Major 90
☑ Critical 100

RAM
□ Minor 80
□ Major 90
□ Critical 100

Disk
☑ Minor 80
☑ Major 90
☑ Critical 100

Interface
☑ Minor 80
☑ Major 90
☑ Critical 100

Enter new values to set different thresholds.

To remove alarming for threshold crossing, deselect the checkbox next to each item. In this example, no SRVR402 alarms or log will be generated since the checkboxes for RAM are deselected.

SRVR401 - CPU
SRVR402 - RAM
SRVR403 - Disk
SRVR404 - Interface

Altering thresholds requires an administrative role with WRITE privilege for ServerMonitorConfigService.

Viewing operational measurements

Operational measurements consist of counters and gauges monitoring the activity of the System Manager processes

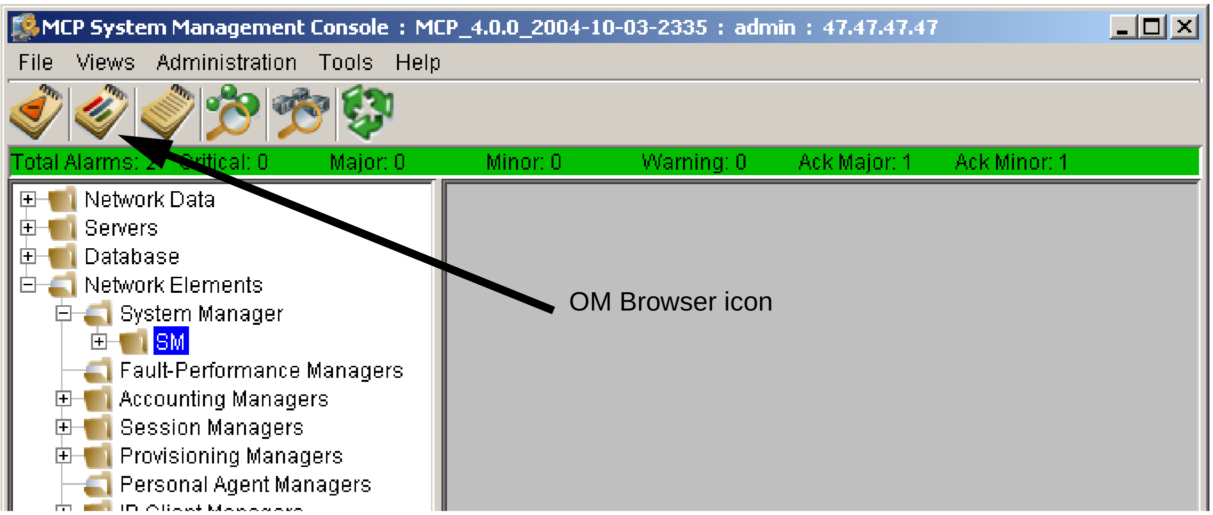
Operational measurements are tallied in memory and recorded in an active file stored in the `/var/mcp/spool` directory on the network element that is generating the OMs. After the interval provisioned in the OfficeTransferPeriod configuration parameter expires, the data is flushed to the active file, the file is closed, and then transferred to the System Manager. The System Manager records 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.

Operational measurements generated by the System Manager are viewed using System Management Console OM Browser. By default, the active operational measurements are displayed. These operational measurements have not been recorded to disk, and represent the events that occurred since the last OfficeTransferPeriod interval expired. The most recent holding operational measurements can be displayed by selecting Holding from the Type pull down menu. These operational measurements were stored to disk when the last OfficeTransferPeriod interval expired. To view older operational measurements, set an FTP Push job to an OSS machine and view the historic information there.

The OM file retention period is configured at a system level. The procedure for configuring the retention period is documented in the *CVoIP System Management Console User Guide*.

At the System Management Console

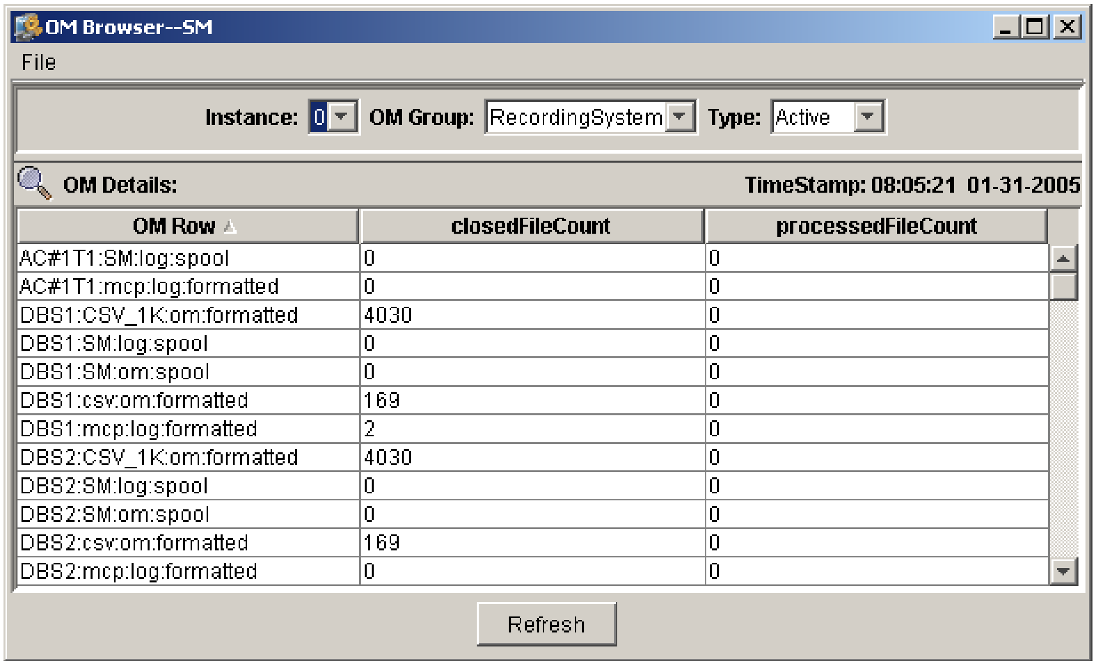
1 Select **Network Elements** > **System Manager** > **SM** to make the OM Browser button active:



OM Browser icon

2 Click the OM Browser icon from the icon toolbar.

The OM Browser window opens. The OM Browser shows OMs for the active System Manager instance.



Instance: 0 OM Group: RecordingSystem Type: Active

OM Details: TimeStamp: 08:05:21 01-31-2005

OM Row	closedFileCount	processedFileCount
AC#1T1:SM:log:spool	0	0
AC#1T1:mcp:log:formatted	0	0
DBS1:CSV_1K:om:formatted	4030	0
DBS1:SM:log:spool	0	0
DBS1:SM:om:spool	0	0
DBS1:csv:om:formatted	169	0
DBS1:mcp:log:formatted	2	0
DBS2:CSV_1K:om:formatted	4030	0
DBS2:SM:log:spool	0	0
DBS2:SM:om:spool	0	0
DBS2:csv:om:formatted	169	0
DBS2:mcp:log:formatted	0	0

3 This procedure is complete.

Security and administration

Topics in this chapter

Security

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

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

To prevent non-trusted employees from logging into the servers, it is recommended that both the password and server's IP address remain confidential. After initial provisioning, an administrative role without IPAddressService privileges can be created, and administrators with maintenance responsibilities can be assigned this role. Administrators with this role cannot view IP addresses, or add servers to the network, or perform much configuration. This role would be appropriate for an alarm and log monitoring only administrative account.

SNMP community string values for a server can be changed from the default 'public' to some other value for network security reasons. Once configured for a server, it applies this community string value to SNMP message traffic of the hosted components. Information on configuring an SNMP Profile to use the new the community string is documented in the *CVoIP System Management Console User Guide*.

Administration

The System Manager utilizes software loads to determine the versions of software that are available for use. Software loads are added onto the server hosting the System Manager via 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 loadlist 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. The procedure for removing a software load is described in the procedure Removing software loads on page 85.

Server backups

Backups of MCS servers allow recovery from a catastrophic hardware failure where a complete restore of the server's software (both third party and MCS software) is required. Backups of the System Manager hosting servers are recommended after third party software updates, such as an applied operating system patch, and after maintenance release updates.

Refer to the *MCS Backup and Recovery Guide* for details regarding backup procedures for MCS servers.

Removing software loads

ATTENTION
Contact your next level of support if you need to perform this task and do not have the required server access.

Before performing this procedure, use the System Management Console to review the software loads used by all instances of all network elements to ensure that the load to be removed isn’t used by a network element.

In a network with redundant instances of the System Manager, the software pools are present on both servers hosting the System Manager. Perform the software removal on both servers to fully remove the older versions.

At a workstation

1 Log on to the server hosting the System Manager.

2 Change directory to the location of the software loads and list them:

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

The list of available software loads is printed.

```
[@hostname]/var/mcp/loads:=> ls
MCP_4.0.0_2004-10-10-2335      MCP_4.0.0_2004-10-17-2335.zip
MCP_4.0.0_2004-10-10-2335.zip  MCP_4.0.0_2004-10-24-2335
MCP_4.0.0_2004-10-17-2335      MCP_4.0.0_2004-10-24-2335.zip
[@hostname]/var/mcp/loads:=>
```

3 From the list, determine the loads that are not in use and can be safely removed.

4

CAUTION
Possible service interruption
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.

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

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

Note: 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_4.0.0_2004-10-10-2335 software load, the commands are as follows:

/bin/rm -rf MCP_4.0.0_2004-10-10-2335
/bin/rm MCP_4.0.0_2004-10-10-2335.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.

5 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.

6 This procedure is complete.

Setting the System Management Console message of the day

Administrators can configure a message of the day file on the System Manager. The contents of this file are displayed at the System Management Console interface after a successful log in. If this procedure is not followed, then no message of the day window is displayed.

Limitiations

The message of the day file is not persisted 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 or create a second version of the file on the second System Manager instance.

Action

At a workstation

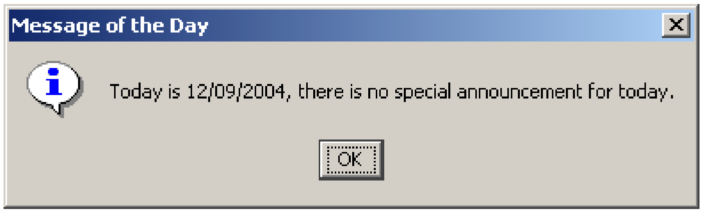
1 Log in to the System Manager server as the nortel user.

2 Change directory:

```
$ cd /var/mcp/run/MCP_4.0/SM_x/data
```

3 Create a file named **motd.txt** with an editor such as vi.

4 Enter the message to display in the motd.txt file. For example, entering "**Today is 12/09/2004. There is no special announcement for today.**" will result in the following Message of the Day window:



Message of the Day

Today is 12/09/2004, there is no special announcement for today.

5 Save the motd.txt file.

At the next successful log in from the System Management Console, the message is displayed.

6 This procedure is complete.

Carrier Voice over IP

Communication Server 2000

System Manager Basics

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 System Manager 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.

Publication number: NN10369-111
Product release: (I)SN08
Document version: Preliminary 03.01
Date: March 2005