



Maintaining an Efficient Network

This chapter contains the following information to help you maintain an efficient network:

- [5.1 How Do I Manage the Database?](#)
- [5.2 How Do I Monitor the Network?](#)
- [5.3 How Do I Modify the Network?](#)
- [5.4 How Do I Manage the Network Software?](#)
- [5.5 How Do I Manage Redundancy and Failover?](#)
- [5.6 Which Ports Are Reserved in Cisco MGM?](#)
- [5.7 How Do I Export Information in Tables?](#)



Note

For information on configuring users and user-related parameters, creating and modifying advisory messages, and accessing various logs, please refer to [Chapter 8, “Managing Security”](#).

Maintaining your network focuses on tasks that will keep your network running smoothly, for example:

- Backing up and restoring memory and/or the database
- Restoring default settings when necessary
- Monitoring tasks and jobs
- Modifying basic server and NE information
- Finding modules or boards
- Updating software images and versions
- Exporting data and generating reports
- Performing administrative database operations

5.1 How Do I Manage the Database?

This section describes procedures for managing the Oracle database and deals specifically with Cisco MGM data stored in the database. For a complete description, refer to the Oracle documentation—specifically the *Oracle9i Server Administrator's Guide*.

A useful tool for managing the database is the Oracle Enterprise Manager, part of the Oracle9i Client CD. The Oracle Enterprise Manager provides an integrated solution for managing heterogeneous environment and combines a graphical console, agents, common services, and tools to provide a comprehensive systems-management platform for managing Oracle products.

This section contains the following information:

- [5.1.1 Viewing and Modifying Database Properties](#)
- [5.1.2 Importing and Exporting Data to and from the Oracle Database](#)
- [5.1.3 Backing Up and Restoring the Database](#)
- [5.1.4 Pruning the Database](#)
- [5.1.5 Using the SQL*PLUS Client to Manage the Database](#)
- [5.1.6 Basic SQL Commands for Cisco MGM Schema Objects](#)
- [5.1.7 Enhancing Database Performance](#)
- [5.1.8 Removing an Old Version of the Cisco MGM Database](#)

5.1.1 Viewing and Modifying Database Properties

The Database Properties pane shows and defines database pruning parameters and configuration that the Cisco MGM server uses to connect to the Oracle database. It contains the following tabs:

- **Configuration Tab**—The Configuration tab fields define the values used by the Cisco MGM server to log into the Oracle database. Fields are grouped into two columns: Active and After Restart. The Active column displays the values used by the Cisco MGM server. The After Restart column shows the values that the Cisco MGM server uses after the server is restarted.



Note [Table 5-1](#) describes the fields within the Database Properties Configuration tab.

- **Pruning Tab**—The Pruning tab defines the Cisco MGM database pruning frequency. Pruning frequency changes take effect as soon as you save them. You do not need to reboot the Cisco MGM server.



Note [Table 5-2](#) describes the fields within the Database Properties Pruning tab.

- **Database Backup Tab**—The Database Backup tab allows you to start a database backup from the Control Panel. After entering the password, click **Start** to begin the database backup. This tab is disabled if the database is not installed in ARCHIVELOG mode. The ARCHIVELOG mode is stored in the MGM_config_table by the server installer.



Note [Table 5-3](#) describes the fields within the Database Properties Database Backup tab.

To view and modify the database properties:

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
 - Step 2** Click **Database Properties** to open the Database Properties pane. See [Figure 5-1](#).

Step 3 (Optional) Click the **Configuration** tab. [Table 5-1](#) describes the fields within the Database Properties Configuration tab.

Step 4 (Optional) Click the **Pruning** tab. [Table 5-2](#) describes the fields within the Database Properties Pruning tab.



Note For more details, see section [5.1.4 Pruning the Database, page 5-13](#).

Step 5 (Optional) Click the **Database Backup** tab. [Table 5-3](#) describes the fields within the Database Properties Database Backup tab.



Note For more information on database backups, see section [5.1.3 Backing Up and Restoring the Database, page 5-7](#).



Note Fields in the Database Backup tab are disabled if the database is not installed with the ARCHIVELOG mode option equal to true (see the Configuration tab for details).

Step 6 Click **Save**.

Figure 5-1 Control Panel—Database Properties Pane

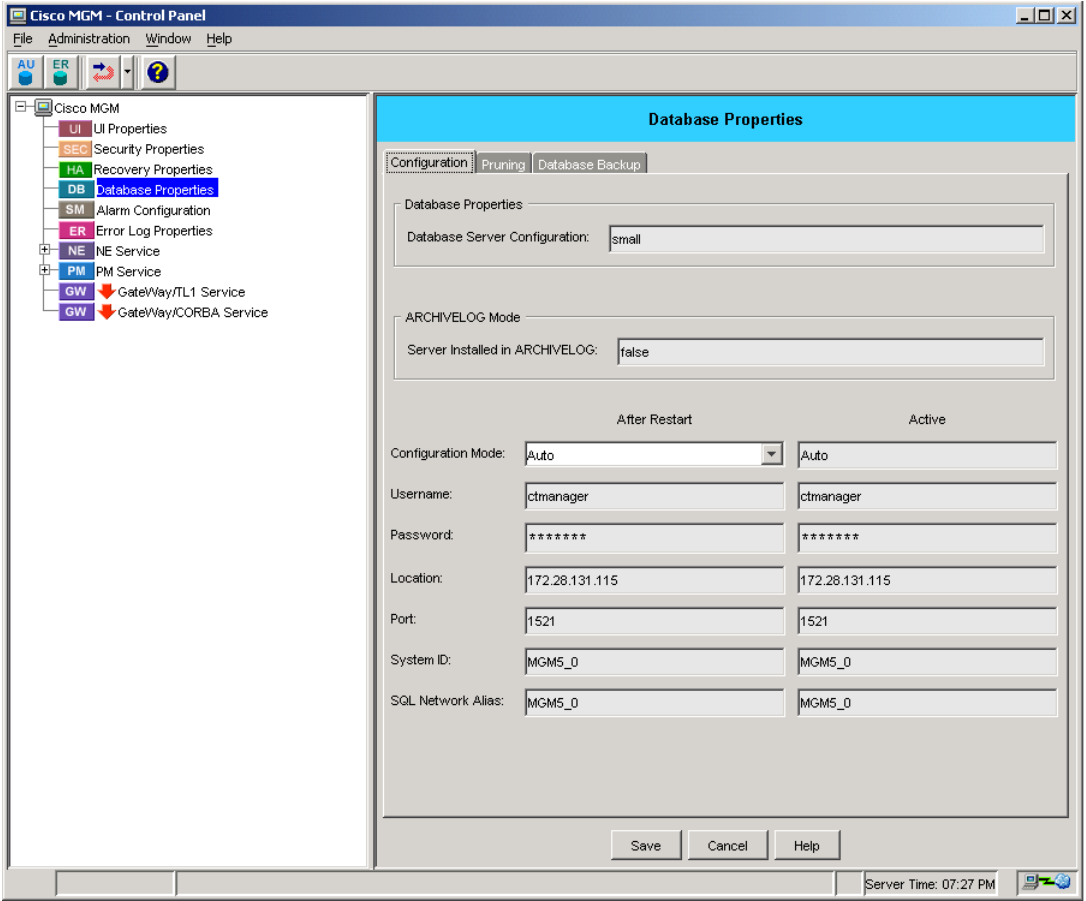


Table 5-1 Field Descriptions for the Database Properties—Configuration Tab

Field	Description
Database Server Configuration	Displays the size of the database server.
Server Installed in ARCHIVELOG	If set to True, Cisco MGM supports automatic pruning of the /db05 partition when the database is in ARCHIVELOG mode.

Table 5-1 Field Descriptions for the Database Properties—Configuration Tab (continued)


Field	Description
Configuration Mode	<p>Configuration Mode tells the Cisco MGM server the values to use to log into the Oracle database. When set to Auto, the Cisco MGM server uses the configuration that was set when Cisco MGM was installed. When set to Manual, the After Restart fields can be edited, and the Cisco MGM server will use the edited values when the server is rebooted.</p> <p>Note If you change the configuration mode to Manual, enter the following commands to set the ORACLE_HOME and ORACLE_SID environment variables before logging into Cisco MGM again:</p> <pre>setenv ORACLE_HOME Oracle home directory setenv ORACLE_SID MGM5_0 setenv LD_LIBRARY_PATH \$ORACLE_HOME/lib setenv PATH \$PATH:\$ORACLE_HOME/bin</pre> <p>Restart the Cisco MGM server after setting these environment variables.</p> <p> Caution If you set the configuration mode to Auto and restart the Cisco MGM server, the MGMServer.cfg file is overwritten with the default values for username, password, location, port, system ID, and SQL network alias.</p>
Username	Displays the username that the Cisco MGM server uses to access the Oracle database.
Password	Displays the password that gives the username access to the Oracle database.
Location	Displays the IP address that the Cisco MGM server uses to connect to the database.
Port	Displays the port number that is used to connect to the database.
System ID	<p>Displays the Oracle system ID. The ORACLE_SID specifies the system identifier (SID) value of the database instance that you create with the Cisco MGM installer. For a single-instance database, the SID value should be the same as the name of the database it manipulates (initialization parameter DB_NAME), and no more than four characters.</p> <p>Note During Cisco MGM installation, the default system ID is MGM5_0.</p>
SQL Network Alias	<p>Displays the SQL*Net listener alias set in the system listener.ora file. When the listener is running, entering the ps command displays the following output (not all systems display <i>listener_alias</i>):</p> <pre>tnslsnr [listener_alias] [-inherit]</pre> <p>Shadow processes (dedicated servers) spawned by the SQL*Net listener have the following syntax:</p> <pre>oracleSID [(LOCAL=NO)]</pre>

Table 5-2 *Field Description for the Database Properties—Pruning Tab*

Field	Description
PM Data	Specifies the number of days to save performance monitoring (PM) data before Cisco MGM runs the database pruning script. The default value is 7. You can also specify the time of day when the PM data will be saved by choosing the hour and minute from the HH, MM, and AM/PM fields. Minutes are listed in 5-minute intervals. Click Enable to activate the PM data pruning.
FM Data	Specifies the number of days to save FM data before Cisco MGM runs the database pruning script. The default value is 7. You can also specify the time of day when the FM data will be saved by choosing the hour and minute from the HH, MM, and AM/PM fields. Minutes are listed in 5-minute intervals. Click Enable to activate the FM data pruning.
Audit Log Data	Specifies the number of days to save audit log data before Cisco MGM runs the database pruning script. The default value is 7. You can also specify the time of day when the audit log data will be saved by choosing the hour and minute from the HH, MM, and AM/PM fields. Minutes are listed in 5-minute intervals. Click Enable to activate the audit log data pruning.
Error Log Data	Specifies the number of days to save Error Log data before Cisco MGM runs the database pruning script. The default value is 7. You can also specify the time of day when the Error Log data will be saved by choosing the hour and minute from the HH, MM, and AM/PM fields. Minutes are listed in 5-minute intervals. Click Enable to activate the Error Log data pruning.
Audit Trail Data	Specifies the number of days to save audit trail data before Cisco MGM runs the database pruning script. The default value is 7. You can also specify the time of day when the audit trail data will be saved by choosing the hour and minute from the HH, MM, and AM/PM fields. Minutes are listed in 5-minute intervals. Click Enable to activate the audit trail data pruning.
Self Monitor Data	Specifies the number of days to save self-monitoring data before Cisco MGM runs the database pruning script. The default value is 7. You can also specify the time of day when the self monitoring data will be saved by choosing the hour and minute from the HH, MM, and AM/PM fields. Minutes are listed in 5-minute intervals. Click Enable to activate the self monitoring data pruning.
Job Monitor Data	Specifies the number of days to save job monitoring data before Cisco MGM runs the database pruning script. The default value is 7. You can also specify the time of day when the job monitoring data will be saved by choosing the hour and minute from the HH, MM, and AM/PM fields. Minutes are listed in 5-minute intervals. Click Enable to activate the job monitoring data pruning.

Table 5-3 *Field Descriptions for the Database Properties—Database Backup Tab*

Field	Description
Password	The password for the system user.
Backup Status	The status of the database backup.
Archive Log Pruning Parameters	Displays the archive log pruning parameters.

5.1.2 Importing and Exporting Data to and from the Oracle Database

Use the Oracle Export utility to write data from an Oracle database to an operating system file in binary format. The file is stored outside the database and read to another Oracle database by using the Import utility. For more information about using Oracle Import and Export utilities, refer to the *Oracle9i Utilities* document. Alternatively, use the Oracle Enterprise Manager to import and export data.

The Export utility provides a simple way to transfer data objects between Oracle databases. The Export utility extracts the object definitions and table data from an Oracle database and stores them in an Oracle binary-format export dump file located on disk or on tape.

The export dump file is sent by using FTP—or, if on tape, physically transported—to a different site. By using the Import utility, the export dump file is transferred between databases that reside on machines not connected through a network.

**Note**

Only the Oracle Import utility can read export dump files.

5.1.3 Backing Up and Restoring the Database

This section describes how to back up and restore Cisco MGM data and how to use basic Oracle backup and recovery tools:

- [5.1.3.1 Overview of the Oracle Logical Backup](#)
- [5.1.3.2 Oracle Export Utility](#)
- [5.1.3.3 Performing a Logical Backup \(Export\)](#)
- [5.1.3.4 Oracle Import Utility](#)
- [5.1.3.5 Restoring with a Logical Backup \(Import\)](#)
- [5.1.3.6 Backing Up the Database](#)
- [5.1.3.7 Restoring the Database](#)
- [5.1.3.8 Configuring Manual NE Backup Parameters](#)

This section also explains the structure of `/opt/CiscoMGMServer`, a directory that is created automatically when you install Cisco MGM 5.0.

**Note**

The default directory `/opt/CiscoMGMServer` may have been changed during installation of the Cisco MGM server.

Cisco MGM uses an Oracle database. It is recommended that you protect your data by backing it up regularly. Backups can be stored on a local or network-mounted, disk-based file system; on a local tape drive; or on a remote tape drive.

Commercially available tools for Oracle and system-level backup include:

- Legato Networker (or “Solstice Backup” when purchased from Sun Microsystems)
- VERITAS NetBackup
- BMC Software SQL Backtrack
- GNU Oraback.sh

**Caution**

Whenever a backup is done, it must include both the database and all other Cisco MGM directories. Likewise, whenever a restore is done, it must include both the database and all other Cisco MGM directories.

5.1.3.1 Overview of the Oracle Logical Backup

It is recommended to backup the Oracle database using a logical backup. A logical backup involves reading a set of database records and writing them to a file. These records are read independently of their physical location. Oracle uses the Export (exp) and Import (imp) utilities to perform a logical database backup.

A logical backup has the following advantages:

- Checks for corrupted data blocks and verifies database consistency
- Eliminates database fragmentation
- Allows incremental export and import to store only tables that have changed since the last export
- Is portable to another machine or database

A logical backup has the following disadvantages:

- Cannot recover transactions
- Takes longer than a physical backup
- Lacks referential integrity (export is done one table at a time)

5.1.3.2 Oracle Export Utility

The Oracle Export utility reads the database, including the data dictionary, and writes the output to a binary file called an export dump file. The created file contains all of the commands necessary to recreate the selected database objects.

The Oracle Export utility permits three types of exports:

- Complete—A full database export including the data dictionary for all tables
- Incremental—Includes all of the tables that have changed since the last full export
- Cumulative—Includes all of the tables that have changed since the last full cumulative or the last full export

**Note**

Exporting directly to a Network File System (NFS)-mounted file system is not recommended due to the unusually large amount of data transfer required. The export dump file may be moved to an NFS-mounted system after exporting to a local file system.

**Tip**

Save the export dump file on a file system independent from the one used by the Cisco MGM database.

5.1.3.3 Performing a Logical Backup (Export)

Complete the following steps to perform a full export of the entire database:

**Note**

The export command is located in the `/oraclesw9i/product/9.2/bin` directory.

Step 1 Enter the following commands:

```
# su - oracle
% echo $ORACLE_SID
```

**Note**

Make sure that the value of the `ORACLE_SID` environment variable matches the system identifier (SID) of the database instance to export. During Cisco MGM installation, the default SID for Cisco MGM 5.0 is `MGM5_0`. If the SID is changed during Cisco MGM installation, the new SID becomes the default SID of the system.

Step 2 Enter the following commands to begin the export:

```
% exp userid=system/manager full=Y constraints=Y file=export_filename buffer=2800000
log=/oraclesw9i/MGM-exp.log
```

5.1.3.4 Oracle Import Utility

The Oracle Import utility reads the binary export dump file created by the Export utility and executes the embedded commands.

**Note**

The import command is located in the `/oraclesw9i/product/9.2/bin` directory.

The exported data does not need to be imported to the same database used to generate it. Also, it is not required that you import all the exported data. Upon a full import, the Oracle Import utility creates all the database objects, including tablespaces, data files, and users.

5.1.3.5 Restoring with a Logical Backup (Import)

This procedure assumes that the Cisco MGM database has already been created.

**Note**

Refer to the *Cisco Media Gateway Manager 5.0 Installation Guide* to create a Cisco MGM database, if one does not already exist.

Complete the following steps:

Step 1 Insert the Cisco MGM server installation CD.

Step 2 Enter the following commands to create the mgmanager user:

```
%sqlplus /nolog << EOF
SVRMGR> connect sys/change_on_install as sysdba
SVRMGR> @/cdrom/cdrom0/mgms/create_user.sql
SVRMGR> exit
>EOF
```

Step 3 Enter the following command to import the mgmanager schema:

```
% imp system/manager file=export_filename fromuser=ctmanager touser=ctmanager commit=y
ignore=y buffer=1000000 log=mgm-imp.log
```

Step 4 Enter the following commands to recompile all invalid database objects:

```
% cd $ORACLE_HOME/rdbms/admin
% sqlplus internal
SQL> @utlrp.sql
SQL> exit
```

5.1.3.6 Backing Up the Database



Note

Create a directory named /mgm_backup for storage of the database backup. This directory must be created before starting the backup.

To back up the database:

Step 1 In the Domain Explorer window, choose **Administration > Control Panel**.

Step 2 In the Control Panel window, click **Database Properties** to open the Database Properties pane. See [Figure 5-1](#).

Step 3 In the Database Properties pane, click the **Database Backup** tab.



Note

This option is only available if ARCHIVELOG mode was selected during the Cisco MGM installation process.

Step 4 Enter the sys Oracle user password. The password is **change_on_install**.

Step 5 Click **Start**.



Note

The database backup files are stored in /mgm_backup.

The backup log files can be viewed at oraclesw9i/admin/ORACLE_SID/udump/backup_db.log.

5.1.3.7 Restoring the Database

To restore the database:

**Caution**

Do not restore the database unless it is corrupted and inaccessible. If your database is inaccessible, your Cisco MGM server will not be running. The restore will overwrite the existing data files and restore the database from the backup files.

Step 1 If the Cisco MGM server is running, log into it as the root user and enter the following command to shut down the server:

```
mgms-abort
```

Step 2 Log into the database server.

Step 3 Enter the following commands:

```
cd /opt/CiscoMGMServer/bin
./restore_db.sh /mgm_backup /tmp
```

**Note**

The default directory `/opt/CiscoMGMServer` may have been changed during installation of the Cisco MGM server.

**Note**

The restore log file can be viewed at `/tmp/restore_db.log`

Step 4 Log into the Cisco MGM server as the root user and enter the following command to start the server:

```
mgms-start
```

Step 5 Start your Cisco MGM client(s).

5.1.3.8 Configuring Manual NE Backup Parameters

Use the NE Service Properties pane to set manual NE backup parameters.

Step 1 In the Domain Explorer window, choose **Administration > Control Panel**.

Step 2 In the Control Panel window, click **NE Service** to open the NE Service Properties pane. Click the **NE Manual Backup** tab. [Table 5-4](#) describes the fields in the NE Manual Backup tab.

Step 3 Click **Save**. Changes take effect immediately; however, the backup already scheduled for the next 24 hours remains in effect. A backup with the new parameters will occur after the previously scheduled backup runs.

Table 5-4 NE Service—NE Manual Backup Tab

Field	Subfield	Description
Select Modify Mode	—	Allows you to specify whether the manual backup should apply to a specific NE model or to all applicable NE models.
Configuration Parameters	Number of Backup Copies	Allows you to specify the number of backup copies to keep (the default is 7). Each time Cisco MGM creates a new backup file it checks the existing number of backup copies. Cisco MGM deletes files as needed, beginning with the oldest file, so as not to exceed the specified number of backup copies to keep.

5.1.3.9 Configuring Automatic NE Backup Parameters

Use the NE Service Properties pane to set automatic NE backup parameters.

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
- Step 2** In the Control Panel window, click **NE Service** to open the NE Service Properties pane. Click the **NE AutoBackup** tab. [Table 5-5](#) describes the fields in the NE AutoBackup tab.
- Step 3** Click **Enable Auto Backup**.
- Step 4** Click **Save**. Changes take effect immediately; however, the backup already scheduled for the next 24 hours remains in effect. A backup with the new parameters will occur after the previously scheduled backup runs.
-

Table 5-5 NE Service—NE AutoBackup Tab

Field	Subfield	Description
Select Modify Mode	—	Allows you to specify whether the manual backup should apply to a specific NE model or to all applicable NE models.
Configuration Parameters	NE Model	If NE Model is selected under Select Modify Mode, this field allows you to specify the NE model that will be backed up manually.
	Backup Frequency	Default value that defines the backup frequency.
	Number of Backup Copies	Allows you to specify the number of backup copies to keep (the default is 7). Each time Cisco MGM creates a new backup file it checks the existing number of backup copies. Cisco MGM deletes files as needed, beginning with the oldest file, so as not to exceed the specified number of backup copies to keep.
Backup Time	—	Time when the backup is scheduled to begin.

5.1.4 Pruning the Database

Cisco MGM provides features to prune the database. Pruning is the removal of information that is deemed old or less significant, and can include the following data:

- Fault Management data
- Performance data
- Audit Trail data
- Audit Log data
- System Log Error Log
- Self Monitor data
- Job Monitor data

You can change the pruning settings using the Control Panel. You can select when exactly the pruning has to occur daily (at non-peak hours like 00:00 hrs), and can also select the pruning period (like prune all data except data for the last 7 days).

**Note**

Pruned data is entirely lost from the database.

5.1.4.1 Setting the Time and Date for Automatic Pruning

Choosing to prune the database automatically prunes daily all PM data, FM data, audit log data, audit trail data, and Error Log data older than the specified retention period. To configure automatic database pruning:

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
- Step 2** In the Control Panel window, click **Database Properties** to open the Database Properties pane. See [Figure 5-1](#).
- Step 3** In the Database Properties pane, click the **Pruning** tab. [Table 5-2](#) describes the fields in the Database Properties Pruning tab. The following information is displayed:
- PM data
 - FM data
 - Audit Log data
 - Error Log data
 - Audit Trail data
 - Self Monitor data
 - Job Monitor data
- Step 4** Click **Enable** for each field as desired, and set the number of days and time of pruning.
- Step 5** After making the selections, click **Save**. Changes take effect immediately.
-

5.1.4.2 Using Pruning Scripts

Running database pruning scripts allows you to prune Cisco MGM data from the Oracle database at any given time. Pruning scripts allows you to prune the following types of data:

- Audit log data
- Audit trail data
- Error log data
- Event data
- All PM data
- NEs and all related information
- Server monitoring data


Note

For information about pruning NEs in a high availability environment, refer to the *Cisco Media Gateway Manager 5.0 High Availability Installation Guide*.

To use a pruning script:

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

Step 2 Enter the following command to change to the Cisco MGM server bin directory:

```
cd /opt/CiscoMGMServer/bin
```


Note

The default directory `/opt/CiscoMGMServer` may have been changed during installation of the Cisco MGM server.

Step 3 Enter the following command to see a list of pruning scripts:

```
ls -al prune*
```

Step 4 Select a script and a parameter (based on database pruning) and enter the corresponding command on the UNIX shell.

For example, to prune Error Log data older than 25 days, enter the following command:

```
./prune_errlog.sh 25
```

Table 5-6 describes parameters that can be passed to each script and the tables that are affected.

Table 5-6 Database Pruning

What to Prune (Script Name)	Tables Affected	Input Parameters	Remarks
Prune audit log data (prune_auditlog.sh)	transaction_log_table	Number of days 1–31	Removes all audit log entries that were created before <i>n</i> days.
Prune error log data (prune_errlog.sh)	error_log_table	Number of days 1–31	Removes all transaction log entries that were created before <i>n</i> days.

Table 5-6 Database Pruning (continued)


What to Prune (Script Name)	Tables Affected	Input Parameters	Remarks
Prune alarm and event data (prune_fm.sh)	alarm_event_table active_alarm_table	Number of days 1–31	Removes all alarm and event entries that were created before <i>n</i> days.
Prune admin job table (prune_admin_job_table.sh)	admin_job_table	Number of days 1–31	Removes all admin job entries that were created before <i>n</i> days.
Prune server monitor table (prune_server_monitor.sh)	server_monitor_table	Number of days 1–31	Removes all server monitor entries that were created before <i>n</i> days.
Prune PM data (prune_pm.sh)	all_data tables	Number of days 1–31	Removes all PM entries that were created before <i>n</i> days.
 Caution Before running the script, shut down all Cisco MGM clients and the Cisco MGM server. See the “1.4.1 Starting and Stopping the Cisco MGM Server” section on page 1-6.	active_alarm_table additional_device_info admin_job_table alarm_count_table alarm_event_table aps_group_table audit_log_table circuit_dest_tbl circuit_span_tbl circuit_tbl circuit_vcg_tbl domain_table eqpt_info_table eqpt_relationship_table if_cross_connect if_dwdm_channel_group if_optical_phy_config_table interface_aps_info interface_dwdm_frequency interface_stack_table managed_et_tab map_cust_table mib2_interface_table ne_inventory_table ne_port_status_table ne_swimage_table	NE SYS ID	Removes all information about the NE from the database. Use this script with extreme caution.

Table 5-6 Database Pruning (continued)

What to Prune (Script Name)	Tables Affected	Input Parameters	Remarks
Remove an NE (prune_ne.sh) (continued)	???_table ?????_tableoss_alarm_fldr_tid_d eny_tbl pm_historical_appointments proxy_server_table server_monitor_table sway_user_port_table tca_event_table transaction_log_table unmanaged_ne_inventory_table user_map_table circuit_dest_tbl circuit_span_tbl link_table ne_info_table	NE SYS ID	Removes all information about the NE from the database. Use this script with extreme caution.
Prune server monitoring data (prune_server_monitor.sh)	server_monitor_table	Number of days 1-31	Removes all server monitoring data.

5.1.5 Using the SQL*PLUS Client to Manage the Database

To access the database and Cisco MGM schema objects, use the SQL*PLUS client that ships with Oracle products. The SQL*PLUS client is available for Microsoft Windows 2000 or NT 4.0 PCs or Sun Solaris 8 workstations. Refer to the Oracle documentation to install and run the SQL*PLUS client on a Windows 2000 or NT 4.0 PC.

On a Sun Solaris workstation, the SQL*PLUS client is installed as part of the Oracle server installation. The following guidelines are for logging into SQL*PLUS as a Cisco MGM user and managing Cisco MGM schema objects and data. Refer to the *SQL*PLUS User Guide* for a complete description.

Step 1 On the Sun Solaris machine running Oracle, log in as the Oracle owner user. Use the username that was used when installing Oracle9i.



Note To verify the username, enter the **id** command on the shell.

Step 2 Verify that the following UNIX environment variables for the Oracle user are set correctly:

- ORACLE_HOME
- ORACLE_SID
- PATH variable has \$ORACLE_HOME/bin in the path
- LD_LIBRARY_PATH

Step 3 On the command line, enter the following command:

```
sqlplus ctmanager/mgm123!
```

The message “Connected to: Oracle9i...” and the SQL> prompt should appear. If not, enter the username and password again.

Step 4 Enter any SQL command supported by Oracle upon connection to SQL*PLUS. For a list of SQL commands supported by Oracle, refer to the *SQL*PLUS User Guide*.

5.1.6 Basic SQL Commands for Cisco MGM Schema Objects

Table 5-7 lists commands that display, update, or modify Cisco MGM schema objects. Run each command in SQL*PLUS by entering the command at the SQL> prompt.

Table 5-7 SQL Commands for Cisco MGM Schema Objects

SQL Command	Description
<code>select table_name from user_tables;</code>	Returns a list of all table names owned by the mgmanager user.
<code>select view_name from user_views;</code>	Returns a list of all views owned by the Cisco MGM user.
<code>describe table_name;</code>	Takes a <i>table_name</i> as a parameter (valid table names are those returned by the previous two commands) and lists the name, type, and size of columns in the table.
<code>describe view_name;</code>	Takes a <i>view_name</i> as a parameter (valid view names are those returned by the previous two commands) and lists the name, type, and size of columns in the view.
<code>select col1, col2... coln from table_name;</code>	Takes <i>col1...coln</i> and <i>table_name</i> as parameters and displays data for all the columns listed. To display data for all columns, use an asterisk (*) instead of col1, col2, and so on.
<code>select col1, col2... coln from table_name where col1 = value1 and col2 = value2...</code>	Takes <i>col1...coln</i> and <i>table_name</i> as parameters and displays data for all the columns listed that meet the condition specified in the “where” clause. For example, the command: <code>select nedbaccessid from ne_info_table where nesysid = 'ANGEL';</code> returns the value of column nedbaccessid from table ne_info_table for all rows for which nesysid = ANGEL.
<code>select col1, col2... coln from view_name where col1 = value1 and col2 = value2...</code>	Takes <i>col1...coln</i> and <i>view_name</i> as parameters and displays data for all the columns listed that meet the condition specified in the “where” clause.
<code>delete table_name;</code>	Takes <i>table_name</i> as a parameter and deletes the entire contents of the table. To make the change permanent, enter commit ; at the SQL> prompt.

Step 5 Enter the following command to start the Cisco MGM server:

```
mgms-start
```

5.1.7 Enhancing Database Performance

To improve database performance when Cisco MGM clients access Cisco MGM data, tune the Oracle database as outlined in “Part IV: Optimizing Oracle Instance Performance” in the *Oracle9i Tuning Guide*.

5.1.8 Removing an Old Version of the Cisco MGM Database

If necessary, remove all Cisco MGM schema objects from the database. However, all Cisco MGM information from the database will be deleted. An example of when to remove all Cisco MGM schema objects from the database is during reinstallation of the Cisco MGM server when data from a previously installed version is irrelevant.

To remove all Cisco MGM schema objects from the database:

Step 1 Shut down the Cisco MGM server and all Cisco MGM clients.

Step 2 On the Sun Solaris workstation running Oracle, log in as the Oracle owner user. Use the username that was used when installing Oracle9i.



Note To verify the username, enter the **id** command on the shell.

Step 3 Enter the following commands to shut down the Cisco MGM database:

```
%sqlplus /nolog << EOF
SVRMGR> connect sys/change_on_install as sysdba
SVRMGR> shutdown abort;
SVRMGR> EOF
```

Step 4 Enter the following commands:

```
cd /db01
/bin/rm -rf ORACLE_SID
```

Step 5 Change the directory to the location of the Cisco MGM Data1 tablespace (/db02).

Step 6 At the UNIX shell prompt, enter the following command:

```
ls -alR mgmdata1
```

Step 7 Enter the following commands:

```
/bin/rm -rf ORACLE_SID
/bin/rm -rf mgmdata1/ORACLE_SID*
```

Step 8 Change the directory to the location of the Cisco MGM Data2 tablespace (/db03).

Step 9 Enter the following command:

```
/bin/rm -rf mgmdata2/ORACLE_SID*
```

Step 10 Change the directory to the location of the Cisco MGM Index tablespace. This was the third directory specified during the Cisco MGM server installation. The default location is /db04.

Step 11 Enter the following command:

```
/bin/rm -rf mgmindex/ORACLE_SID*
```

5.2 How Do I Monitor the Network?



Note

For specific fault monitoring information, see [Chapter 9, “Managing Faults.”](#)

This section contains the following information:

- [5.2.1 Establishing a Telnet Session to a Node](#)
- [5.2.2 Connecting to Nodes Through Secured Shell](#)
- [5.2.3 Monitoring a Network Element](#)
- [5.2.4 Monitoring a Card with Chassis View](#)
- [5.2.5 Monitoring a Line or Port with Chassis View](#)
- [5.2.6 Monitoring Scheduled Tasks](#)
- [5.2.7 Monitoring Service Status](#)
- [5.2.8 Searching for a Network Element](#)
- [5.2.9 Monitoring Cisco MGM Client/Server Configuration Details](#)
- [5.2.10 Monitoring Network Manageability Statistics](#)
- [5.2.11 Managing the VSI Controllers](#)

By managing the graphical representations of the network nodes and device objects with Chassis View, you can:

- Provide status updates for nodes, cards, and lines
- Display the front or rear view of the node
- Perform provisioning tasks, such as, shelf, card, and line levels by quickly navigating to the Configuration Center
- Display the LED status for each card reflecting both standby and active states

5.2.1 Establishing a Telnet Session to a Node

To establish a telnet session to a node:

Step 1 In the Chassis View, Diagnostic Center, Configuration Center or Statistics Report tree, select the source node from the Hierarchy pane and choose **Tools > Administration > Telnet**. Or, right-click the source node and choose **Administration > Telnet**.

Step 2 When the login prompt appears in the Telnet window, you must:

- a. Enter the Service Level name.
- b. Enter the Service Level password.

You have successfully established a telnet session to a node.

5.2.2 Connecting to Nodes Through Secured Shell

When you connect as an Operator to an MGX node through Cisco MGM, or when Cisco MGM connects to MGX, secured shell (SSH) enhances the security.



Note

To use SSH through the Cisco MGM client, the SSH secured shell must be installed and the path to the executable must be set in the environmental variable PATH. For more information, refer to the SSH Communications Security Corporation at the following URL: <http://www.ssh.com>

To connect to a node using SSH:

Step 1 In the Configuration Center, to choose the node in the Hierarchy pane, you can:

- a. Choose the node.
- b. Enter the node name or IP address into the text box.

Step 2 To use SSH, you can:

- a. Right-click the source node and choose **Administration > SSH**.
- b. Select the source node and choose **Tools > Administration > SSH**.

Step 3 Enter the default switch username **cisco** into the text box.



Note

If you decide not to use ssh by choosing telnet, you do not need to enter a username.

Step 4 Click **OK** to open the SSH secure shell window.

Step 5 At the prompt, enter the password to log on the node through SSH.

5.2.3 Monitoring a Network Element

You can monitor the status of the NEs through Chassis View. Alarm Browser also provides up-to-date information that can be used for managing faults. See [Chapter 9, “Managing Faults.”](#)

To monitor an NE:

Step 1 In the Chassis View tree, to choose the NE, you can:

- a. Choose the NE.
- b. Enter the node name or IP address into the text box.

- Step 2** Press **Enter**.
- The chosen NE is displayed along with the current status for each card.
- Step 3** Click the **Front View** tab or **Rear View** tab of the NE. The default is the front view.
- Step 4** Check the status of the NE from Inspector View.
-

5.2.4 Monitoring a Card with Chassis View

You can select a card to monitor when the objects are associated with a particular card. The following settings are monitored using the objects:

- SONET interface settings
- Interface partition settings
- Revision numbers of hardware, software, and firmware installed on the card
- Lines, interfaces, and ports on the card

To monitor a card:

-
- Step 1** In Chassis View, there are two ways to choose the card:
- Choose the card from the Hierarchy pane, or
 - Click the slot that you want to display from the node view. A yellow border highlights the chosen slot in the node view.
- Step 2** Click the **Front View** tab or **Rear View** tab of the node. The default is the front view. See [Figure 5-2](#).
- Step 3** Check the status of the card from Inspector View.
- Step 4** Right-click the slot and choose the corresponding application. If you want to configure the settings for the card, choose **Configuration Center**.

The Configuration Center is launched with a view of the network elements.

5.2.6 Monitoring Scheduled Tasks

The Job Monitor table provides information about scheduled administrative tasks—memory backup, memory restore, and software download. For example, you can see the system username of the person who entered a specific task, the time that the task began, and the time that the task ended.

**Note**

A job consists of multiple tasks.

Each entry consists of the following:

- Task Owner—User ID used during login.
- NE ID—NE ID on which the operation is executed.
- Task Creation Time—Server time when the request was made.

After these requests are executed, the job's status is updated accordingly in the Job Monitor table.

5.2.6.1 Viewing the Job Monitor Table

To view the Job Monitor table:

Step 1

Choose **Administration > Job Monitor** in the Domain Explorer window. The Job Monitor table appears and displays the fields described in [Table 5-8](#).

**Note**

Some fields in the Job Monitor Table apply only to certain tasks, NEs, or NE versions.

Table 5-8 Job Monitor Table Descriptions

Column Name	Description
Job ID	ID number corresponding to the selected job.
Task ID	ID number corresponding to the task. If a job includes more than one NE, each NE has a separate task ID for the job.
Task Type	Indicates the type of task: <ul style="list-style-type: none"> • Automatic memory backup • Memory backup • Memory restore • Software download
Task Owner	System username of the person who entered the task.
NE ID	Name of the NE on which the task is scheduled to run.
Task Status	Current status of the task: Queued, Running, Canceled, Failed, Succeeded, or Waiting: <ul style="list-style-type: none"> • Queued—The task is scheduled but has not yet begun. • Running—The task is in progress. • Canceled—The task has been canceled. • Succeeded—The task succeeded. • Failed—The task failed. • Waiting: The node manager must be initialized before a task can begin. If the node manager is not initialized, the status of the task is Waiting. After the node manager becomes initialized, the task status changes to Queued.
Task Creation Time	Date and time when the task was entered into the system.
Task Scheduled Time	Date and time when the task is scheduled to begin.
Task Start Time	Date and time when the task began.
Task End Time	Date and time when the task ended.
Display Information	Displays information related to the Task Type column.
User Comments	Displays any user-entered comments relating to the task.
Additional Information	Displays any additional information.

5.2.6.2 Viewing the Job Monitor Filter Dialog Box

Use the Job Monitor Filter dialog box to filter job data according to criteria that you select and to display the results in the Job Monitor Table. [Table 5-9](#) provides descriptions:

Table 5-9 Job Monitor Filter Dialog Box Descriptions

Tab	Description
Creation Time (time zone)	Allows you to filter job monitor data for a specified time period, ranging from the past hour to the past 180 days. Additionally, you can click the User Specified radio button to specify an exact filter starting and ending time by month, day, year, and hour. The time zone can be Greenwich mean time (GMT), a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. Click No Time Specified if you want to filter events and the time period is not important.
NE ID	Allows you to select network elements (NEs) back and forth between the list of available NE IDs and selected NE IDs. The filter runs on the NEs in the Selected NE ID list.
Task Owner	Allows you to move owners back and forth between the list of available owners and selected owners. The filter runs on the owners in the Selected Task Owner list.
Job/Task ID	<p>Allows you to filter jobs by job and task IDs. Jobs consist of multiple tasks. For example, if you perform a memory backup for multiple NEs, the backup operation is a job, and each NE is a task.</p> <ul style="list-style-type: none"> • If you specify a start and end ID range in the job ID field but leave the task ID field blank, the filter runs on the job ID range. • If you specify a start and end ID range in the task ID field but leave the job ID field blank, the filter runs on the task ID range. • If you specify a start and end ID range in both the job ID and task ID fields, the filter first applies the values in the job ID field, then narrows the filter according to the values in the task ID field. For example, if you specify that job ID Start = 1, job ID End = 3, task ID Start = 1, and task ID End = 2, the returned value is all entries with a job ID of 1, 2 or 3 and a task ID of 1 or 2.
Task Type	<p>Allows you to move task types back and forth between the list of available task types and selected task types. Task types include:</p> <ul style="list-style-type: none"> • Automatic memory backup • Memory backup • Memory restore • Software download <p>The filter runs on the tasks in the Selected Task Type list.</p>
Task Status	<p>Allows you to filter tasks by status:</p> <ul style="list-style-type: none"> • Queued—The task is scheduled but has not yet begun. • Running—The task is in progress. • Canceled—The task has been canceled. • Failed—The task failed. • Succeeded—The task succeeded. • Waiting—The node manager must be initialized before a task can begin. If the node manager is not initialized, the status of the task is Waiting. After the node manager becomes initialized, the task status changes to Queued.

5.2.6.3 Canceling a Scheduled Job or Task

To cancel a scheduled job or task from the Job Monitor table list:

-
- Step 1** In the Domain Explorer window, choose **Administration > Job Monitor**.
- Step 2** Select a task to cancel; then, click the **Cancel Task** or **Cancel Job** tool (or choose **Edit > Cancel Task**, or **Edit > Cancel Job**).



Note Cancel is enabled only for jobs and tasks with a Queued status. When a job contains more than one task in a Queued status, choosing **Cancel Job** cancels all tasks with the same job ID.

- Step 3** Click **OK** in the confirmation dialog box.
-

5.2.6.4 Job Monitor Notes

The Job Monitor Note dialog box allows you to view and add notes to jobs displayed in the Job Monitor window. If a job has a note, a Job Monitor Note tool appears under the User Comments column. To view, add, or delete a note, select a job and click the tool. Comments are visible to all users.

The following table provides descriptions:

Table 5-10 *Field Descriptions for the Job Monitor Note Dialog Box*

Field	Description
Note	Provides space for you to type your comments about the selected job. To add comments to the previous comments, click the Append radio button. To overwrite the previous comments, click Replace . To delete the comments, click Delete .
History	Displays comments entered by previous users.

To edit a Job Monitor user note:

-
- Step 1** In the Domain Explorer window, choose **Administration > Job Monitor**.
- Step 2** Select a task and choose **Edit > User Note**.
-

You can export the information in the Job Monitor Table to a file (see [5.7.1 Exporting Data to a Text File](#)), or you can generate an HTML file (see [5.7.2 Generating an HTML Report](#)).

5.2.7 Monitoring Service Status

The Service Monitor Table allows you to view the status of the services that are running on the Cisco MGM server. [Table 5-11](#) provides descriptions:

Table 5-11 Column Name Descriptions for the Service Monitor Table

Column Name	Description
Service Name	Displays the name of the selected service.
Logged In At	Displays the last time the user logged in.
IP Address	Displays the IP address of the selected service.
Session ID	Displays the unique session ID.

**Note**

The **showmgm** command is an alternate way of viewing processes or services that are running in the Cisco MGM server.

You can export the information in the Service Monitor Table to a file (see [5.7.1 Exporting Data to a Text File](#)), or you can generate an HTML file (see [5.7.2 Generating an HTML Report](#)).

5.2.8 Searching for a Network Element

Cisco MGM allows you to search for a specific NE in the network. The search always starts from the root node and returns to the root node after reaching the last node.

-
- Step 1** In the Domain Explorer, choose **Edit > Find**.
- Step 2** In the Find dialog box, from the Object Type drop-down list, select Network Element/Group.
- Step 3** In the Object Properties section, search for an NE using one of the following methods:
- Name—Click this radio button and enter the name of the NE you are searching for.
 - IP Address—Click this radio button and enter the IP address of the NE you are searching for.
 - Description—Click this radio button and enter a description of the NE that you are searching for.
- Step 4** Check the **Ignore Case** check box to make the search noncase-sensitive.
- Step 5** Click **OK**. In the Domain Explorer, the NE is highlighted in the tree section and the NE properties are displayed in the properties section.
-

**Note**

In the Domain Explorer, you can also choose **Edit > Find Next** to find the next object that matches the initial Find specification.

5.2.9 Monitoring Cisco MGM Client/Server Configuration Details

The Cisco MGM Properties pane displays information about the Cisco MGM server and client configuration. In the Control Panel, choose Cisco MGM from the Hierarchy pane to display the Cisco MGM Properties pane. This pane has two tabs; Server Configuration and Client Configuration. [Table 5-12](#) provides descriptions:

Table 5-12 Cisco MGM Properties Descriptions

Tab	Field	Description
Server Configuration	Server Name	Displays the workstation name where the Cisco MGM server application resides.
	IP Address	Displays the IP address of the Cisco MGM server.
	Server Port	Displays TCP port number of the Cisco MGM server.
	Software Version	Shows the Cisco MGM software version that is running.
Client Configuration	Host Name	Displays the workstation name where the Cisco MGM client application resides.
	IP Address	Displays the IP address of the Cisco MGM client.
	Version	Shows the Cisco MGM software version that is running.
	Username	Displays the name that was used to log into the Cisco MGM client.

**Note**

The Server and Client configuration details cannot be edited.

5.2.10 Monitoring Network Manageability Statistics

These tasks are used in the Diagnostic Center to monitor statistics events for network manageability:

- [5.2.10.1 Running a Diagnostic Check at the Network Level](#)
- [5.2.10.2 Running a Diagnostic Check at the Node Level](#)
- [5.2.10.3 Statistics Entries for Network Manageability](#)
- [5.2.10.4 Sending a Trouble Ticket](#)

By monitoring network manageability, you can:

- Collect element management health-related statistics.
- Browse over detailed information about past element management health statistics.
- Provide statistics about the success rates, failure rates, and throughput of Cisco MGM to network interfacing protocols, such as FTP, and SNMP.
- Report the number of successes and failures that happened in the last hour.
- Retrieve statistics for a given time period.
- Identify problems with Cisco MGM and the ability to effectively manage the network.
- Identify the root causes for problems that can occur due to general network problems.
- Display information about all the nodes at the network level.
- Display information at the node level.

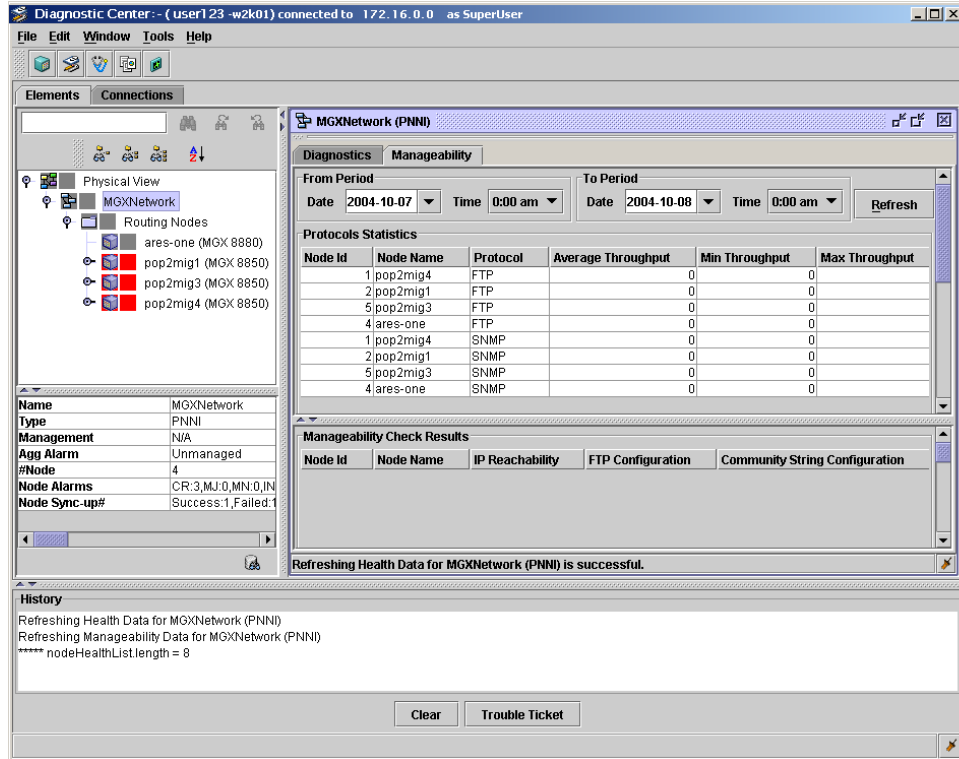
5.2.10.1 Running a Diagnostic Check at the Network Level

In the Diagnostic Center, you can verify that all the nodes in the network are being managed correctly by Cisco MGM.

To run a diagnostic check at the network level:

-
- Step 1** In the Diagnostic Center, double-click or drag and drop the network from the Hierarchy pane to the right hand pane, to display the diagnostics at the network level.
 - Step 2** Click the **Manageability** tab. See [Figure 5-3](#).
 - Step 3** In the **From Period** area:
 - a. Choose the date to start from the **Date** drop-down arrow.
 - b. Choose the time from the **Time** drop-down arrow.
The default time is 12:00 a.m (0000).
 - Step 4** In the **To Period** area:
 - a. Choose the date to end from the **Date** drop-down arrow.
The maximum number of days to keep data is 30 days. The minimum number of days is 1.
 - b. Choose the time from the **Time** drop-down arrow.
The default time is 12:00 a.m (0000).
 - Step 5** Click **Refresh** to refresh the health data for the network.
 - Step 6** Verify the statistics values for each node ID and node name from the **Protocols Statistics** area.
For parameter definitions, see [Table 5-13](#).
 - Step 7** Verify the manageability data results for the node from the **Manageability Check Results** area.
For parameter definitions, see [Table 5-14](#).
 - Step 8** Click **Refresh** to retrieve all check result entries in the manageability table for every node in the network.
-

Figure 5-3 Diagnostic Center—Manageability Tab



5.2.10.2 Running a Diagnostic Check at the Node Level

In the Diagnostic Center, you can verify that selected nodes are being managed correctly by Cisco MGM.

To run a diagnostic check at the node level:

- Step 1** In the Diagnostic Center, double-click or drag and drop the node from the Hierarchy pane to the right hand pane, to display the diagnostics at the node level.
- Step 2** Click the **Manageability** tab. See [Figure 5-3](#).
- Step 3** In the **From Period** area:
 - a. Choose the date to start from the **Date** drop-down arrow.
 - b. Choose the time from the **Time** drop-down arrow.
The default time is 12:00 a.m (0000).
- Step 4** In the **To Period** area:
 - a. Choose the date to end from the **Date** drop-down arrow.
The maximum number of days to keep data is 30 days. The minimum number of days is 1.
 - b. Choose the time from the **Time** drop-down arrow.
The default time is 12:00 a.m (0000).
- Step 5** Click **Refresh** to retrieve all statistics entries for the node.

For parameter definitions, see [Table 5-13](#).

- Step 6** In the **Node Login Information** area:
- a. Enter the user name in the **User Id** field.
 - b. Enter password in the **Password** field.
- Step 7** Click **Check Manageability** to run a diagnostic check for the node.
- Step 8** Verify the check results from the **Manageability Check Results** area.
- For parameter definitions, see [Table 5-14](#).

5.2.10.3 Statistics Entries for Network Manageability

The statistics entries that are used for network manageability are described in [Table 5-13](#) and [Table 5-14](#). [Table 5-13](#) lists the parameters for the protocol statistics that are health-related.

Table 5-13 Health Related Parameters

Name	Description
Node Id	Identifies the ID for the configured node.
Node Name	Identifies the configured name of the node.
Protocol	Specifies the protocol for either FTP or SNMP.
Average Throughput	Measures the average FTP throughput performance in bytes per second for the switch during the specified time period. The average SNMP throughput is measured in seconds per request for the switch during the specified time period.
Min Throughput	Measures the minimum throughput performance for FTP, and SNMP on a per node basis. The minimum throughput is calculated for FTP, and SNMP operations.
Max Throughput	Measures the maximum throughput performance for FTP, and SNMP on a per node basis. The maximum throughput is calculated for FTP, and SNMP operations. The value is the maximum rate achieved in bytes per second for any one FTP request to complete.
Success	Specifies the number of successful FTP, or SNMP operations for the node during the specifies time period.
Session Failure	Specifies the number of network failures for the session.
Transfer Failure	Specifies the number of network failures for the transfer.
Retry Exceeded	Provides information about the number of times for retries that exceeded the maximum set limit.
File Size Mismatch	Specifies that the file transfer is considered a success if the local file size matches with the remote file size. For a mismatch, an error is reported.
Throttle Error	Determines the maximum limit for the number of pending Get, Set, and GetNext operations reached for the switch.
Session Timeout	Specifies the session timeout period where the FTP request remains in the request queue.

Table 5-13 Health Related Parameters (continued)

Name	Description
Transfer Timeout	Specifies the transfer timeout is the estimated period when the transfer is completed. The transfer is done by FTP from the previous transfer of the throughput data for a node. If the file transfer fails to complete within the period, transfer is aborted and an error is reported.
Queue Full	Accommodates a finite number of concurrent TFTP requests and if the queue is fully any new request can trigger a report error.
Generic Error	Displays any generic error returned by the node.

Table 5-14 lists the check results parameters for network manageability.

Table 5-14 Network Manageability Parameters

Name	Description
Node Id	Identifies the ID for the configured node.
Node Name	Identifies the configured name of the node.
IP Reachability	Specifies the results of the IP reachability test.
FTP Configuration	Specifies the results of the FTP reachability test.
Community String Configuration	Specifies the results of the SNMP community string.
Trap IP Configuration	Specifies the results of the trap IP configuration test.
Trap Manager Configuration	Verifies if the Cisco MGM workstation is registered as a trap manager.
Time Stamp	Specifies the time stamp when the manageability check was requested.

5.2.10.4 Sending a Trouble Ticket

The Diagnostic Center collects the output and results of all the diagnostic operations and logs them into the History Panel. You can send a trouble ticket that includes all the data from the History Panel.

To send a trouble ticket:

- Step 1** In the Diagnostic Center, drag and drop the network or node from the Hierarchy pane to the right hand pane, to display the diagnostics at either the network level or the node level.
- Step 2** Click the **Manageability** tab to display the Manageability Configuration window at the node level.
- Step 3** Click **Trouble Ticket** to display the Trouble Ticket window.
Automatically, the entire content from the History Panel is extracted into the Trouble Ticket window.
- Step 4** Enter the email address that you want to send the trouble ticket to in the **To** field.
- Step 5** Enter the title of the trouble ticket in the Subject field.
- Step 6** Click **Attach** to include an Element or Connection file with the trouble ticket, if required.

- Step 7** Click **Send** to send the trouble ticket to recipient.
- Step 8** Click **Save** to save the trouble ticket in the directory.
-

5.2.11 Managing the VSI Controllers

These tasks are used to work with VSI controllers:

- [5.2.11.1 Creating a VSI Controller](#)
- [5.2.11.2 Displaying a VSI Controller](#)
- [5.2.11.3 Deleting a VSI Controller](#)

5.2.11.1 Creating a VSI Controller

A VSI controller must be added when a new node is added. There is one controller per node.

To create a VSI controller, complete the following procedure:

- Step 1** In the Domain Explorer, right-click the node from the Hierarchy pane and choose **Configuration > MGX8880/8850 MG > Configuration Center**.
- Step 2** Click the **Elements** tab to display the Configuration Window for Elements.
- Step 3** Click the **Controllers** tab to display the Controllers Table.
- Step 4** Click **Create** to display the Controllers Create window.
- Step 5** Enter the ID for the VSI controller in the **Controller ID** field.
- Step 6** Choose one of the following controller options from the **Controller Type** drop-down arrow:
- **par**—Portable Auto Route (PAR). The **par** option is a VSI Master controller that implements a Cisco proprietary protocol for network routing and topology in a network, which contains only Cisco switches.
 - **pnni**—Private Network-to-Network Interface (PNNI) controller. The PNNI protocol is used between private ATM Switches and between groups of ATM switches. PNNI is defined for distributing topology information between switches and clusters of switches.
 - **lsc**—Label Switch Controller (LSC). The LSC implements the MPLS protocol. The LSC is a router which is capable of controlling the operation of a separate ATM switch, so that both of them function as a single ATM-LSR (ATM Label Switch Router).
- Step 7** Enter the name for the controller in the **Controller Name** field.
- Step 8** Choose one of the following shelf location options from the **Controller Shelf Location** drop-down arrow:
- **internal**—specifies that the controller resides on the same shelf as the switch.
 - **external**—specifies that the controller resides on the external platform. The controller shelf is connected to the switch by an ATM link.
- Step 9** Enter the slot number that the VSI controller is plugged into in the **Controller Location** field.
- Step 10** Click **Apply** to create a VSI controller.
-

5.2.11.2 Displaying a VSI Controller

To display a VSI controller, complete the following procedure:

-
- Step 1** In the Domain Explorer, right-click the node from the Hierarchy pane and choose **Configuration > MGX8880/8850 MG > Configuration Center**.
 - Step 2** Click the **Elements** tab to display the Configuration Window for Elements.
 - Step 3** Click the **Controllers** tab to display the Controllers Table.
 - Step 4** Select the controller entry from the Controllers Table.
 - Step 5** Click **Details** to display the Controllers Configuration window.
-

5.2.11.3 Deleting a VSI Controller

To delete a VSI controller, complete the following procedure:

-
- Step 1** In the Domain Explorer, right-click the node from the Hierarchy pane and choose **Configuration > MGX8880/8850 MG > Configuration Center**.
 - Step 2** Click the **Elements** tab to display the Configuration Window for Elements.
 - Step 3** Click the **Controllers** tab to display the Controllers Table.
 - Step 4** Select the controller entry from the Controllers Table.
 - Step 5** Click **Delete** to delete the controller entry.
-

5.3 How Do I Modify the Network?

This section contains the following information:

- [5.3.1 Changing the Operational State of an NE](#)
- [5.3.2 Backing Up and Restoring Memory](#)
- [5.3.3 Changing IP Addresses for NEs](#)
- [5.3.4 Viewing and Modifying the Server Configuration](#)
- [5.3.5 Setting Up Session Recovery](#)
- [5.3.6 Changing the Server IP Address when Cisco MGM and Oracle Are on the Same Server](#)
- [5.3.7 Viewing and Modifying Server Configuration Information](#)
- [5.3.8 Restoring Server Configuration Files](#)
- [5.3.9 Initializing the Node Resync Process](#)
- [5.3.10 Configuring Application-Specific Parameters](#)
- [5.3.11 Using UNIX-Level Scripts](#)

5.3.1 Changing the Operational State of an NE

You need to change the operational state of a NE to carry out certain tasks. For example, the operational state field of an NE must be changed to Out of Service before the NE can be deleted.

To change the operational state of an NE:

Step 1 In the Domain Explorer tree, select the NE that will be changed. The Network Element Properties pane appears.

Step 2 In the Operational State field, choose one of the following operational states:

- **In Service**—The NE is deployed and requires monitoring. Cisco MGM collects polling, fault management (FM), configuration management (CM), and PM data from in-service NEs and stores the data in the database.
- **Out of Service**—The NE has been marked Out of Service by a network administrator and does not require monitoring. The Cisco MGM database records the last known state of the NE when it was In Service.
- **Under Maintenance**—The NE is temporarily Under Maintenance but requires monitoring. This state is the same as In Service except that Cisco MGM does not report alarms or events for Under Maintenance NEs.

**Tip**

You can also right-click an NE in the Domain Explorer tree and choose **Mark Under Maintenance**, **Mark In Service**, or **Mark Out of Service** from the shortcut menu.

Two additional operational states cannot be chosen by the user. These operational states are changed by Cisco MGM based on the initialization tasks that are completed:

- **In Service–Initializing**—The NE is marked as In Service–Initializing when Cisco MGM reaches connectivity of the NE (Communication State is marked as Available) and the discovery process starts. The initialization process is completed when fault and inventory have been synchronized. The operational state changes from In Service–Initializing to In Service–Synch Configuration.
- **In Service–Synch Configuration**—The NE is marked as In Service–Synch Configuration when Cisco MGM uploads a configuration for that NE. You can change the operational state of an NE from In Service–Synch Configuration to Out of Service.

Step 3 Click **Save**.

**Timesaver**

If an NE is brought down, mark it as Out of Service to prevent unnecessary polling traffic on the data communications network (DCN).

**Note**

When you mark an NE as Out of Service and then mark it as In Service, the Cisco MGM alarm time stamp in the Alarm Browser window is resynchronized with the time stamp when the NE is put back In Service.

5.3.2 Backing Up and Restoring Memory

Cisco MGM allows you to backup and restore memory for selected NEs. For example, if you wanted to save your settings for a particular NE, you can backup the memory for just that NE.

Cisco MGM backs up configuration and provisioning information residing in the flash memory of an NE. Cisco MGM provides three methods by which to perform the configuration backup operation:

- Manually on demand
- Scheduling (one time only)
- Periodic, automatic scheduling based on a configurable time set by the operator

The operator can specify the number of backup configurations that should be kept at any given time. The default number is seven.


Note

The maximum number of copies that can be saved is fundamentally dictated by the amount of disk space available.

The oldest configuration that was backed up is replaced by the current backup depending on the (configured) number of copies the user wishes to retain at any given time. The memory restore function in Cisco MGM can then be used to rollback to any one of the previous configurations that was saved. Once the configuration is downloaded, the operator will need to issue CLI commands to activate the new configuration.


Note

This restore operation would be service affecting as the node will be re-booted to reflect the restored configuration.

Follow the procedures described in these sections to backup and restore memory (configuration data) on NEs within the following products:

- MGX8880
- MGX8850

5.3.2.1 Backing Up Memory


Note

[Table 5-15](#) describes the fields in the Memory Backup dialog box.

- Step 1** In the Domain Explorer tree, select a management domain or group that contains NEs that are assigned an In Service or Under Maintenance operational state. Alternatively, select an NE that is assigned an In Service or Under Maintenance state.


Note

Memory backup is not allowed for out-of-service NEs.

- Step 2** Choose **Administration > Memory Backup**.

- Step 3** The Memory Backup dialog box appears. Enter the following information (see [Table 5-15](#) for details):
- NE Model

- Available NEs
- (Optional) Job Comments
- Tag Name
- Time (time zone)



Note The time zone can be Greenwich mean time (GMT), a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box.

Click **Finish** to initiate the memory backup procedure.

The configuration file is copied to the `/opt/CiscoMGMServer/admin/nodename/MGX-timestamp-bkp.cfg` file.



Note If User Specified is chosen and **hello** is entered for the tag name, the filename is `MGX-hello-YYYYMMDDHHMM-backup.cfg` where `YYYYMMDDHHMM` is the backup date, consisting of:

YYYY—Four-digit year
 MM—Two-digit month
 DD—Two-digit day
 HH—Two-digit hour (in 24-hour format)
 MM—Two-digit minute

The length of a filename including a user specified name should not exceed 40 characters. If a long filename is chosen, it will be truncated to 15 characters.

After scheduling the backup, look at the Job Monitor Table (**Administration > Job Monitor**) to see the job status. If the job fails, the Additional Information field in the Job Monitor Table provides extra information.

If a memory backup job fails, it raises an EMS alarm. All prior memory backup failure EMS alarms on an NE are cleared under the following conditions:

- After a successful memory backup operation on the NE
- When the operational state of the NE changes to Out of Service

Table 5-15 Memory Backup Dialog Box Descriptions

Field	Description
NE Model	Select the NE type that you want to back up. The type you select determines the NEs that are displayed in the Network Elements area.
Available NEs	Use the Add and Remove buttons to move the NEs that you want to back up to the Selected NEs list, or to remove NEs from the list.
Job Comments (Optional)	Enter comments about the backup, if needed.

Table 5-15 Memory Backup Dialog Box Descriptions (continued)

Field	Description
Tag Name	Add a tag to the system-generated filename. If you select System Default, no tag name is added. If you select User Specified, you can enter a tag name. The length of a filename including a user specified name should not exceed 40 characters. If a long filename is chosen, it will be truncated to 15 characters.
Time (time zone)	Set a time for the backup. Click Now to begin backup immediately, or click At Time and specify when to begin backup, in 5-minute increments. Note The time zone can be Greenwich mean time (GMT), a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box.

5.3.2.2 Restoring Memory

**Note**

[Table 5-16](#) describes the fields in the Memory Restore dialog box.

Use the Memory Restore dialog box to restore provisioning and configuration information stored in the flash memory of an NE. (This information is backed up by using the Memory Backup dialog box.)

Step 1 In the Domain Explorer tree, select an MGX8880, or an MGX 8850 NE that is assigned an In Service or Under Maintenance operational state.

**Note**

Run the Memory Restore procedure *one* NE at a time.

Step 2 With the NE selected, choose **Administration > Memory Restore**.

Step 3 The Memory Restore dialog box appears. Enter the following information (see [Table 5-16](#) for more details):

- NE Model
- Network Elements (select only one)
- (Optional) Job Comments
- Source
- Time (time zone)

Step 4 Click **Finish** to initiate the memory restore procedure.

To view the results of the memory restore operation, open the Job Monitor Table. For information about the Job Monitor Table, see section [5.2.6 Monitoring Scheduled Tasks](#), page 5-23.

Table 5-16 Memory Restore Dialog Box Descriptions

Field	Description
NE Model	Select the NE model that you want to restore. The model you select determines the NEs that are displayed in the Network Elements field.
Network Elements	Use the Add and Remove buttons to move the NE that you want to restore to the Selected NE list. You can run the Memory Restore procedure for only one NE at a time.
Job Comments (Optional)	Enter comments about the restore procedure, if needed.
Source	Specify the location of the backup file that you want to use to restore the NE: <ul style="list-style-type: none"> Click Local to browse a local client directory for the backup file. Click Server to restore the file from the Cisco MGM server. The files shown are in the directory <code>/opt/CiscoMGMServer/admin/nodename</code>. <p>Note The Server radio button is not active unless a file exists in that directory.</p> <ul style="list-style-type: none"> Remote option is grayed out
Time (time zone)	Set a time for memory restore. Click Now to begin memory restore immediately, or click At Time and specify when to begin memory restore, in 5-minute increments. <p>Note The time zone can be Greenwich mean time (GMT), a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box.</p>

5.3.3 Changing IP Addresses for NEs

In Cisco MGM, the IP address field for an NE is read-only, and cannot be modified. If a user changes the IP address on the MGX switch, Cisco MGM receives traps and updates the IP address on the clients and in the database.

5.3.4 Viewing and Modifying the Server Configuration

The Control Panel window shows the Cisco MGM client and server configuration and allows modification of the configuration. Certain modifications take effect immediately and change the active server configuration. Other changes take effect when the server is restarted.

The different property sheets within the Control Panel window allow you to start or stop performance monitoring services and NE services by NE type. Also use the Control Panel to start or stop Cisco MGM GateWay/CORBA services. Only Cisco MGM users who are logged in as SuperUser or SysAdmin can access the Control Panel. In the Domain Explorer, choose **Administration > Control Panel** to view the Control Panel.

The following are listed in the Control Panel:

- UI Properties—Configure application-specific parameters.
- Security Properties—Configure Cisco MGM security parameters and specify usernames and passwords for all the NEs.

- Recovery Properties—View a list of servers that clients will log into if access to the primary server is disrupted and view a list of critical services that the server monitors.
- Database Properties—View database configuration, pruning time periods, and information that the server uses to log into the Oracle database.
- Alarm Configuration Properties—View threshold and non-threshold parameters.
- Error Log Properties—View configuration parameters about error information that the server records.
- NE Service—Select an NE type and view and update server configuration, which includes port information, timing parameters, maximum number of administrative tasks, and NE backup parameters.
- PM Service—Select an NE type and view and modify PM Configuration settings and PM Collection Parameters for the particular NE.
- GateWay/CORBA Service—Stop, start, or configure parameters for the GateWay/CORBA service.

**Note**

The NE Service and GateWay/CORBA services can take up to 60 seconds to initialize after the GUI status has changed to indicate that the service is up. The status is an indication of the successful initiation of the service startup, not successful initialization.

5.3.5 Setting Up Session Recovery

Administrators can list the servers that clients will log into if access to the primary server is disrupted. To set up session recovery:

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
- Step 2** Click **Recovery Properties** to open the Recovery Properties sheet.
- Step 3** Click the Session Recovery tab. [Table 5-17](#) describes the fields within the Session Recovery tab.
- Step 4** In the Session Recovery area, specify the following:
- Wait Time—Enter the number of seconds that the client waits before attempting to log into a backup server.
 - No. of Retries—If the first backup server is not available, enter the number of times that the client should retry logging back before connecting to the next server on the list.
- Step 5** In the Server List area is a list of servers that client will log into if access to the primary server is disrupted. Click **Add** if you want to add a server to the list. Click **Remove** if you want to remove a server from the list.
-

**Note**

If access to the primary server is disrupted, the client tries to log back into the primary server by default. If the client cannot log back into the primary server, and if the server list contains server names, the client tries to log into each backup server in the order listed until the last server in the list is reached, or until the client successfully logs into a server.

Table 5-17 Recovery Properties—Session Recovery Tab

Field	Description
Wait Time	If disruption to the primary Cisco MGM server occurs, the Wait Time field provides the number of seconds the client waits before attempting to log into the backup server.
No. of Retries	If the first backup Cisco MGM server is not available, this field provides the number of times the client should retry logging in before moving to the next server on the list.
Server List	Lists the Cisco MGM servers that Cisco MGM clients will log into if access to the primary Cisco MGM server is disrupted. The Add button adds a Cisco MGM server to the Cisco MGM server list. The Remove button removes a Cisco MGM server from the list. If access to the primary Cisco MGM server is disrupted, the Cisco MGM client tries to log back into the primary server by default. If the Cisco MGM client cannot log back into the primary server, and if the server list contains server names, the client tries to log into each backup server in the order listed until the last server in the list is reached, or until the client successfully logs into a server.

5.3.6 Changing the Server IP Address when Cisco MGM and Oracle Are on the Same Server



Note

You will need to update the configuration files after changing the server IP address, see [5.3.6.1 Updating the Configuration Files after Changing the Cisco MGM Server IP Address](#).

To change the IP address of a standalone Cisco MGM server with a single IP interface when Cisco MGM and Oracle are on the same server:

-
- Step 1** Log into the Cisco MGM server as the root user.
- Step 2** Enter the following command to shut down the Cisco MGM server:
- ```
mgms-stop
```
- Step 3** Enter the following commands to shut down Oracle:
- ```
su - oracle
sqlplus ctmanager/mgm123!
SQL> connect sys/change_on_install as sysdba
SQL> shutdown immediate;
SQL>exit
```
- Step 4** Complete the following:
- Enter the following command to change the IP address in the `/etc/netmasks` file:

```
#vi /etc/netmasks
```
 - Enter the following command to change the IP address in the `/etc/hosts` file:

```
# vi /etc/hosts
```

- c. Enter the following command to change the IP address in the `etc/hostname.xxx` file, where `xxx` is the IP interface that is defined in the Solaris server:

```
# vi /etc/hostname.xxx
```

- d. Enter the following command to change the default router file, if required:

```
# vi /etc/defaultrouter
```

- e. Enter the following command to change the subnet mask on the Cisco MGM server:

```
# vi /etc/netmasks
```

Step 5 Complete the following application-level steps:

- a. Enter the following command to change the IP address in the Oracle listener file:

```
# vi /oraclesw9i/producl/9.2/network/admin/listener.ora
```

- b. Enter the following command to change the IP address in the Oracle tnsnames file:

```
# vi /oraclesw9i/producl/9.2/network/admin/tnsnames.ora
```

- c. Enter the following command to change the IP address in the Cisco MGM server configuration file:

```
# vi /opt/CiscoMGMServer/cfg/CTMServer.cfg
```



Note The default directory `/opt/CiscoMGMServer` may have been changed during installation of the Cisco MGM server.



Note Make sure to change all IP addresses where they are referenced.

Step 6 Enter the following commands to halt and reboot the Cisco MGM server:

```
# sync;sync;halt
OK boot -r
```

5.3.6.1 Updating the Configuration Files after Changing the Cisco MGM Server IP Address

If you change the Cisco MGM server IP address (as shown in section [5.3.6 Changing the Server IP Address when Cisco MGM and Oracle Are on the Same Server, page 5-41](#)) you must replace the old IP address with the new IP address in the configuration files shown in [Table 5-18](#). Use a standard UNIX text editor such as `vi` to update the files. Changes in the configuration files take effect after rebooting the server.

Table 5-18 Configuration Files that Require Updating

Filename	Location
UNIX Configuration Files	
hosts	/etc
netmasks	/etc
defaultrouter	/etc

Table 5-18 Configuration Files that Require Updating (continued)

Filename	Location
Oracle Configuration Files	
tnsnames.ora	/oraclesw9i/product/9.2/network/admin
listener.ora	/oraclesw9i/product/9.2/network/admin
Cisco MGM Server Configuration File	
MGMServer.cfg	/opt/CiscoMGMServer/cfg

**Note**

The default directory /opt/CiscoMGMServer may have been changed during installation of the Cisco MGM server.

5.3.7 Viewing and Modifying Server Configuration Information

The NE Service Properties pane allows you to view and update Cisco MGM server configuration information, which includes port information, timing parameters, and network element (NE) backup parameters. All server configuration changes take effect when you save them, with the exception of changes to the Cisco MGM server port. Port information changes require that you restart the Cisco MGM server before the change takes effect. The NE Service Properties pane has three tabs:

- NE AutoBackup—Allows you to configure automatic NE backup parameters (See [5.1.3.9 Configuring Automatic NE Backup Parameters](#))
- NE Manual Backup—Allows you to configure manual NE backup parameters (See [5.1.3.8 Configuring Manual NE Backup Parameters](#))

5.3.8 Restoring Server Configuration Files

To restore the server configuration files:

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

Step 2 On the command line, enter the following:

```
cd/opt/CiscoMGMServer/bin
./restore_config.sh <backup file doc> <log dir> <ISHA>
```


**Note**

The default directory /opt/CiscoMGMServer may have been changed during installation of the Cisco MGM server.

**Note**

If the server is an HA server, the ISHA value is 1. If the server is not an HA server, the ISHA value is 0.

Table 5-19 Field Description for the NE Service Properties

Field	Description
Service Status	Displays the current status of the service: Active or Not Active.
Service Control	Allows you to stop or start a process. Notice that the Service Control button toggles between Activate and Deactivate, and that the Service Status field changes accordingly.
Error Level	<p>Allows you to choose the error level for alarms on the selected NE to include in the Error Log (Critical, Major, Minor, Informational, Debug, or Trace). Critical, major, minor, and informational errors are logged to the database; trace and debug information is logged to a log file.</p> <p> Caution Cisco MGM performance will degrade significantly if the trace or debug option is left on. All operations will slow down and you may lose alarm and event notifications. Use trace or debug only when troubleshooting with a customer support engineer.</p>
Threshold	Displays the number of NEs that will be serviced by one instance of the NE service.

5.3.9 Initializing the Node Resync Process

To initialize the node resync process for a node, complete the following procedure:

-
- Step 1** In the Diagnostic Center, from the Hierarchy pane:
- Double-click or drag the network to the right-hand pane to display the diagnostics at the node level and select a node.
 - Double-click or drag the node to the right-hand pane to display the diagnostics at the node level.
- By default, the **Diagnostics** tab is selected. The Node Diagnostics window is displayed.
- Step 2** Choose **Level 1** or **Level 2** options from the Node Resync pane:
- **Level 1**—Resolves inconsistencies between the switch and equipment manager as well as between equipment manager and segment tables.
 - **Level 2**—Retrieves the full connection file from the switch and resolves inconsistencies between the equipment manager and equipment manager caches as well as between equipment caches and databroker caches. It also resolves inconsistencies between equipment manager and segment tables. This option is automatically used if the number of inconsistencies is large.
- Step 3** Click **Resync** to begin the node resync process.
- Step 4** Verify the results of the node resync process from the **Node Resync Result** area.
-

5.3.10 Configuring Application-Specific Parameters



Note

Table 5-20 describes the fields in the User Interface Properties pane.

The User Interface (UI) Properties pane allows you to configure application-specific parameters. Specifically, you can do the following:

- **Fault Management**—Specify automatic or manual alarm acknowledgement, overwrite alarm notes, and un-acknowledge alarms (for more details, see [Chapter 9, “Managing Faults”](#).)
- **Domain Management**—Specify how long node names are truncated within Network Maps (for more details, see [Chapter 4, “Building the Network”](#).)

From the Domain Manager, choose **Administration > Control Panel**. In the Control Panel window, click **UI Properties** to open the User Interface Properties pane.

Table 5-20 User Interface Properties Field Descriptions

Field	Description
Fault Management	<ul style="list-style-type: none"> • Alarm Acknowledgement—Allows you to specify automatic or manual alarm acknowledgement in the Alarm Browser window. If you choose manual alarm acknowledgement, you must manually acknowledge alarms. Cleared alarms move from the Alarm Browser to the Alarm Log. If you choose automatic alarm acknowledgement, the Cisco MGM server automatically acknowledges alarms when they are cleared and moves them from the Alarm Browser to the Alarm Log. Before alarms move to the Alarm Log, they must be both cleared <i>and</i> acknowledged. <p>Note You can still manually acknowledge alarms in automatic acknowledgement mode.</p> <ul style="list-style-type: none"> • Overwrite Alarm Notes—Enables or disables the ability to overwrite alarm notes created by another user. • Alarm Un-Acknowledgement—Enables or disables the ability to unacknowledge alarms that have been acknowledged.
Domain Management	Allows you to specify how node names longer than 25 characters are truncated in the Network Map. If a string is longer than 25 characters, the first 22 characters display followed by an ellipsis (...). You can choose to truncate the first or last characters of the node name.

5.3.11 Using UNIX-Level Scripts

The following UNIX shell scripts are provided to perform administrative functions from the command line on the Cisco MGM server:

- mgms-start
- mgms-abort
- mgms-stop
- mgms-stop-service
- showmgm

- `getinfo.sh`
- `prune_auditlog.sh`
- `prune_errlog.sh`
- `prune_audittrail.sh`
- `prune_fm.sh`
- `prune_pm.sh`
- `prune_ne.sh`
- `prune_server_monitor.sh`

These scripts should normally be run as root. However, Cisco MGM facilitates running these scripts as non-root users using `sudo`. During the Cisco MGM server installation, the setup program prompts you to specify the name of the UNIX group to which you want to assign administrator privileges. By default, this group is set to `root`. If you specify a group other than `root`, the setup program verifies that the UNIX group exists on the system and adds entries to the `/etc/sudoers` file for each of the commands listed above. As such a UNIX user who is a member of the specific group can run the commands using `sudo`. `Sudo` is bundled with Cisco MGM and is located in `/opt/CiscoMGMServer/admin/sudo/`. In order to use the `sudo` bundled with Cisco MGM the following command should first be run.

**Note**

The default directory `/opt/CiscoMGMServer` may have been changed during installation of the Cisco MGM server.

Further details about the use and configuration of `sudo` are provided in the Cisco MGM Installation Guide.

5.4 How Do I Manage the Network Software?

Cisco MGM provides a mechanism to download software image from the Cisco MGM server onto the MGX8880 switch. When the software download is scheduled, an FTP connection is opened to the switch using the IP address, User ID and password. The software image is downloaded to the `FW` directory. The FTP connection is closed and Cisco MGX processes resume.

**Note**

There is no support for downloading images from an external TFTP server. Software images can be downloaded only if they are locally present on the Cisco MGM server.

When the software image is downloaded, you can use the following commands at the CLI:

- **`dsprev`** to display the image on the switch
- **`loadrev`** to load the image on the switch
- **`setrev`** to set the image on the switch
- **`runrev`** command to activate the image on the switch.

Follow the procedures described in this section to download new or modified images to NEs:

- [5.4.1 Downloading Software Images](#)

5.4.1 Downloading Software Images



Note [Table 5-21](#) describes the fields in the Download Software Dialog.



Note If a software download has a status of Queued, and if it has a task in the running list, the download cannot be canceled.



Caution If you mark an NE as an Out of Service while a software download is in progress on that NE, the software download might not complete successfully.

To download software images to NEs, Cisco recommends that DCN bandwidth be 56 kbps or higher. If DCN bandwidth is less than 56 kbps, software download might take an extended period of time. Performing software downloads in parallel increases the length of time by a multiple of the number of NEs targeted.

Step 1 In the Domain Explorer tree, select a management domain or group that contains NEs that are assigned an In Service or Under Maintenance operational state. Alternatively, select an NE that is assigned an In Service or Under Maintenance state.



Note Only one software download can occur on a specific NE at any given time.

Step 2 Choose **Administration > Software Download**. The Software Download dialog box appears. See [Figure 5-4](#).

Step 3 Enter the following information:

- NE Model
- Network Elements
- Job Comments
- Source
- Time



Caution If the Cisco MGM client and server run on the same machine and thus the Local source directory is the same as the default destination directory, an error message is generated. To retrieve the software image selected from the Local source directory, navigate to the appropriate path and restore it from the *<software image name>.old* file.

- Step 4** Click **Finish** to initiate the software download to the standby memory on the NE.
- Step 5** Cisco MGM stores two software versions: active and standby. When you download software, it is saved as the standby version.

Figure 5-4 Software Download Window

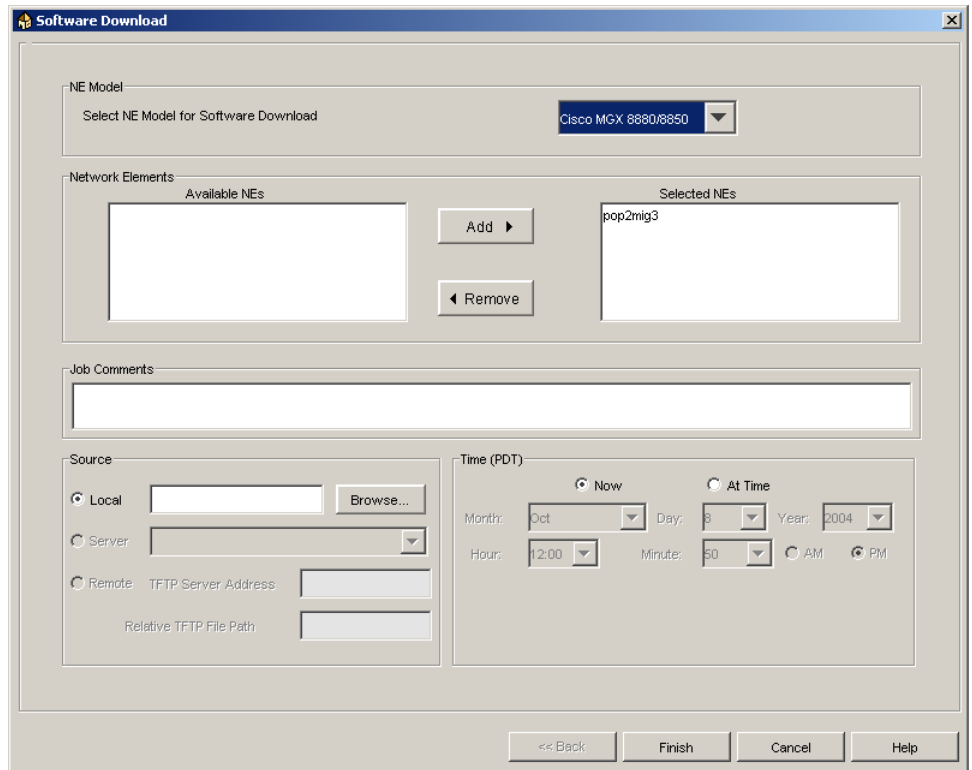


Table 5-21 Field Description for the Software Download Dialog

Field	Description
NE Model	Select the NE type to which you want to download software. The type you select determines the NEs that are displayed under Network Elements.
Network Elements	Use the Add and Remove buttons to move NEs to the Selected NEs list or remove NEs from the list. Software will be downloaded to NEs in the Selected NEs list.
Job Comments	Enter comments about the software download (optional).

Table 5-21 Field Description for the Software Download Dialog (continued)

Field	Description
Source	Specify the location of the software: <ul style="list-style-type: none"> • Local allows you to select an image on the current client system. • Server allows you to select an image on the Cisco MGM server to which your client is connected. • Remote option is grayed out.
Time (time zone)	Set a time for the download. Click Now to begin download immediately, or click At Time and specify when to begin download, in 5-minute increments. <p>Note The time zone can be Greenwich mean time (GMT), a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box.</p>

5.5 How Do I Manage Redundancy and Failover?

This section contains the following information:

- [5.5.1 Configuring Card Redundancy](#)

5.5.1 Configuring Card Redundancy

These tasks are used to configure card redundancy:

- [5.5.1.1 Adding Redundancy](#)
- [5.5.1.2 Modifying a Card for Redundancy](#)

Card redundancy uses a secondary card of the same type to serve as a standby card and takes over if the active card fails. Automatic protection switching (APS) on a SONET line can be combined with front card redundancy. The ATM link is protected from both line and card failures.

You can setup card redundancy at the shelf level.

5.5.1.1 Adding Redundancy

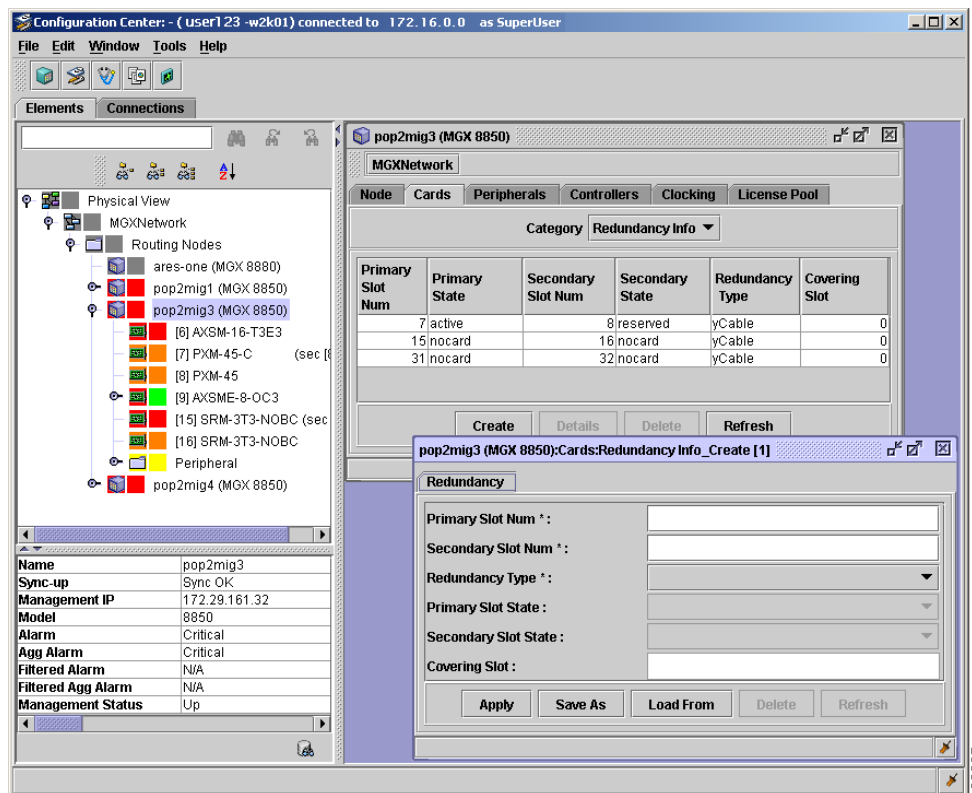
By adding redundancy, you can link two slots to support card-level redundancy for a pair of service modules. A redundant pair consists of a primary slot and a secondary slot. Both cards must be in the active state for you to configure redundancy. After configuration, the secondary service module goes into the standby state.

To add redundancy:

-
- Step 1** In the Domain Manager, select the node and choose **Configuration > MGX880/8850 MG > Configuration Center** to display the Configuration Window for Elements.
 - Step 2** Click the **Cards** tab to display a summary report of all the cards that are installed on the node.
 - Step 3** Choose **Redundancy Info** from the **Category** drop-down arrow to display the redundancy status for the node.
 - Step 4** Click **Create** to display the Redundancy Configuration window. See [Figure 5-5](#).

- Step 5** Enter the slot number of the Primary module in the redundant configuration in the **Primary Slot Num** field.
- Step 6** Enter the slot number of the Secondary module in the redundant configuration in the **Secondary Slot Num** field.
- Step 7** Choose one of the following redundancy options for the Primary module from the **Redundancy Type** drop-down arrow:
- **yCable**—specifies a 1:1 (y cable) redundancy configuration for a yCable. For the **yCable** option, only one module is used and acts as the backup for the other.
 - **oneToN**—specifies a 1:N redundancy configuration for oneToN. For the **oneToN** option, only one module (secondary) is used and acts as the backup for other primary modules.
- Step 8** Click **Apply** to add redundancy.

Figure 5-5 Redundancy Information Window



5.5.1.2 Modifying a Card for Redundancy

To modify a card for redundancy:

- Step 1** In the Domain Manager, select the node and choose **Configuration > MGX880/8850 MG > Configuration Center** to display the Configuration Window for Elements.
- Step 2** Click the **Cards** tab to display a summary report of all the cards that are installed on the node.

- Step 3** Choose **Redundancy Info** from the **Category** drop-down arrow to display the redundancy status for the node.
- Step 4** Select the card from the list of redundant cards.
- Step 5** Click **Details** to display the Redundancy Configuration window. See [Figure 5-5](#).
- Step 6** Enter the slot number of the Secondary module in the redundant configuration in the **Secondary Slot Num** field.
- Step 7** Choose one of the following redundancy options for the Primary module from the **Redundancy Type** drop-down arrow:
- **yCable**—specifies a 1:1 (y cable) redundancy configuration for a yCable. For the **yCable** option, only one module is used and acts as the backup for the other.
 - **oneToN**—specifies a 1:N redundancy configuration for oneToN. For the **oneToN** option, only one module (secondary) is used and acts as the backup for other primary modules.
- Step 8** Click **Apply** to modify the card for redundancy.
-

5.6 Which Ports Are Reserved in Cisco MGM?

The Cisco MGM server communicates with the managed network via the data communication network (DCN) using the CORBA protocol.



Note

If there is a firewall between the Cisco MGM server and the NE, a static CORBA port needs to be assigned manually. This port can then be opened on the firewall.



Caution

Reserved ports are required for the Cisco MGM server to communicate with NEs, the GUI, or other northbound gateways. Care must be taken when changing any reserved port in Cisco MGM, as a change could mean that communication is lost.

This section includes the following information:

- [5.6.1 Client-Server Communication Protocols](#)
- [5.6.2 Ports between the Cisco MGM Server and Clients](#)
- [5.6.3 Ports between the Cisco MGM Server and MGX Switches](#)
- [5.6.4 Changing the Cisco MGM Server Port](#)

5.6.1 Client-Server Communication Protocols

Cisco MGM uses the following protocols for client-server communication:

- CORBA
- JMOCO (Cisco Proprietary TCP/IP-based request/response protocol)
- SSH or Telnet
- Java Database Connectivity (JDBC)

5.6.2 Ports between the Cisco MGM Server and Clients

Table 5-22 lists the ports that the Cisco MGM server uses to communicate with the Cisco MGM clients.

Table 5-22 Cisco MGM Server and Client Ports

Module or Protocol	Port
Apache HTTP port	8051
CORBA IIOP listener port on CTM server	Dynamic
CORBA naming service	14005
CORBA notification service	Dynamic
Database listener port	1521 (configurable)
Internal process-to-process communication ports	9000 to 9011
JMOCO port	27613 (configurable)
JMS web server	8033
JNDI port	1099
Orbix ports	3075, 3079, 3094
RMI Registry port	19999
RTM Proxy port	8161
SNMP command port	161 Note Port 161 is used only for communication between SNMP-managed NEs and the CTM server, not for communication between the CTM client and server.
SNMP trap forwarding port	8765 (configurable)
SNMP trap port	162 Note Port 162 is used only for communication between SNMP-managed NEs and the CTM server, not for communication between the CTM client and server.
SSH port	22
Telnet port	23
UDP port to receive traps	2500
Web services port	1551

5.6.3 Ports between the Cisco MGM Server and MGX Switches

Table 5-22 lists the ports that the Cisco MGM server uses to communicate with the Cisco MGX switches.

Table 5-23 Cisco MGM Server and MGX Switches

Module or Protocol	Port
Daytime port	13
SSH port	22
Telnet port	23
UDP port to receive traps	2500

5.6.4 Changing the Cisco MGM Server Port

Use the NE Service Properties pane to change the TCP port number of the Cisco MGM server. All Cisco MGM clients use the JMOCO port to connect to the Cisco MGM server. See Table 5-22 for detailed information on the JMOCO port.

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
- Step 2** In the Control Panel window, click **NE Service** to open the NE Service Properties pane. Click the **NE Poller** tab.
- Step 3** Change the server port in the Cisco MGM Server Port field. The server port in the Active column displays the current port. The server port in the After Restart column displays the port that is active after the server is restarted.
- Step 4** Click **Save**. Changes to this parameter take effect only after the server is restarted.
-

5.7 How Do I Export Information in Tables?

You can export fault, performance, configuration or administration information from a table within Cisco MGM to a flat file. The options to export information in tables to a text file or an HTML file are available from the following windows:

- Alarm Browser
- Alarm Log
- Audit Log
- Cisco MGM Users
- Domain NE Table
- Equipment Inventory Table
- Error Log
- Job Monitor

- Service Monitor
- Supported NE Table

Most Cisco MGM tables support an export function to export the table contents to a flat file. It is possible to select the separator as comma, tab, or a user specified character. Other options include the ability to check for the separator in the exported data. All rows in the active page of the selection can be exported or only selected rows.

Some Cisco MGM tables can return large numbers of rows. To support large tables Cisco MGM provides a paging feature. If more than 1000 rows of data are returned, data is grouped in pages of up to 1000 rows. It then possible to page forward and back to view the entire set of data.

The following sections discuss how to export information in tables to a text file or an HTML file:

- [5.7.1 Exporting Data to a Text File](#)
- [5.7.2 Generating an HTML Report](#)
- [5.7.3 Printing an HTML Report](#)

5.7.1 Exporting Data to a Text File

To export data to a text file:

-
- Step 1** In the Domain Explorer tree, select the management domain, group, or NE node.
 - Step 2** Open a window under the File, Fault, or Administration menu for the selected node. See the options listed in [5.7 How Do I Export Information in Tables?](#)
 - Step 3** Within the table, click the **Export Data to File** tool (or choose **File > Export**). The Export dialog box appears.
 - Step 4** In the Export dialog box, specify whether to export data in comma-separated value format, tab-separated value format, or another user-specified form.
 - Step 5** (Optional) To export only the selected row(s), check the **Export selected row(s) only** check box.
 - Step 6** Specify a location for the file in the **Export to file** text box. Or, click **Browse** to browse for a destination location. (The default directory is C:\Cisco\MediaGatewayManagerClient\exports or /opt/CiscoMGMClient/exports.)
 - Step 7** Enter a filename and click **OK** to export the data to the file.
-

5.7.2 Generating an HTML Report

Many Cisco MGM tables have an HTML Report tool for generating an HTML report on selected fault, performance, configuration, or administrative data. To generate an HTML report:

-
- Step 1** In the Domain Explorer tree, select the management domain, group, or NE node.
 - Step 2** Open a window under the File, Fault, or Administration menu for the selected node. See the options listed in [5.7 How Do I Export Information in Tables?](#)
 - Step 3** In the table, click the **Generate HTML Report** tool (or choose **File > HTML Report**). The HTML Report dialog box appears.

Step 4 In the HTML Report dialog box, select either of the following:

- Selected row(s)—Export only the selected rows.
- All rows in current page—Export all rows in the table.

A maximum of 1000 rows per page can be exported.



Note To save more than 1000 rows of data, export them to a text file. For information about exporting to a text file, see section [5.7 How Do I Export Information in Tables?](#), page 5-53.

Step 5 Click **OK** to generate the HTML report. The report is saved automatically on the client system. (The default directory is C:\Cisco\MGMClient\reports or /opt/CiscoMGMClient/reports.)

5.7.3 Printing an HTML Report

To print a Cisco MGM HTML report, use the default browser Print option. To print a Cisco MGM HTML report:

Step 1 Generate the HTML report. See section [5.7.2 Generating an HTML Report](#), page 5-54.

Step 2 Navigate to the directory where the HTML report is saved on the client system. (The default directory is C:\Cisco\MGMClient\reports or /opt/CiscoMGMClient/reports.) Double-click the report to be printed.

Step 3 The default browser displays the HTML report. Use the browser Print option to print the report.
