

Carrier VoIP

IEMS Overview

Document status: Standard
Document version: 04.02
Document date: 20 October 2006

Copyright © 2006, Nortel Networks
All Rights Reserved.

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners.

Contents

IEMS Overview	7
System requirements	8
Comparison of the Java Web Start and Web Client interfaces	11
Using Java Web Start Client	14
Logging in to the IEMS server	15
Configuring login settings	17
Overview of the Java Web Start Client interface	18
Launching the IEMS Java Web Start Client	21
Launching applications from IEMS	23
Launching element managers	32
Launching applications for APS Manager	33
Launching applications from CICM Manager	34
Launching Core Element Manager	36
Launching a CEM Commissioning Manager CLI	37
Launching applications for CS 2000 Core Manager	39
Launching applications for FPM	40
Launching applications for GWC Manager	42
Launching applications for MCS Manager	43
Launching applications for MG 9000 Manager	46
Launching applications for MDM	47
Launching the SAM21 Manager	51
Launching UAS Manager	52
Launching applications for an EMS platform	53
Launching applications for an MDM platform	54
Launching applications for an SDM platform	55
Launching an application for an SPFS platform	56
Launching EMS applications	58
Launching applications for APS	59
Launching the Certificate Manager GUI	60
Launching an LMM application	62
Launching applications for an NPM application	63
Launching an OSSGate application	64
Launching the CLI for a QoS Collector application	65

Launching the CLI for an SBRM application	66
Launching a TMM application	67
Launching applications for network elements	68
Launching the CLI for the Call Agent platform	69
Launching a MAPCI Session for Call Agent Core and CS 2000 Core	70
Launching a CICM NE	71
Launching the Client Session Monitor	72
Launching applications for an Ethernet Routing Switch 8600 NE	73
Launching applications for a GWC NE	75
Launching MAS Manager	77
Launching applications for an MCS/CSE and Media Portal NE	80
Launching applications for the MG 3200 NE	82
Launching applications for an MG 7480/15000/20000 and MSS 15000 NE	83
Launching applications for an MS 2000 NE	87
Launching applications for a SAM21 NE	88
Launching the Server Security Manager	90
Launching applications for Session Server Trunks	92
Launching applications for a STORM NE	94
Launching the CLI for a UAS NE	95
Launching the UNEM browser for UNEM	96
Launching applications for a UMUX Manager	98
Launching applications for a USP NE	99
Using IEMS diagnostics	101
Checking the status of IEMS modules	102
Configuring IEMS diagnostics parameters	110
Running a ping test on the GWC network element or SPFS platform	112
Running a traceroute on the GWC network element or SPFS platform	116
Overview of Core Element Manager integration with IEMS	119
Overview of high availability & co-residency	126
Reconnecting Java Web Start client with the server	127
Replicating data for high availability	128
Using Java Web Start Client features	129
Viewing context sensitive help	130
Configuring the look and feel of Java Web Start Client	131
Using the broadcast message feature of Java Web Start Client	132
Showing or hiding the toolbar in Java Web Start Client	133
Using the IEMS tree	134
Using the LED indicator	140
Setting the theme for Java Web Start Client	141
Using custom view filtering criteria	142
Sorting data in Java Web Start Client	144
Description of IEMS operational measurements	146
Logging out of the Java Web Start client	154

Overview of the Web Client interface 155
Launching the IEMS Web Client 158
Personalizing the Web Client 159
Logging out from the Web Client 160
Troubleshooting tips 161
Configuring Domain Name Service on an SPFS-Based Server 164

IEMS Overview

The Integrated Element Management System (IEMS) client interface is the interface to the Carrier Voice over IP Operations and Maintenance Center Platform. This section provides an overview of the interfaces and describes the basic features of the IEMS client.

New in this release

Feature changes

These are the following feature changes in this release.

- IEMS Call Server 2000 SIP integration
This feature integrates the new SSLines platform SIP applications. It integrates the management of the fault and performance interfaces of the SSLines platform applications. This feature also includes rebranding changes to the existing Session Server managed object.
- IPsec Certificate Manager Support
This feature integrates the Certificate Manager application with IEMS to provide the following capabilities from the IEMS GUI:
 - Add the Certificate Manager as an application to the IEMS topology.
 - View Certificate Manager alarms on IEMS.
 - Launch the Certificate Manager GUI client from IEMS using single sign-on.
- MS2000 IPsec Configuration via IEMS
This feature adds IPsec and IKE configuration capabilities to the MS2000 node configuration tool. This allows the craftsperson to enable IPsec for secure messaging between the IEMS and MS2000 as well as configure the IPsec and IKE parameters necessary for the MS2000 to securely send and receive messages to and from the GWC.
- MG 3200 integration
This feature adds support for the MG 3200 into the IEMS. It adds the capability to add a MG 3200 to the IEMS topology, to view faults, to view performance measurements, and to perform configuration of a MG 3200.

System requirements

This section details the hardware and software system requirements for IEMS server and IEMS client.

IEMS hardware and software requirements

Category	Minimum requirements
IEMS server requirements	
Initial deployment	<p>IEMS can reside on the following platforms and configurations:</p> <ul style="list-style-type: none"> • Standalone (IEMS on SPFS) <ul style="list-style-type: none"> — on a single N240 (simplex) 4G — on a dual N240 (HA) 4G — on a single T1400 (simplex) 4 Gig only • Co-residency (CMT and IEMS on SPFS) <ul style="list-style-type: none"> — on a single N240 (simplex) 4G — on a dual N240 (HA) 4G <p>This release is compliant with European Union Environmental Directives (EUED - RoHS and WEEE).</p>
IEMS client requirements	
Processor	750 MHz Pentium processor or greater
Memory	1 GB RAM
<p>Note 1: Disk requirements related to Oracle DB, NDS DB, log storage, IEMS performance output CSV/XML data files are not include in these values.</p> <p>Note 2: These requirements are targeted at using the Web Start client. The IEMS also supports the HTML client which requires less resources.</p> <p>Note 3:If Mozilla is the default browser in the Microsoft Windows platform, the Mozilla browser does not always come to the foreground when an application is launched from the IEMS Client.</p> <p>Note 4:Java TM Web Start 1.4.2_08 is included with the Java TM 2 Runtime Environment version 1.4.2_08. This can be downloaded from the IEMS server. Refer to http://your_iems_server_hostname.</p>	

Category	Minimum requirements
Storage (see Note 1)	Approximately: 311 MB for the Security Server 106 MB for the IEMS application server 800 MB for CEM
Monitor	SVGA monitor or greater (16 bit colors or higher) Recommended: 1024x768 or higher
Network connection	For Java Web Start Client: 100BT or higher For Web Client (HTML): 64 kbps or higher
Operating system	Microsoft Windows 2000/XP or later Sun Solaris 2.8/2.9 to current
Internet browser for an IEMS client on a Microsoft Windows operating system	Netscape 6.2 to current Microsoft Internet Explorer 6 SP1 to current
Internet browser for an IEMS client on a Sun Solaris operating system (see Note 3)	Netscape 6.2 to current Mozilla 1.4 to current
Java TM 2 Run Time Environment (see Note 4)	Requires JRE version 1.4.2_08
Software requirements to launch applications from IEMS Web Start Client	
CS2K Management tools	Requires JRE version 1.4.2_08
ERS 8600	Requires the installation of the Device Manager application.
IEMS Web Start client	Requires JRE version 1.4.2_08
MAS	Requires the installation of the Microsoft Remote Desktop Connection Software application on the client PC. The MAS client is supported on the Microsoft Windows OS only.
<p>Note 1: Disk requirements related to Oracle DB, NDS DB, log storage, IEMS performance output CSV/XML data files are not include in these values.</p> <p>Note 2: These requirements are targeted at using the Web Start client. The IEMS also supports the HTML client which requires less resources.</p> <p>Note 3: If Mozilla is the default browser in the Microsoft Windows platform, the Mozilla browser does not always come to the foreground when an application is launched from the IEMS Client.</p> <p>Note 4: Java TM Web Start 1.4.2_08 is included with the Java TM 2 Runtime Environment version 1.4.2_08. This can be downloaded from the IEMS server. Refer to http://your_iems_server_hostname.</p>	

Category	Minimum requirements
MCS/MCP System Management console for MCS Manager	Requires JRE version 1.4.2_09 Requires a Microsoft Windows platform-based client workstation
MCS client	Requires JRE version 1.4.2_09 The client launch requires the installation of the MCS client application on the client PC. The MCS client is supported on Microsoft Windows only.
Multiservice Data Manager (MDM)	In Microsoft Windows, MDM requires the installation of Exceed to launch the legacy Motif tools. IEMS also supports launching a Java MDM operator client GUI from the Java Web Start client.
Legacy MDM tools	In Microsoft Windows, requires the installation of Exceed.
NPM	Requires JRE version 1.4.2_08
SAM21 manager	Requires JRE version 1.4.2_08
USP	Requires JRE version 1.4.2_08
<p>Note 1: Disk requirements related to Oracle DB, NDS DB, log storage, IEMS performance output CSV/XML data files are not include in these values.</p> <p>Note 2: These requirements are targeted at using the Web Start client. The IEMS also supports the HTML client which requires less resources.</p> <p>Note 3: If Mozilla is the default browser in the Microsoft Windows platform, the Mozilla browser does not always come to the foreground when an application is launched from the IEMS Client.</p> <p>Note 4: Java TM Web Start 1.4.2_08 is included with the Java TM 2 Runtime Environment version 1.4.2_08. This can be downloaded from the IEMS server. Refer to http://your_iems_server_hostname.</p>	

Comparison of the Java Web Start and Web Client interfaces

The IEMS Client GUI provides a graphical display of information, accessed from the IEMS Server. IEMS functions, including displaying the discovered devices, and viewing alarms, and events are performed through the IEMS Client.

Since access to IEMS information is performed through a client, the selection of the client is up to the user. The two types of user interfaces available, and the advantages of one over the other, are provided in the following table:

Comparison of the Java Web Start and Web Client GUIs

Feature	Java Web Start Interface	Web Client
Browser	The correct virtual machine must be included with the browser. For browser requirement details, see System requirements .	Browser is required but plug-ins are not necessary. For browser requirement details, see System requirements .
Distribution	Nothing to install on the client platform except for the requirement of browser with the JRE Plug-in. For details, see System requirements .	Nothing to install on the client. Only a browser is required. For browser requirement details, see System requirements .
Information update	Automatic and immediate updates of data take place on the client.	Need to refresh the client HTML pages manually to view updated data.
Link	Requires a high speed link of 1 Mbps or higher.	Functions well over a low-speed dial-up Internet connection of 64 kbps.

The following table compares the Java Web Start and Web Client GUIs based on features:

Comparison of the Java Web Start and Web Client GUIs based on features

Feature	Java Web Start Client	Web Client
Inventory and Topology		
Tree Node operations such as Add Node, Modify Node, Delete Node and Move Node.	Available	Not available

Feature	Java Web Start Client	Web Client
Update status of managed objects	Available upon right click of the managed object	Not available
Object specific menu bar	Available	Not available
Topology operations such as Add, Delete, Re-layout, and Save options.	Available	Not available
Resynchronize inventory	Available in the right click menu of objects in the Inventory view	Not available
Administration and security		
Group Administration	Available	Not available
User Administration	Available	Available except for User privileges configuration
Change password for the user	Available under the Tools menu and in Security Administration GUI	Available only in the "Modify User Profile" option under the Admin tab-->User Admin.
Fault management		
Resynchronize alarms	Available in the right click menu of objects in the Topology view	Not available
Event clean up option	Available under the 'Tools' menu	Not available
Dynamic update of alarms	Available	Alarm summary panel is automatically refreshed every 30 seconds.
Alarm filter	Available	Not available
Event filter	Available	Not available
Performance Management		
XML templates: used for performance data template creation	Available under the 'Tools' menu	Not available
Configured collection	Available under "Administration Tools" in the IEMS tree	Not available
Others		
Broadcast message	Available	Not available
Theme manager	Ten themes are available	Only "Olive Green" and "Steel Blue" are available
"Order by" option: used to order the objects in the map	Available under the Edit menu	Not available

Feature	Java Web Start Client	Web Client
Audit logs and security logs	Available under the Tool menu	Not available
Launching applications for managed objects	Available	Not applicable
GUI look and feel	Metal, CDE/Motif, and Windows look and feel available	Not applicable
Detach window	Available	Not available
Topology tool bar used to customize map symbols.	Available	Not available
Configuration of northbound OSS	Available	Not available

Using Java Web Start Client

This section describes the procedures to launch the IEMS Java Web Start Client in different operating systems (OS). This subsection contains describes how to log into the IEMS server through the Java Web Start Client.

Logging in to the IEMS server

Application

Use this procedure to log in and connect to the IEMS server using a web browser.

IEMS supports up to 20 simultaneous JWS clients and 44 simultaneous HTML clients.

- the iemsadm user is not allocated a single sign on (SSO) token. As a result, when performing command line or GUI launches from the IEMS client, SSO is not supported.
- complex password rules are not enforced for the iemsadm user.
- the iemsadm user does not support the password change period minimum and maximum thresholds.
- the iemsadm user does not support group authentication logging.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Connect to the IEMS server using a web browser with the URL in the format: `https://hostname:9091`.

A page similar to the following figure is displayed:



- 2 Select your next step.

If you want to log in	Do
using Web Client	step 3
using Java Web Start Client	step 4

You can launch the Web Client from the Java Web Start Client by clicking the HTML UI button in the toolbar.

- 3 Log in using the Web Client.
- Type the user name and password.
 - Select the **Web Client** button to connect to the Web Client.
 - Go to [step 5](#).
- 4 Log in using the Java Web Start Client.
- Click the **Web Start Client** button.
This launches the login dialog.
As a security precaution, when you type text in the password field, it is not displayed.
 - Enter the valid user name and password and click the **Connect** button.
A splash screen is displayed. Once the splash screen disappears, a Security Notice is displayed.
 - Click the **OK** button to launch the IEMS Java Web Start Client.
- 5 If you leave the IEMS client screen idle for a specified time period, you are locked out of the screen, If this happens, enter your user name and password in the IEMS Lock screen.

For the procedure to configure idle time before lock out, refer to "Modifying login session timeouts on the SPFS-based server" in *IEMS Administration and Security*, NN10336-611.
- 6 You have completed this procedure.

—End—

Configuring login settings

The login settings including password and user accounts are explained in this subsection.

Logging in after the password has expired

If a user attempts to connect to the IEMS server after their password has expired, the Login Failed dialog appears with message "Your password has expired". To change the password, log in using administrator privileges and change the password. Refer to the procedure "Changing a user password" in *IEMS Administration and Security*, NN10336-611.

User account expiration

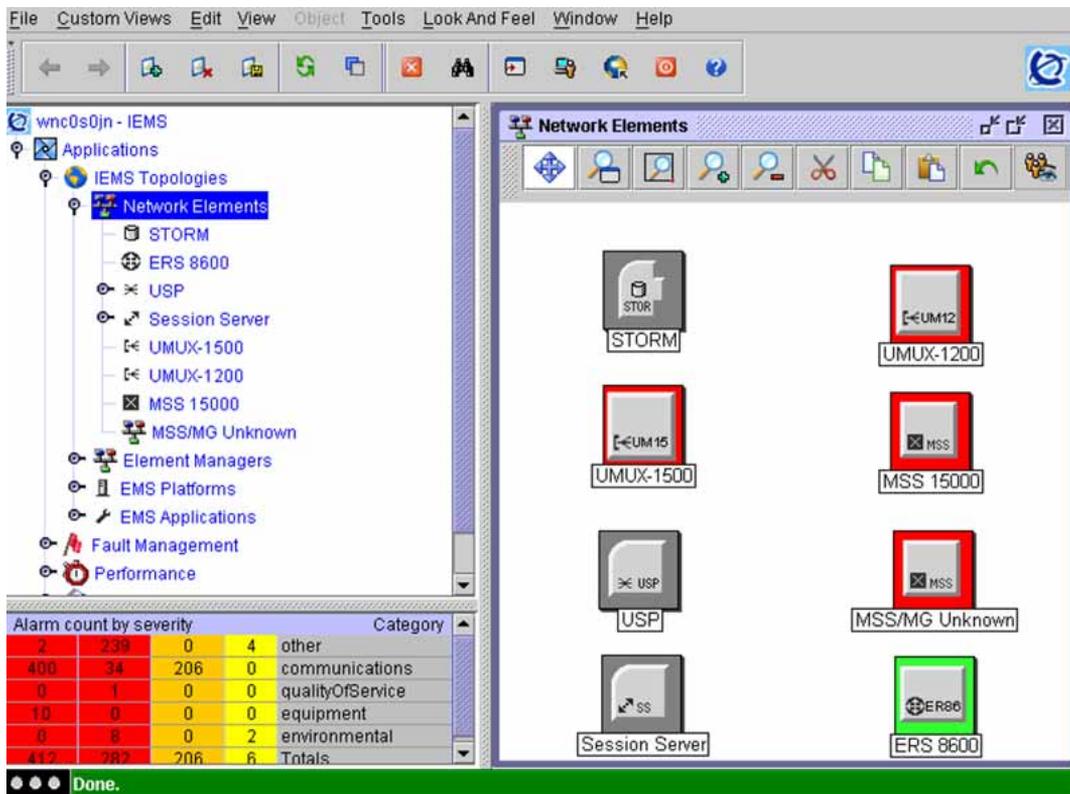
User account expiration dialog is displayed with the message "Your account has expired". In this condition, no access to the IEMS Java Web Start Client is permitted until the account is reactivated by the administrator through the Security Administration GUI.

User disabled status

If an account is disabled by the administrator using the security administration GUI, the individual account cannot access the IEMS Java Web Start Client. The Login Failed dialog is displayed with the message "Your account is disabled".

Overview of the Java Web Start Client interface

The Java Web Start Client graphical user interface (GUI) contains a menu bar, toolbar, topology toolbar, IEMS tree, alarm count panel, status bar, and IEMS display panel as showing in the following. This sub-section provides a detailed description of the configurations available initially on the screen.



Menu bar

The menu bar contains drop-down menus including File, Custom Views, Edit, View, Actions, Tools, Look And Feel, Window, and Help.

The menus appearing in the menu bar are context sensitive to the object selected in the IEMS Java Web Start Client. The menus and the menu items appear or disappear dynamically according to the object selected in the IEMS Java Web Start Client.

Toolbar

The toolbar is a component that displays a collection of actions, commands, or control functions. Toolbars are useful to provide access to the frequently used components. The default position for the toolbar is below the menu bar. A tool tip is provided for each tool button, which indicates the operations

performed by them. The tool buttons include Go Back to Previous, Go Forward to Next, Save, Print, Refresh, Delete, Stop, and Help. The toolbar is movable and floatable.

The tool buttons appearing in the toolbar are context sensitive to the object selected in the IEMS Java Web Start Client. The tool buttons appear or disappear dynamically according to the object selected in the IEMS Java Web Start Client.

Tool Tip

A tool tip is the text that is displayed when you move your cursor over a specific icon. For example, if you place your cursor over any network element icon in the Network Elements display window and hold it there, text appears describing that element. You can change the text that appears over that element by selecting Edit -> Change Tool Tip Text. Then you can choose to show the Display Name, Name, Status, Icon Name, or Menu Name for that element.

Tree

A tree is used to display a set of IEMS applications with their hierarchical data relationships. The fundamental object in a tree is called a node, which represents a data item in the given hierarchical set. Thus, a tree is composed of one or more nodes. The root node is the top node of the hierarchical data.

Nodes inside the root nodes are called child nodes. Nodes that contain no child nodes are called leaf nodes. By choosing a particular node, the corresponding panel is displayed on the right-side frame.

Alarm count panel

The alarm count panel shows the alarm count of each severity (Critical, Major, Minor, Warning, and Clears) for each alarm category. The alarm count panel is located below the IEMS tree. Double-clicking the count displayed in the alarm count panel causes the alarms of the specific severity to display in the corresponding alarm panel. This panel is updated automatically and the counts can be seen continuously, irrespective of the functional view (whether maps or events are chosen). The tool tip and the cursor shape changes when the mouse pointer is pointed on alarm counts. By selecting the counts in the alarm count panel, the respective alarms in the right-hand side panel are displayed.

Status bar

The status bar is located at the bottom of the screen. It indicates the status of the current process. The status bar displays "Done" when all the contents are loaded, or displays "loading..." if the process is still active. The status bar changes from dark blue to green during the loading of the product.

Display panel

The display panel is shown on the right hand side as a frame within the main window. The panel shows the frame that corresponds to the selection made on the tree.

Launching the IEMS Java Web Start Client

Application

Use this procedure to launch the IEMS Java Web Start Client.

IEMS Java Web Start Client is launched by connecting to the IEMS Server and logging in.

To launch the IEMS Java Web Start Client, the correct version of JRE must be installed in the client workstation. For details, see [System requirements](#).

Launching the Java Web Start Client in various platforms

The Java Web Start Client runs on multiple platforms, including Microsoft Windows and Sun Solaris. From any of the browsers in the system, IEMS Java Web Start Client can be launched by navigating to the URL comprising the name and port number of the host. The complete URL is in the form of `https://hostname:9091`. Click the **Web Start Client** button on the page to invoke the login dialog. After entering the user name and the password, connection to the IEMS Server is accomplished.

Action

Step	Action
At the IEMS workstation	
1	<p>Connect to the IEMS Server host from the browser using a URL in the format of <code>https://hostname_or_IP_Address:9091</code>.</p> <p><code>https://succession-sol1:9091</code></p> <p>In the above example, "succession-sol1" is the name of the machine in which the server is running, and "9091" is the port number on which the server is running.</p>
2	<p>Select the Web Start Client button to display the authentication dialog.</p> <p>If the JRE prompts for JRE update from the java.sun.com site, abort it by clicking the Abort button. Click the "Client Software Install Guide" hyperlink (<code>http://<IEMS server host name>/client/installguide.html</code>) in the IEMS login page to check whether the correct JRE version is installed.</p>
3	<p>Enter the correct user name and password and select the Connect button.</p> <p><i>A flash screen appears after you successfully log in.</i></p>

- 4 Click the **OK** button in the Security Notice window to launch the IEMS Java Web Start Client.
- 5 You have completed this procedure.

—End—

Launching applications from IEMS

Applications, element managers, or commands can be launched from the topology GUI in IEMS. The applications, element managers, or commands launched depend on the selected object. The following sections provide procedures that describe how to launch applications from the topology GUI for objects listed below, as well as common procedures to launch applications for objects managed by IEMS.

- [Launching EMS Element Managers](#)
- [Launching EMS Platforms](#)
- [Launching EMS Applications](#)
- [Launching EMS Network Elements](#)

Requirements for the client workstation

In order to access the launch applications, the client must have the requirements specified in [System requirements](#).

Launching applications from IEMS

The following table lists the element managers, EMS platforms, EMS applications, and network elements that are supported on IEMS.

A device can be added to the IEMS inventory in the following ways:

- You can manually add a device to the inventory.
- Some element managers have an inventory interface that the IEMS uses to discover the devices that they manage. This discovery occurs when adding the respective element manager to the IEMS. This includes APS Manager, GWC Manager, MG 9000 Manager, MDM, SAM21 Manager, UAS Manager, and UNEM.
- When adding some element managers to the IEMS, the respective NE and/or platform is automatically added to the Network Element folder in the IEMS Topologies tree. The mode of discovery is indicated in this table for each device.

Name	Type of application that can be launched from IEMS	Mode of discovery
Element Managers		
Audio Provisioning Server (APS) Manager	GUI	Manually added
CEM Manager	GUI	Manually added
CICM Manager	GUI Command line	Manually added
CS 2000 Core Manager (manages Call Agent Core and CS 2000 Core NEs)	GUI Command line	Manually added
GWC Manager	GUI	Manually added
Fault and Performance (FPM) Manager	GUI Command line	Manually added
MCS Manager (manages MCS/CSE and Media Portal)	GUI Command line	Manually added
MCS Manager for Session Server Lines (SSLines)		Manually added
MG 9000 Manager	GUI	Manually added
MDM (manages MG 7480/15000/20000 and Multiservice Switch 15000 NEs)	GUI Command line	Manually added
SAM21 Manager	GUI	Manually added
Universal Audio Server Manager	GUI	Manually added
UMUX Network Element Manager (UNEM) (manages UMUX 900/1200/1500 NEs)	GUI	Manually added
EMS platforms		
MDM	Command line	Automatic discovery supported from (I)SN08
SDM	Command line	Automatic discovery
SPFS	GUI Command line	Manually added
EMS applications		
Certificate Manager	GUI	Manually added
Line Maintenance Manager	GUI	Manually added
Network Patch Manager	GUI	Manually added
OSSGate	GUI Command line	Manually added

Name	Type of application that can be launched from IEMS	Mode of discovery
QoS Collector Application	Command line	Manually added
Synchronized Backup and Restore Manager (SBRM)	Command line	Manually added
Trunk Maintenance Manager	GUI	Manually added
EMS network elements		
Call Agent Core managed by CS 2000 Core Manager	GUI	Automatic discovery
Call Agent Platform managed by CS 2000 Core Manager	Command line	Automatic discovery
CICM NE	GUI	Manually added
CS 2000 Core	GUI Command line	Automatic discovery
ERS 8600	GUI Command line	Manually added
GWC NE	GUI Command line	Automatic discovery
MAS NE	GUI	Manually added
MCS NE	GUI Command line	Automatic discovery
Media Portal NE managed by MCS Manager	GUI Command line	Automatic discovery
Media Server 2000	GUI Command line	Manually added
MG 3200	GUI	Manually added
MG 7480/15000/20000 NE managed by MDM	GUI Command line	Automatic discovery
MG 9000		Automatic discovery
MSS 15000 NE managed by MDM	GUI Command line	Automatic discovery
SAM21 NE	GUI Command line	Automatic discovery
Session Server Trunks (SSTrunks)	GUI Command line	Manually added
Session Server Lines (SSLines)	GUI Command line	Automatic discovery

Name	Type of application that can be launched from IEMS	Mode of discovery
STORM	GUI Command line	Manually added
Universal Audio Server	Command line	Automatic discovery
Universal Signaling Point (USP)	GUI Command line	Manually added
UMUX 1500, 1200, 900	GUI	Automatic discovery
Virtual Switching Point (VSP) NE managed by MDM	GUI	Automatic discovery
MTX NE managed by CEM Manager	GUI	Automatic discovery
MSC NE managed by CEM Manager	GUI	Automatic discovery
HLR NE managed by CEM Manager	GUI	Automatic discovery
TRI NE managed by CEM Manager	GUI	Automatic discovery

Identifying object map symbols

The various map symbols used in the topologies to represent the objects in IEMS Client are tabulated below:

Map Symbol	Associated EMS/NE
Element managers	
	Audio Provisioning Server Manager (APS Manager)
	Communication Server 2000 Core Manager (CS 2000 Core Manager)
	Core Element Manager (CEM)

Map Symbol	Associated EMS/NE
	Multimedia Communication Server 5200 Manager (MCS Manager)
	Fault and Performance Manager (FPM)
	Communication Server 2000 Gateway Controller Manager (CS 2000 GWC Manager)
	Media Gateway 9000 Manager (MG 9000 Manager)
	Communication Server 2000 SAM21 Manager (CS 2000 SAM21 Manager)
	UMUX Network Element Manager (UNEM)
	Universal Audio Server Manager (UAS Manager)
	Centrex IP Client Manager (CICM Manager)
	Integrated Element Management System (IEMS)

Map Symbol	Associated EMS/NE
	MCS system manager unit
	FPM (Fault and Performance Manager)
EMS applications	
	Audio Provisioning Server (APS)
	Line Maintenance Manager (LMM)
	Trunk Maintenance Manager (TMM)
	OSSGate
	Network Patch Manager (NPM)
	QoS Collector Application (QCA)
	Synchronized Backup Restore Manager (SBRM)

Map Symbol	Associated EMS/NE
	Certificate Manager (CM)
EMS platforms	
	Server Platform Foundation Software (SPFS)
	Multiservice Data Manager
	SuperNode Data Manager (SDM)
Network elements	
	Centrex IP Client Manager (CICM) NE managed by CICM Manager.
	Media Application Server (MAS)
	Media Gateway 3200 (MG 3200)
	Media Server 2000 (MS 2000)

Map Symbol	Associated EMS/NE
	ERS 8600 (Ethernet Routing Switch 8600)
	Storage Management (STORM)
	Universal Signaling Point (USP)
	Communication Server 2000 Core NE (CS 2000 Core NE) managed by CS 2000 Core Manager
	Call Agent Core managed by CS 2000 Core Manager
	Call Agent Platform is subnode of Call Agent Core
	Multimedia Communication Server (MCS) NE managed by MCS Manager
	Virtual Switching Point (VSP) NE managed by Multiservice Data Manager
	Multiservice Switch 15000 (MSS 15000) NE managed by Multiservice Data Manager

Map Symbol	Associated EMS/NE
	Multiservice Switch 7000 (MSS 7000) NE managed by Multiservice Data Manager
	Multiservice Switch 20000 (MSS 20000) managed by Multiservice Data Manager
	Media Gateway (MG) managed by Multiservice Data Manager
	RTP Media Portal NE
	Universal Multiplexer 900 NE (UMUX 900 NE)
	Universal Multiplexer 1200 NE (UMUX 1200 NE)
	Universal Multiplexer 1500 NE (UMUX 1500 NE)

Launching element managers

This section describes the procedures to launch applications for element manager objects from the IEMS topology panel.

Launching applications for APS Manager

Application

Use this procedure to launch the APS Manager from the IEMS Java Web Start Client.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
- 2 Select the Element Managers topology node in the IEMS Topologies tree.
- 3 Select an APS Manager map symbol in the IEMS display panel.
- 4 Right-click the map symbol and select the **APS Manager** menu item.
The CS 2000 Management Tools application opens. The APS Manager can be accessed through SSO (Single Sign On).
- 5 You have completed this procedure.

—End—

Launching applications from CICM Manager

Application

Use this procedure to launch applications for CICM Manager from IEMS Java Web Start Client.

Prerequisites

The prerequisites for launching the CICM Manager are:

- The HTTPS proxy must be configured using the SPFS CLI tool for launching CICM Manager from the IEMS client. To configure the Apache Web Server on an SPFS-based server for the HTTPS proxy, see "Configuring the Apache Web Server for HTTPS proxy" in *Nortel ATM/IP Solution-level Configuration*, NN10409-500. To configure the HTTPS proxy for CICM Manager, refer to *CICM Configuration*, NN10240-511.
- You must launch CICM Manager in Microsoft Windows with the default browser configured as Microsoft Internet Explorer.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select **Element Managers** under in the IEMS Topologies tree.
- 3 Right-click the desired CICM node in the IEMS display panel, and select the required menu item. The menu items are listed in the following table.

Menu item	
View Children	Displays the map symbols for configured units associated with the CICM parent node. Once displayed, right-click on the desired unit and select the required menu item.

Menu item	
Launch CICM Manager	Launches the CICM Manager in the browser according to the specified URL
Launch Command Line	Enables communication with remote devices from IEMS using SSH.

4 You have completed this procedure.

—End—

Launching Core Element Manager

Application

Use this procedure to launch the Core Element Manager (CEM) for NEs managed by CEM from the IEMS Java Web Start Client.

Examples of NEs that can be managed by CEM are Mobile Telephone Exchange NE (MTX NE), Mobile Switching Center NE (MSC NE), Home Location Register NE (HLR NE), and TRI NE.

The CEM is available with selected versions of Carrier VoIP platforms and is available in selected sites of Carrier VoIP platforms.

The users belonging to "ems" and "mgc" can launch the CEM from the NEs managed by CEM.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
- 2 Select **Network Elements** under IEMS Topologies, then right-click the map symbol of an NE that is managed by CEM and select **View Children**.
- 3 Right-click the desired map symbol and select the **Launch CEM** menu item to launch the dialog.
The CEM is launched in the right-hand frame of the IEMS Java Web Start Client. Access to the CEM is permitted through SSO.
- 4 You have completed this procedure.

—End—

Launching a CEM Commissioning Manager CLI

Application

Use this procedure to launch the CEM Commissioning Manager application. Commissioning Manager can be used for configuration of network elements which are represented within the Commissioning Manager system as a set of managed node instances. You can use Commissioning Manager CLI to create, edit, and delete managed node instances.

Prerequisites

To perform this procedure you must have root privileges.

Action

Perform the following steps to complete this procedure.

Step Action

At your workstation

- 1 Log in to the IEMS server by typing

```
> telnet <server>
```

 and pressing the Enter key.
 where
 server is the IP address or host name of the server where IEMS resides
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing:

```
$ su - root
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change the directory by typing

```
# cd  
/opt/nortel/cem/data/coreEMS/nodes/server/bin
```

 and pressing the Enter key.
- 6 Launch the CLI by typing

```
# ./configCEMS -c
```

 and pressing the Enter key.

7 You have completed this procedure.

—End—

Launching applications for CS 2000 Core Manager

Application

Use this procedure to launch the following from IEMS Java Web Start Client:

- Core Manager Maintenance application for CS 2000 Core Manager
- MAPCI Session for CS 2000 Core Manager

Action

Step Action

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select the Element Managers topology node in the IEMS Topologies tree.
- 3 Select a CS 2000 Core Manager map symbol in the IEMS display panel.
- 4 Right-click the map symbol and select the required menu item. The menu items are listed in the following table.

Menu item	
Launch Core Mgr Maintenance	Communication with the device through IEMS using SSH on executing the command "/sdmtools/bin/sdmmtc" is enabled.
Launch MAPCI Session	Communication with the device through IEMS using SSH is enabled.

If you are unable to passthrough, configure the passthrough using the procedure "Adding or removing passthru users" in *CS 2000 Core Manager Administration and Security*, NN10170-611.

- 5 You have completed this procedure.

—End—

Launching applications for FPM

This subsection contains the following procedures:

- "Launching the MCP System Management Console" (page 40)
- "Launching the CLI for FPM" (page 41)

Launching the MCP System Management Console

Application

Use this procedure to launch the MCP System Management Console for FPM from the IEMS Java Web Start Client.

Prerequisites

The prerequisites for launching MCP Management Console are:

- You must install the correct JRE version on the client workstation. For details, see [System requirements](#).
- You must launch the MCP System Management Console from a Microsoft Windows platform-based client workstation.

Action

Step	Action
At the IEMS workstation	
1	Launch the IEMS Java Web Start Client (refer to "Launching the IEMS Java Web Start Client" (page 21)).
2	Select the Element Managers topology node in the IEMS Topologies tree.
3	Select an FPM map symbol and right-click to choose the Launch MCP System Management Console menu item. <i>The application launches in the client browser according to the specified URL.</i>
4	You have completed this procedure.

—End—

Launching the CLI for FPM

Application

Use this procedure to launch the Command Line Interface (CLI) for FPM from the IEMS Java Web Start Client.

Communication between the IEMS and the device is established through SSH (secure shell). The SSH mode uses the user name of the device (configured during provisioning of parent MCS Manager) to establish communication between IEMS and the device.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
- 2 Select the Element Managers topology node of the IEMS Topologies tree.
- 3 Select an FPM map symbol and right-click to choose the **Command Line** menu item.

Communication between the device and IEMS using SSH is enabled. SSH uses the user name configured for the device (while adding the device to IEMS) to communicate, and prompts for the password to log into the device.
- 4 You have completed this procedure.

—End—

Launching applications for GWC Manager

Application

Use this procedure to launch applications for the Gateway Control Manager (GWC) from the IEMS Java Web Start Client.

Prerequisites

None

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select the Element Managers topology node in the IEMS Topologies tree.
- 3 Select a GWC Manager map symbol in the IEMS display panel.
- 4 Right-click the map symbol and select the required menu item. The menu items are listed in the following table.

Menu item	
GWC Mgr (CMT)	Opens the GWC Manager client
GWC Mgr Network View	Opens the GWC Manager network view

Note: GWC Manager is accessed through Single Sign On (SSO).

- 5 You have completed this procedure.

—End—

Launching applications for MCS Manager

This subsection contains the following procedures:

- "Launching MCP System Management Console for the MCS System Manager version" (page 43)
- "Launching the CLI for MCS system manager" (page 44)
- "Launching the MCP Provisioning Client for MCS Manager for SSLines" (page 45)

The MCS system manager (MCS SM) is also known as MCS 5200 Manager.

Launching MCP System Management Console for the MCS System Manager version

Application

Use this procedure to launch MCP System Management Console for the MCS System Manager.

Prerequisites for launching MCP Management Console

The requirements for launching the MCP Management Console from the MCS system manager are as follows:

- The client workstation must have the correct JRE version installed. For details, see [System requirements](#).
- The MCP System Management Console can be launched only for Microsoft Windows platform-based client workstations.

Action

Step	Action
------	--------

At the IEMS workstation

- | | |
|---|--|
| 1 | Launch the IEMS Java Web Start Client. Refer to " Launching the IEMS Java Web Start Client " (page 21). |
| 2 | Select the Element Managers topology node in the IEMS Topologies tree.

OR

Select the MCS SM node under the Element Managers topology node of the IEMS Topologies tree. |

- 3 Select an MCS system manager map symbol and right-click to choose the **Launch MCP System Management Console** menu item.

When you click this menu item, the application is launched in the client browser according to the specified URL.

- 4 You have completed this procedure.

—End—

Launching the CLI for MCS system manager Application

Use this procedure to launch the CLI for the MCS System Manager version.

For the MCS system manager, you can launch the Command Line Interface (CLI). The communication between the IEMS and the device is established through SSH (secure shell). The SSH mode uses the username of the device (configured during provisioning of MCS system manager) to establish communication between IEMS and the device.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select the Element Managers topology node in the IEMS Topologies tree.

OR

Select the MCS SM node under the Element Managers topology node of the IEMS Topologies tree.
- 3 Select an MCS system manager map symbol and right-click to choose the **Command Line** menu item.

This option enables communication between the device and IEMS using SSH. SSH uses the user name configured for the device (while adding the device to IEMS) to communicate, and prompts for the password to log into the device.
- 4 You have completed this procedure.

—End—

Launching the MCP Provisioning Client for MCS Manager for SSLines

Application

Use this procedure to launch the MCP Provisioning Client for MCS Manager for SSLines.

Prerequisites

To launch the MCP Provisioning Client, you must:

- configure the provisioning clients. For detail of how to configure the provisioning clients, refer to "Configuring Provisioning Clients" in *IEMS Configuration*, NN10330-511.
- launch MCP Provisioning Client from Microsoft Windows platforms.

Action

Step	Action
At the IEMS workstation	
1	Launch the IEMS Java Web Start Client. Refer to " Launching the IEMS Java Web Start Client " (page 21).
2	Right-click Element Managers in the IEMS tree or the MCS_SM map symbol for SSLines.
3	Select the Launch MCP Provisioning Client menu item. <i>The application is launched in the client browser according to the specified URL.</i>
4	You have completed this procedure.
—End—	

Launching applications for MG 9000 Manager

Application

Use this procedure to launch the following applications for the MG 9000 Manager from IEMS Java Web Start Client:

- MG 9000 Manager
- IP SEC tool for the MG 9000 Manager

The IP Sec tool manages the IP security parameters for a MG 9000 element manager server.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select the Element Managers topology node in the IEMS Topologies tree.
- 3 Select an MG 9000 map symbol in the IEMS display panel.
- 4 Right-click the map symbol and select the required menu item. The menu items are listed in the following table.

Menu item	
MG9K Manager	Opens the MG 9000 Manager client. The MG 9000 Manager is accessed through SSO (Single Sign On).
IP Sec Tool	Opens the IP Sec tool in the browser as specified in the URL.

- 5 You have completed this procedure.

—End—

Launching applications for MDM

Application

Use this procedure to launch the following applications for MDM in the IEMS client:

- MDM Operator Client for MDM
- legacy MDM tools for MDM
- the CLI for MDM

Prerequisites

The requirements for launching the Legacy MDM tools are as follows:

- To launch the MDM X11 Client, run the X server in the client workstation. For Solaris/Linux, the Xserver runs by default; For Windows, Hummingbird or Exceed is used as the Xserver.
- To launch MDM X11Client, the client-server IP address must be provisioned using the procedure "[Provisioning the client-server IP address for MDM Manager](#)" (page 49).

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Go to the Element Managers topology in the IEMS Topologies tree.
- 3 Select your next step.

If you want to launch	Do
MDM Operator Client GUI for MDM	step 4
legacy MDM tools for MDM	step 6
the cli for MDM	step 13

- 4 Right-click the MDM map symbol and select the MDM Operator Client GUI menu item.
- 5 Go to [step 14](#).
- 6 Right-click the MDM map symbol and select the Legacy MDM Tools menu item.

If the client-server IP address is not provisioned, an error message is displayed asking you to provision the client-server IP address. Refer to procedure "[Provisioning the client-server IP address for MDM Manager](#)" (page 49) for details.

- 7 Select the IP address from the list and click the **OK** button.

The Legacy MDM Tools window launches similar to the following:

- 8 If the IEMS client is opened in Microsoft Windows, select the location of Hummingbird or Exceed using the **Browse** button.
- 9 Type the user name and password in the corresponding fields.
- 10 Select the required tool from the Options field.
- 11 Click the **Execute** button to launch the selected tool.

The selected tool in Legacy MDM Tools window is launched with MDM using secured communication via SSH.

Note: IEMS saves the location of the script or the executable file and commands in the client system from which the IEMS Java Web Start Client is launched.

- 12 Go to [step 14](#).
- 13 Right click an MDM map symbol and select the Command Line menu item.

This option enables communication between the device and IEMS using secure shell (SSH).

14 You have completed this procedure.

—End—

Provisioning the client-server IP address for MDM Manager

Application

Use this procedure to provision the client-server IP address for MDM Manager from MDM.

Note: The procedure to provision the client-server IP address for MDM Manager should be performed once only.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select the Element Managers topology node in the IEMS Topologies tree.
- 3 Select the required MDM map symbol in the IEMS display panel.
- 4 Right-click the map symbol and select the **Client-Server IP provisioning** menu item.

The system displays a window similar to the following:



- 5 Enter the MDM Client-Server primary IP address in the Primary IP Address field.
- 6 Enter the MDM Client-Server secondary IP address in the Secondary IP Address field.
- 7 Click the **OK** button.
- 8 You have completed this procedure.

—End—

Launching the SAM21 Manager

Application

Use this procedure to launch the SAM21 Manager client from the IEMS Java Web Start Client.

Action

Step	Action
<i>At the IEMS workstation</i>	
1	Launch the IEMS Java Web Start Client. Refer to " Launching the IEMS Java Web Start Client " (page 21).
2	Select the Element Managers topology node in the IEMS Topologies tree.
3	Select a SAM21 Manager map symbol in the IEMS display panel.
4	Right-click the map symbol and select the SAM21 Mgr GUI menu item. <i>The SAM21 Manager client opens.</i>
5	You have completed this procedure.
—End—	

Launching UAS Manager

Application

Use this procedure to launch the UAS Manager from IEMS Java Web Start Client.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select the Element Managers topology node in the IEMS Topologies tree.
- 3 Select a UAS Manager map symbol in the IEMS display panel.
- 4 Right-click the map symbol and select **UAS Mgr (CMT)** menu item.
The CS 2000 Management Tools application opens.
- 5 You have completed this procedure.

—End—

Launching applications for an EMS platform

This subsection describes the following procedures to launch applications for EMS platform objects from the topology panel.

Launching applications for an MDM platform

Application

Use this procedure to launch the CLI for the MDM platform from the IEMS Java Web Start Client.

The CLI application for the MDM platform can be launched from IEMS Java Web Start Client.

Action

Step	Action
<i>At the IEMS workstation</i>	
1	Launch the IEMS Java Web Start Client. Refer to " Launching the IEMS Java Web Start Client " (page 21).
2	Click EMS Platforms under IEMS Topologies to display all grouped EMS platform map symbols.
3	Right-click the grouped MDM map symbol and select View Children .
4	Right-click the desired MDM node in the IEMS display panel, and select the Command Line menu item. <i>Communication with the remote device from IEMS is enabled using SSH.</i> Note: Communication with the device is established directly without bypassing through the proxy IEMS server.
5	You have completed this procedure.

—End—

Launching applications for an SDM platform

Application

Use this procedure to launch the CLI application for the SDM platform from IEMS Java Web Start Client.

The CLI application for SDM platform can be launched from IEMS Java Web Start Client.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
- 2 Select **EMS Platforms** under IEMS Topologies, then right-click the SDM map symbol and select **View Children**.
- 3 Right-click the desired SDM node in the IEMS display panel, and select the **Command Line** menu item.
Selecting this menu item enables communication with a remote device from IEMS using SSH. Access to the CLI is permitted through SSO (Single Sign On).
- 4 You have completed this procedure.

—End—

Launching an application for an SPFS platform

Application

Use this procedure to launch an application for the SPFS platform from the IEMS Java Web Start Client.

Prerequisites

None

Action

Step	Action
<i>At the IEMS workstation</i>	
1	Launch the IEMS Java Web Start Client. Refer to " Launching the IEMS Java Web Start Client " (page 21).
2	Click EMS Platforms under IEMS Topologies to display all grouped EMS platform map symbols.
3	Right-click the grouped SPFS map symbol and select View Children .
4	Right-click the desired SPFS node in the IEMS display panel, and select the required menu item. The menu items are listed in the following table.

Menu item	
View Children	Displays the map symbols for configured units associated with the SPFS parent node. Once displayed, right-click on the desired unit and select the required menu item.
Command Line	Enables communication with a remote device from IEMS using SSH
Servman Applications Status	Enables you to view the status of all applications running on the SPFS platform from IEMS using SSH
Swact Cluster	Enables swacting of platforms from IEMS using SSH
Restart SPFS	Restarts SPFS using SSH
IPSec Tool	Opens the IPSec tool. Available to launch from the SPFS parent node.

Menu item	
Update Radius secret	Opens the Radius Secret Configuration window. Available to launch from the SPFS parent node.
Launch Remote Ping	Opens the Remote Ping Parameters window. Available to launch from the SPFS unit.
Launch Remote TraceRoute	Opens the Remote TraceRoute window. Available to launch from the SPFS unit.

5 You have completed this procedure.

—End—

Launching EMS applications

This subsection describes the procedures to launch applications for EMS application objects from the topology panel.

Launching applications for APS

Application

Use this procedure to launch applications for an APS application from the IEMS Java Web Start Client.

You can launch the APS Manager (CMT) and APS Audio Configuration tool for the APS application from the IEMS Java Web Start Client.

Action

Step	Action
<i>At the IEMS workstation</i>	
1	Launch the IEMS Java Web Start Client. Refer to " Launching the IEMS Java Web Start Client " (page 21).
2	Select the APS application node under the EMS Applications node in the IEMS Topologies tree.
3	Select an APS application map symbol in the IEMS display panel.
4	Right-click the map symbol and select the APS Mgr(CMT) menu item. <i>This opens the APS application.</i> OR Right-click the map symbol and select the APS Audio Configuration Tool menu item. <i>This opens the APS Audio Configuration Tool.</i>
5	You have completed this procedure.
—End—	

Launching the Certificate Manager GUI

Application

Use this procedure to launch the Certificate Manager GUI from the IEMS Java Web Start Client.

Certificate Manager automates the management and replacement of device certificates for supported devices. In addition to this, a web interface can be used for configuration. The Certificate Manager GUI can be launched from a web browser or from the IEMS client window.

For more information about Certificate Manager, see *Nortel ATM/IP Solution-level Administration and Security*, NN10402-600.

Prerequisites

This procedure has the following prerequisites:

- you must belong to the secadm or the secro group administration group to launch the Certificate Manager.
 - Secadm group privileges permit you to use all operations in Certificate Manager.
 - Secro group privileges permit you only to view and browse in the Certificate Manager tool, but not to modify the certificates or alarms.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Select your first step.

If you want to open the Certificate Manager GUI	Go to
from the IEMS Java Web Client	step 2
from your browser	step 6

- 2 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 3 Expand **EMS Applications** under IEMS Topologies, then select Certificate Manager in the IEMS Topologies tree.

- 4 Right-click the desired Certificate Manager node in the IEMS display panel, and select the **Launch PK Manager** menu item.

The Certificate Manager application opens.

- 5 Go to [step 7](#).

- 6 Open the Certificate Manager GUI in your web browser by entering:

`https://<hostname>:8443/pkgui/`

where

`hostname` is the hostname of the server where Certificate Manager is installed

The Certificate Manager login screen opens.

- 7 Enter your user name and password and click the **Log In** button.

- 8 You have completed this procedure.

—End—

Launching an LMM application

Application

Use this procedure to launch the LMM for the LMM application from the IEMS Java Web Start Client.

The Line Maintenance Manager can be launched for the LMM application from the IEMS Java Web Start Client.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
- 2 Select **EMS Applications** under IEMS Topologies, then right-click the LMM map symbol and select View Children.
- 3 Right-click the desired LMM node in the IEMS display panel, and select the **Line Maintenance Manager (LMM)** menu item.
The LMM application opens. The LMM application is accessed through SSO (Single Sign On).
- 4 You have completed this procedure.

—End—

Launching applications for an NPM application

Application

Use this procedure to launch the Network Patch Manager (NPM) and CLI applications for the NPM application from IEMS Java Web Start Client.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
- 2 Select **EMS Applications** under IEMS Topologies, then right-click the NPM map symbol and select **View Children**.
- 3 Right-click the desired NPM node in the IEMS display panel and select the required menu item. The menu items are listed in the following table.

Menu item	
Network Patch Manager (NPM)	Opens the NPM application. The NPM application is accessed through SSO (Single Sign On).
Command Line	Enables communication with remote applications or devices from IEMS using SSH.

- 4 You have completed this procedure.

—End—

Launching an OSSGate application

Applications

Use this procedure to launch the OSSGate application from the IEMS Java Web Start Client.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
- 2 Select **EMS Applications** under IEMS Topologies, then right-click the OSSGate map symbol and select **View Children**.
- 3 Right-click the desired OSSGate node in the IEMS display panel, and select the required menu item. The menu items are listed in the following table.

Menu item	
Launch OSSGate	Enables communication with the application from IEMS using SSH
Launch BPT Servlet	Opens the BPT servlet in the browser as specified in the secured URL. The BPT servlet application is accessed through SSO (Single Sign On).
Launch BPT Command Line	Enables communication with remote devices from IEMS using SSH.

- 4 You have completed this procedure.

—End—

Launching the CLI for a QoS Collector application

Applications

Use this procedure to launch the CLI for the QoS Collector application from IEMS Java Web Start Client.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
- 2 Select **EMS Applications** under IEMS Topologies, then right-click the QOS Collector map symbol and select **View Children**.
- 3 Right-click the desired QOS Collector node in the IEMS display panel, and select the **Launch Command Line** menu item.
Communication with the application from IEMS using SSH is enabled. The QoS Collector application is accessed through SSO (Single Sign On).
- 4 You have completed this procedure.

—End—

Launching the CLI for an SBRM application

Application

Use this procedure to launch the Synchronized Backup Restore Manager (SBRM) CLI application from the IEMS Java Web Start Client.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
- 2 Select **EMS Applications** under IEMS Topologies, then right-click the SBRM map symbol and select **View Children**.
- 3 Right-click the desired SBRM node in the IEMS display panel, and select the **Command Line** menu item.
Communication with the application from IEMS using SSH is enabled.
- 4 You have completed this procedure.

—End—

Launching a TMM application

Application

Use this procedure to launch the Trunk Maintenance Manager (TMM) for the TMM application from IEMS Java Web Start Client.

Action

Step	Action
<i>At the IEMS workstation</i>	
1	Launch the IEMS Java Web Start Client (refer to " Launching the IEMS Java Web Start Client " (page 21)).
2	Select EMS Applications under IEMS Topologies, then right-click the TMM map symbol and select View Children .
3	Right-click the desired TMM node in the IEMS display panel, and select the Trunk Maintenance Manager (TMM) menu item. <i>The TMM application opens. The TMM application is accessed through SSO (Single Sign On).</i>
4	You have completed this procedure.
—End—	

Launching applications for network elements

This subsection describes the procedures to launch applications for NE objects from the topology panel.

Launching the CLI for the Call Agent platform

Application

Use this procedure to launch the Command Line Interface (CLI) for the Call Agent platform from IEMS Java Web Start Client.

Action

Step	Action
<i>At the IEMS workstation</i>	
1	Launch the IEMS Java Web Start Client (refer to " Launching the IEMS Java Web Start Client " (page 21)).
2	Select the Call Agent Platform topology (under the Network Elements-->Call Agent Core-->Call Agent Platform topology node or Network Elements -> Call Agent Core -> CS2000 Core) in the IEMS Topologies tree.
3	Select a Call Agent Platform map symbol in the IEMS display panel.
4	Right-click the map symbol and select the Call Agent Platform Command Line menu item. <i>Communication with remote devices from IEMS is enabled using SSH.</i>
5	You have completed this procedure.
—End—	

Launching a MAPCI Session for Call Agent Core and CS 2000 Core

Application

Use this procedure to launch the MAPCI Session for Call Agent Core and CS 2000 Core NE from IEMS Java Web Start Client.

Action

Step	Action
<i>At the IEMS workstation</i>	
1	Launch the IEMS Java Web Start Client (refer to "Launching the IEMS Java Web Start Client" (page 21)).
2	Select Network Elements under IEMS Topologies, then right-click the Call Agent Core map symbol and select View Children .
3	Right-click the desired Call Agent Core map symbol and select the Launch MAPCI Session menu item. <i>Communication with the remote device from IEMS is enabled using SSH.</i>
4	You have completed this procedure.

—End—

Launching a CICM NE

Application

Use this procedure to launch the CICM NE.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Click **Network elements** under IEMS Topologies to display all grouped network element map symbols.
- 3 Right-click the grouped CICM map symbol and select **View Children**.
- 4 Right-click the desired CICM node in the IEMS display panel, and select the required menu item. The menu items are listed in the following table.

Menu item	
View Children	Displays the map symbols for configured units associated with the CICM parent node. Once displayed, right-click on the desired unit and select the required menu item.
Launch CICM Manager	Launches the CICM Manager in the browser according to the specified URL

- 5 You have completed this procedure.

—End—

Launching the Client Session Monitor

Application

Use this procedure to launch the Client Session Monitor (CSM) through the Java Web Start Client.

CSM tracks and records password-based authentications, client starts, and client stops of the users. CSM tracks MG9000 element manager and CS2000 client starts and stops.

CSM allows you to view reports that display which client application sessions are active and for which user. You can also view historical data of client application usage by user, date, or device using CSM.

To configure the CSM, refer to *Configuring the Client Session Monitor in ATM/IP Solution-level Configuration*, NN10409-500.

Prerequisites

You must belong to the SEC* group to perform this procedure.

Action

Step	Action
------	--------

At the IEMS workstation

- | | |
|---|---|
| 1 | Launch the Security Administration tool. Refer to Starting the Security Administration tool in <i>IEMS Administration and Security</i> , NN10336-611. |
| 2 | Select Client Session Monitor from the View menu to launch the CSM GUI client. |
| 3 | If prompted, log in using your user name and password.
<i>A window opens which displays all current application sessions.</i> |
| 4 | You have completed this procedure. |

—End—

Launching applications for an Ethernet Routing Switch 8600 NE

Application

Use this procedure do the following from the IEMS Java Web Start Client:

- configure the Ethernet Routing Switch (ERS) 8600 executable path
- launch the ERS 8600
- launch the CLI for the ERS 8600

Prerequisites for launching ERS 8600 Device Manager

To launch the GUI you must install ERS 8600 Device Manager on the client workstation. For details of how to install the Device Manager, refer to *Installing ERS 8600 Switch Modules-312749F*.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
- 2 Select **Network Elements** under IEMS Topologies, then right-click the ERS 8600 map symbol and select **View Children**.
- 3 Select your next step.

you want to	
configure the ERS 8600 Device Manager executable path	go to step 4
launch the ERS 8600 Device Manager	go to step 6
launch the CLI for the ERS 8600 Device Manager	go to step 8

- 4 To configure the ERS 8600 Device Manager executable path and launch the ERS 8600 Device Manager, follow these steps:
 - a. Right-click the desired ERS 8600 map symbol and select the **ERS 8600 --> Configure** menu item.
A file chooser dialog box opens.
 - b. Click the **Browse** button to select the ERS 8600 Device Manager executable file path.

- c. Click the **Launch** button.

The ERS 8600 Device Manager is launched with the configured executable path.

Note 1: You can use the procedure to change the existing executable path.

Note 2: IEMS saves the location of the most recently executed script or executable file in the client system from which the IEMS Java Web Start Client is launched.

- 5 Go to [step 9](#).

- 6 To launch the ERS 8600 Device Manager from IEMS, follow these steps:

- a. Right-click the desired ERS 8600 map symbol and select the **ERS 8600 Device Manager-->Launch** menu item.

The ERS 8600 Device Manager is launched.

Note: If the executable path has not already been configured using the procedure in [step 4](#), the window to configure the executable path is launched.

- 7 Go to [step 9](#).

- 8 To launch the CLI for the ERS 8600 network element, right-click the map symbol and select the **Command Line** menu item. The same user name must be used to proxy into the IEMS and log in to the ERS 8600 network element. It is highly recommended that the ERS 8600 uses the Central Security Service so that the same account is authenticated locally on IEMS and remotely on ERS 8600. If ERS 8600 does not enable Central Security Service, the user accounts on IEMS and ERS 8600 are different, but the user name must be the same. If a different user name is used, authentication failure will occur.

Note: Access to the CLI is permitted after authentication from the device.

- 9 You have completed this procedure.

—End—

Launching applications for a GWC NE

Application

Use this procedure to launch applications for the GWC network element from the IEMS Java Web Start Client.

Action

Step	Action
At the IEMS workstation	
1	Launch the IEMS Java Web Start Client. Refer to " Launching the IEMS Java Web Start Client " (page 21).
2	Click Network Elements under IEMS Topologies to display all grouped network element map symbols.
3	Right-click the grouped GWC map symbol and select View Children .
4	Right-click the desired GWC node in the IEMS display panel, and select the required menu item. The menu items are listed in the following table.

Menu item	
View Children	Displays the map symbols for configured units associated with the GWC parent node. Once displayed, right-click on the desired unit and select the required menu item.
GWC Unit Mgr	Opens the GWC Manager client
Launch Command Line	Enables communication with devices from IEMS using SSH
Launch LMM	Launches the LMM client in the browser specified in the URL
Launch TMM	Launches the TMM client in the browser specified in the URL
Launch NPM	Launches the NPM client in the browser specified in the URL
Launch CS2K Tools	Launches the CS 2000 Core client in the browser specified in the URL

Menu item	
Launch Remote Ping	Opens the Remote Ping Parameters window
Launch Remote TraceRoute	Opens the Remote TraceRoute window

5 You have completed this procedure.

—End—

Launching MAS Manager

This subsection contains the following procedures:

- "Configuring the RDC connection profile in the PC" (page 77)
- "Configuring the MAS Manager launch path and launching MAS Manager" (page 78)

Configuring the RDC connection profile in the PC

Application

Use this procedure to download and configure the Remote Desktop Connection (RDC) software. You must perform this procedure before you perform the procedure "Configuring the MAS Manager launch path and launching MAS Manager" (page 78).

Action

Step	Action
------	--------

At the client workstation

- | | |
|---|---|
| 1 | Under Microsoft Windows, click the Start button. |
| 2 | Select Programs . |
| 3 | Select Accessories . |
| 4 | Select Communications . |
| 5 | Click Remote Desktop Connection . |
| 6 | Click Options . |
| 7 | Enter 127.0.0.2:3390 for Windows XP or 127.0.0.1 for Windows 2000 and older versions in the Computer field. |
| 8 | Enter the appropriate MS Domain for your network. |
| 9 | Save the connection profile as <MAS-conn-profile-directory>/MAS.rdp. |

The file name must contain 'MAS.rdp' when saving the connection profile. The default <MAS-conn-profile-directory> used by RDC on Win2000 is the 'My Documents' folder of the user.

—End—

For further details on the installation of this software, refer to *Nortel Media Application Server Installation*, NN10455-301.

Configuring the MAS Manager launch path and launching MAS Manager

Application

Use this procedure to configure the MAS Manager launch path and to launch the MAS Manager from the IEMS Java Web Start Client. You can use this procedure to change the existing launch path. IEMS saves the location of the most recently executed script or launch file in the client system from which the IEMS Java Web Start Client is launched.

Prerequisites for launching MAS Manager

MAS Manager launch is available only on a Microsoft Windows PC that has the MAS Manager software installed. You must download the Remote Desktop Connection (RDC) software from the Microsoft web site and configure the RDC profile. Refer to "[Configuring the RDC connection profile in the PC](#)" (page 77).

MAS Manager cannot be launched on a Sun Solaris platform. If you try to launch MAS Manager on a Sun Solaris platform, the following message is displayed:

"Sorry! MAS client can be launched only in Windows"

If the executable path is not configured using the procedure in [step 4](#), the window to configure the executable path is launched.

For further details on installation of this software, refer to *Nortel Media Application Server Installation*, NN10455-301.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select **Network Elements** under IEMS Topologies, then right-click the MAS map symbol and select **View Children**.

- 3 Select your next step.

If you want to	
configure the MAS Manager launch path	go to step 4
launch the MAS Manager	go to step 8

- 4 Right-click the desired MAS map symbol and select the **MAS Manager-->Configure** menu item.

A file chooser dialog is launched.

- 5 Click the **Browse** button and enter the path to the MAS.rdp file that was created in "[Configuring the RDC connection profile in the PC](#)" ([page 77](#)).

- 6 Click the **Launch** button.

Communication is established between IEMS and the device through SSH proxy.

- 7 You have completed this procedure.

- 8 To launch the MAS Manager, right-click the desired MAS map symbol and select the **MAS Manager-->Launch** menu item.

Access to the MAS Manager is permitted after authentication.

- 9 You have completed this procedure.

—End—

Launching applications for an MCS/CSE and Media Portal NE

Application

Use this procedure to do the following:

- launch the MCP System Management Console for an MCS/CSE or Media Portal NE
- launch the Command Line Interface (CLI) for an MCS/CSE or Media Portal NE

Prerequisites

To launch an MCP Management Console you must:

- install the correct JRE version in the client workstation. For details, see [System requirements](#).
- launch the MCP System Management Console from Microsoft Windows platforms

Action

Step	Action						
At the IEMS workstation							
1	Launch the IEMS Java Web Start Client. Refer to " Launching the IEMS Java Web Start Client " (page 21).						
2	Select Network Elements under IEMS Topologies, then right-click the MCS/CSE or Media Portal NE map symbol map symbol and select View Children .						
3	Select your next step.						
<table border="1"> <thead> <tr> <th colspan="2">If you want to</th> </tr> </thead> <tbody> <tr> <td>launch the MCP System Management Console for MCS/CSE or Media Portal NE</td> <td>go to step 4</td> </tr> <tr> <td>launch the Command Line Interface (CLI) for MCS/CSE or Media Portal NE</td> <td>go to step 7</td> </tr> </tbody> </table>		If you want to		launch the MCP System Management Console for MCS/CSE or Media Portal NE	go to step 4	launch the Command Line Interface (CLI) for MCS/CSE or Media Portal NE	go to step 7
If you want to							
launch the MCP System Management Console for MCS/CSE or Media Portal NE	go to step 4						
launch the Command Line Interface (CLI) for MCS/CSE or Media Portal NE	go to step 7						
4	To launch the MCP System Management Console, right-click the desired MCS/CSE or Media Portal NE map symbol.						
5	Select the Launch MCP System Management Console menu item.						

The application is launched in the client browser according to the specified URL.

- 6 Go to [step 9](#).
- 7 To launch the CLI for an MCS/CSE or Media Portal NE, right-click the desired MCS/CSE or Media Portal NE map symbol.
- 8 Select the **Command Line** menu item.
An SSH connection to the parent System Manager of the NE is enabled. You must manually connect to the NE host using SSH or telnet.
- 9 You have completed this procedure.

—End—

Launching applications for the MG 3200 NE

Application

Use this procedure to launch applications for the MG 3200 NE from IEMS Java Web Start Client.

Prerequisites

Configure the HTTPS proxy in the MG 3200 using the SPFS CLI tool. Refer to *Configuring MG 3200 HTTPS proxy in the Nortel Media Gateway 3200 H.248 Configuration Guide, LTRT-72904*.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select **Network Elements** under IEMS Topologies, then right-click the MG 3200 map symbol and select **View Children**.
- 3 Right-click the desired MG 3200 node in the IEMS display panel, and select the required menu item. The menu items are listed in the following table.

Menu item	
Configure MG3200 Automated INI Backup	Opens the Automated INI file backup window
Launch Configuration GUI	Opens the MG 3200 Configuration GUI
IPSec and IKE Config Tool	Opens the IPSec and IKE Config Tool

- 4 You have completed this procedure.

—End—

Launching applications for an MG 7480/15000/20000 and MSS 15000 NE

This subsection contains the following procedures:

- "Launching the CLI for Multiservice Switch NEs from Java Web Start Client" (page 83)
- "Launching Legacy MDM tools" (page 84)

You can launch the Command Line Interface (CLI) for Legacy MDM tools for Multiservice Switch NEs (MG 7480/15000/20000 and MSS 15000 NEs) from IEMS Java Web Start Client.

Launching the CLI for Multiservice Switch NEs from Java Web Start Client

Application

Use this procedure to launch the CLI for Multiservice Switch NEs from IEMS Java Web Start Client.

Action

Step	Action
At the IEMS workstation	
1	Launch the IEMS Java Web Start Client (refer to "Launching the IEMS Java Web Start Client" (page 21)).
2	Select Network Elements under IEMS Topologies, then right-click an MG 7480/15000/20000 or MSS 15000 NE map symbol and select View Children .
3	Right-click the desired map symbol and select the Command Line menu item to launch the dialog. <i>Communication with the MDM (parent element manager) from IEMS is established using SSH. The CLI is launched after authenticating the user name and password.</i>
4	You have completed this procedure.
—End—	

Launching Legacy MDM tools

Application

Use this procedure to complete the following tasks:

- provision the client-server IP address for Multiservice Switch NEs
- launch Legacy MDM tools for Multiservice Switch NEs

Prerequisites

The requirements for launching the Legacy MDM tools are as follows:

- You must run the X server in the client workstation to launch the MDM X11 Client. For Solaris/Linux, the Xserver runs by default. For Windows, Hummingbird or Exceed is used as the Xserver.
- You must provision the client-server IP address as detailed in [step 1](#) before you launch the MDM X11 Client.

Action

Step	Action
------	--------

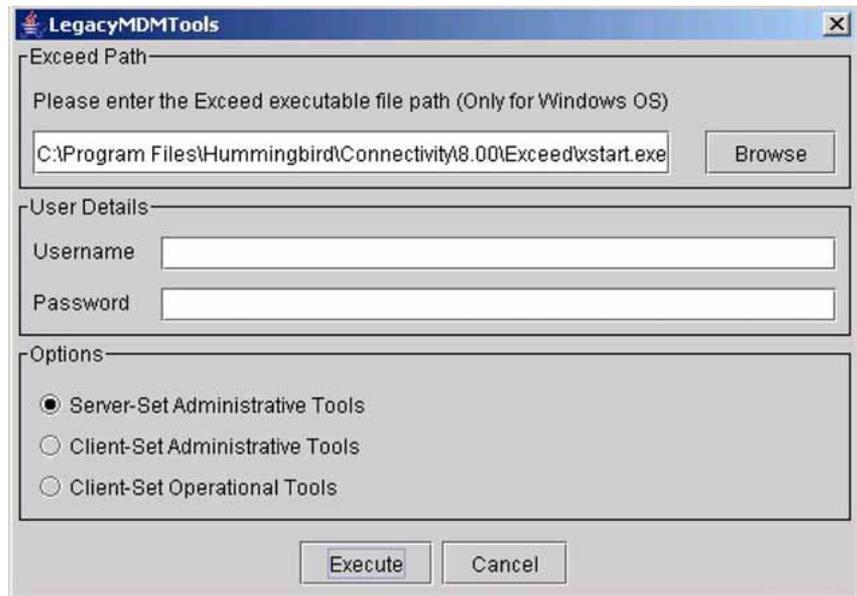
At the IEMS workstation

- | | |
|---|---|
| 1 | <p>To provision the client-server IP address for Multiservice Gateway and Multiservice Switch NEs follow these steps:</p> <ol style="list-style-type: none"> Launch the IEMS Java Web Start Client (refer to "Launching the IEMS Java Web Start Client" (page 21)). Select Network Elements under IEMS Topologies, then right-click an MG 7480/15000/20000 or MSS 15000 NE map symbol and select View Children. Right-click the desired map symbol and select the Client-Server IP provisioning menu item to launch the dialog. |
|---|---|

The system displays a window similar to the following screen shot.



- d. Enter the MDM Client-Server primary IP address in the Primary IP Address field.
 - e. Enter the MDM Client-Server secondary IP address in the Secondary IP Address field.
 - f. Click the **OK** button.
- 2** To launch Legacy MDM tools for Multiservice Gateway and Multiservice Switch NEs follow these steps:
- a. Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
 - b. Select **Network Elements** under IEMS Topologies, then right-click an MG 7480/15000/20000 or MSS 15000 NE map symbol and select **View Children**.
 - c. Right-click the desired map symbol and select the **Legacy MDM Tools** menu item to launch the dialog.
 If the client-server IP address is not provisioned, an error message is displayed asking to provision the client-server IP address. Refer to [step 1](#) for details.
 - d. Select the IP address from the list and click the **OK** button.
The Legacy MDM Tools window is launched and is similar to the following figure:



- e. If the IEMS client is opened in the Microsoft Windows platform, select the location of Hummingbird or Exceed using the **Browse** button.
- f. Type the user name and password in the corresponding fields.
- g. Select the required tool from the Options field.
- h. Click the **Execute** button to launch the selected tool.

The selected tool in Legacy MDM Tools window is launched using secured communication via SSH.

IEMS saves the location of the script or the executable file and commands in the client system from which the IEMS Java Web Start Client is launched.

- i. You have completed this procedure.

—End—

Launching applications for an MS 2000 NE

Application

Use this procedure to launch the Maintenance and Configuration tool for MS 2000 NE from IEMS Java Web Start Client.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select **Network Elements** under IEMS Topologies, then right-click the MS 2000 map symbol and select **View Children**.
- 3 Right-click the desired map symbol and select the **Config and Maintenance Tool** menu item.
The Maintenance and Configuration tool launches.
- 4 You have completed this procedure.

—End—

Launching applications for a SAM21 NE

Application

Use this procedure to launch the following from the IEMS Java Web Start Client:

- launch a SAM card view for a SAM21 card
- launch the SCU subnet for SAM 21 NE
- launch the SCU Manager for a SAM21 NE

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "[Launching the IEMS Java Web Start Client](#)" (page 21)).
- 2 Click **Network Elements** under IEMS Topologies to display all the grouped network element map symbols.
- 3 Right-click the grouped SAM21 map symbol and select **View Children**.
- 4 Right-click the desired SAM21 node in the IEMS display panel, and select the required menu item. The menu items are listed in the following table.

Menu item	
View Children	Displays the map symbols for configured cards associated with the SAM21 parent node. Once displayed, right-click on the desired card and select the required menu item.
Launch SAM21 Card View	Launches the card view, which is permitted with SSO. Available to launch from the SAM21 card.
Launch SCU Subnet	Launches the SCU subnet. Available to launch from the SAM21 parent node.
Launch SCU Mgr	Launches the SCU Manager. Available to launch from the SAM21 parent node.

5 You have completed this procedure.

—End—

Launching the Server Security Manager

Application

Use this procedure to launch the Server Security Manager (SSM) or IPsec tool. The SSM interface is an HTML web page.

Prerequisites

To perform this procedure, you must have administration privileges.

Action

Step Action

At the IEMS workstation

- 1 Select your first step.

If you want to launch SSM from	Do
an MG 9000 menu in Java Web Start Client	step 2
an SPFS menu in Java Web Start Client	step 7
a web browser	step 12

- 2 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
 - 3 Select the **Element Managers** topology node in the IEMS Topologies tree.
 - 4 Select an MG 9000 map symbol in the IEMS display panel.
 - 5 Right-click the map symbol and select the **IPSec Tool** menu item.
The login screen of the Server Security Manager opens.
 - 6 Go to [step 13](#).
 - 7 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
 - 8 Click **EMS Platforms** under IEMS Topologies to display all grouped EMS platform map symbols.
 - 9 Right-click the grouped SPFS map symbol and select **View Children**.
-

- 10 Right-click the map symbol and select the **IPSec Tool** menu item.
The login screen of the Server Security Manager opens.
- 11 Go to [step 13](#).
- 12 Open the Server Security Manager in your web browser by entering.
`http:// <ip address> /ipsec/security.html`
where
`ip address` is the address of the MG 9000 Manager master server or the MG 2000 Manager master server
The login screen of the Server Security Manager opens.
- 13 Enter your user name and password and click the **Log In** button.
- 14 You have completed this procedure.

—End—

Launching applications for Session Server Trunks

Application

Use this procedure to launch applications for the Session Server Trunks (SSTrunks) NE or SSTrunks unit from IEMS Java Web Start client.

Prerequisites

You must use the SPFS CLI tool to configure the apache proxy to enable the SSTrunks client to launch from the IEMS client. For details, refer to *ATM/IP Solution-level Configuration*, NN10409-500.

Action

Step	Action
At the IEMS workstation	
1	Launch the IEMS Java Web Start Client. Refer to " Launching the IEMS Java Web Start Client " (page 21).
2	Click Network Elements under IEMS Topologies to display all grouped network element map symbols.
3	Right-click the grouped SSTrunks map symbol and select View Children .
4	Right-click the desired SSTrunks node in the IEMS display panel, and select the required menu item. The menu items are listed in the following table.

Menu item	
View Children	Displays the map symbols for configured units associated with the Session Server parent node. Once displayed, right-click on the desired unit and select the required menu item.
Launch SSTrunks	Launches the SSTrunks client.
Command Line	Launches the CLI for communication with the remote device from IEMS using SSH.

Note: IEMS saves the location of script or executable file in the client system from which the IEMS Java Web Start Client is

launched. The recently executed script or executable file location is saved.

- 5 You have completed this procedure.

—End—

Launching applications for a STORM NE

Application

Use this procedure to launch the STORM Manager client or to launch the CLI for a STORM NE from IEMS Java Web Start Client.

Prerequisites

You must configure STORM using the SPFS CLI tool for launching STORM manager from the IEMS client. For details, refer to *Nortel ATM/IP Solution-level Configuration*, NN10409-500. To access the STORM HTTPS graphical interface, the IEMS requires the SPFS HTTPS proxy to be configured. For details, refer to "Configuring the Apache Web Server for HTTPS" in *Nortel ATM/IP Solution-level Configuration*, NN10409-500.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select **Network Elements** under IEMS Topologies, then right-click the STORM map symbol and select **View Children**.
- 3 Right-click the desired STORM map symbol and select the required menu item. The menu items are listed in the following table.

Menu item	
Launch STORM Mgr	Launches the STORM Manager client. Communication with STORM Manager is enabled after authentication from the device.
Launch Command Line	Launches the CLI for communication with the remote device from IEMS using SSH.

- 4 You have completed this procedure.

—End—

Launching the CLI for a UAS NE

Application

Use this procedure to launch the Command Line Interface (CLI) for a UAS NE from IEMS Java Web Start Client.

Action

Step	Action
<i>At the IEMS workstation</i>	
1	Launch the IEMS Java Web Start Client (refer to " Launching the IEMS Java Web Start Client " (page 21)).
2	Select Network Elements under IEMS Topologies, then right-click the UAS map symbol and select View Children .
3	Right-click the desired UAS map symbol and select the Command Line menu item. <i>The CLI is launched. The access to the CLI is permitted after authentication by the device.</i>
4	You have completed this procedure.
—End—	

Launching the UNEM browser for UNEM

Application

Use this procedure to launch the UNEM browser for UNEM from IEMS Java Web Start Client.

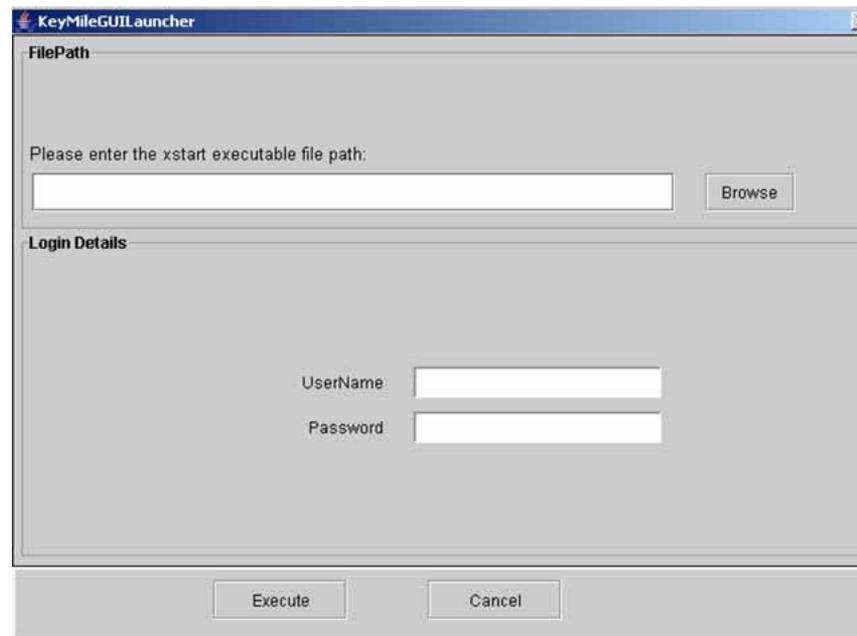
Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select the Element Managers topology in the IEMS Topologies tree.
- 3 Right-click the UNEM map symbol and select the **Launch UNEM Browser** menu item.

The system displays a window similar to the following screen shot for the IEMS Client in Microsoft Windows.



- 4 Click the **Browse** button to select the Exceed application xstart executable file path.
- 5 Type the user name and password in the respective fields.

- 6 Type the command location in the Command editable list box. The command is a shell file, which is present at the specified location.

Example

```
/usr/openwin/bin/xterm -display <Client_PC_IP>:0.0
/nem/unem/bin/private/mapgui
```

- 7 Click the **Execute** button to execute the specified command.
IEMS saves the location of the script or the executable file and commands in the client system from which the IEMS Java Web Start Client is launched.
- 8 You have completed this procedure.

—End—

Launching applications for a UMUX Manager

Application

Use this procedure to launch the UNEM browser for UMUX NEs (UMUX 1500, UMUX 1200, and UMUX 900) from IEMS Java Web Start Client.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select **Element Managers** in the IEMS Topologies tree.
- 3 Right-click the UNEM NE map symbol and select the **Launch UNEM Browser** menu item.
A UNEM Configuration window opens.
- 4 Click the **Browse** button to select the Exceed application xstart executable file path.
- 5 Type the user name and password in the respective fields.
- 6 Type the command location in the Command editable list box. The command is a shell file, which is present at the specified location.

Example

```
/usr/openwin/bin/xterm -display <Client_PC_IP>:0.0
/nem/unem/bin/private/mapgui
```

- 7 Click the **Execute** button to execute the specified command.
IEMS saves the location of the script or the executable file and commands in the client system from which the IEMS Java Web Start Client is launched.
- 8 You have completed this procedure.

—End—

Launching applications for a USP NE

Application

Use this procedure to launch the USP Manager or to launch the CLI for a USP NE from Java Web Start Client.

Prerequisites

To launch the USP Manager for USP NE, you must install the correct JRE version in the client workstation. For details, see [System requirements](#).

- To launch the USP Manager for USP NE, you must install the correct JRE version in the client workstation. For details, see System requirements.
- The USP or USPc GUI must be installed on the client server (for example the SPFS server). For details, refer to *Upgrading the USP*, NN10045-461 and *Upgrading USP - Compact*, NN10046-461.

Action

Step	Action
At the IEMS workstation	
1	Launch the IEMS Java Web Start Client (refer to " Launching the IEMS Java Web Start Client " (page 21)).
2	Select Network Elements under IEMS Topologies to display all grouped network element map symbols.
3	Right-click the grouped USP map symbol and select View Children .
4	Right-click the desired USP node and select the required menu item. The menu items are listed in the following table.

Menu item	
View Children	Displays the map symbols for configured units associated with the USP parent node. Once displayed, right-click on the desired unit and select the required menu item.

Menu item	
Launch USP Manager	Enables communication with the remote device from IEMS using SSH. Access to the USP Manager Client is permitted with Single Sign On (SSO).
Command Line	Launches the CLI for communication with the remote device from IEMS using SSH.

5 You have completed this procedure.

—End—

Using IEMS diagnostics

When the IEMS server starts up IEMS diagnostics is initiated. The result of the diagnostics can be viewed by the craftsperson. The results of the startup diagnostics of the IEMS server are recorded in the /opt/nortel/iems/current/logs/startserver.txt log file.

This subsection explains the following:

- "Checking the status of IEMS modules" (page 102)
- Checking the status of all the IEMS modules
- "Configuring IEMS diagnostics parameters" (page 110)

Checking the status of IEMS modules

Use this procedure to verify the following using the IEMS diagnostics script:

- status of the Apache server
- status of the Tomcat server
- minimum required heap size

Free heap size is the minimum threshold to be free out of the allocated JVM heap size (200 MB) when the IEMS server is running. The recommended minimum free heap size is specified in `diagnostics.xml` located in the `/opt/nortel/iems/current/conf` folder. If the minimum required free heap size is not available, a warning message is displayed. For details on configuring the IEMS CPU heap size, see "[Configuring IEMS diagnostics parameters](#)" (page 110).

- status of the IEMS server port
- IEMS database connection status
- status of southbound SNMP port
- IEMS CPU usage

The table space size can be checked for IEMS table space, performance table space and event table space. The recommended value for the IEMS table space and performance table space is specified in the `DBTableSpace_Size` parameter of `/opt/nortel/iems/current/conf/diagnostics.xml`. The recommended value for the event table is specified in the `maximum number of events` parameter of `DBcleanupJob`. The results for the check of each of the table space are displayed separately. For details on configuring IEMS table space size see "[Configuring IEMS diagnostics parameters](#)" (page 110).

The IEMS diagnostics script (`IEMSDiagnostics.sh`) is located under `/opt/nortel/iems/current/bin`.

To see the usage of IEMS diagnostics script (`IEMSDiagnostics.sh`), enter the following command:

```
# sh IEMSDiagnostics.sh
```

The following output appears:

```
Usage : sh IEMSDiagnostics.sh
ALL = All Tests
[1] = APACHE TEST
[2] = IEMS_TOMCAT Check
```

- [3] = HeapSizeCheck
- [4] = BE portCheck
- [5] = OracleDatabaseCheck
- [6] = SnmpPortCheck
- [7] = Database Table Space Check
- [8] = CPU Check
- [9] = NTSTD[North Bound Port] Check
- [10] = SCC2[North Bound Port] Check

Prerequisites

You must be a root user to perform the IEMS diagnostics script commands.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Telnet to the host where the IEMS server is running.
- 2 Enter the following command to switch to the /opt/nortel/iems/current/bin folder:

```
cd /opt/nortel/iems/current/bin
```

- 3 Select your next step.

If you want to check	
the status of the Apache server	the next step
the status of the Tomcat server	step 7
the minimum required heap size	step 10
the status of the IEMS server port	step 13
IEMS database connection status	step 16
the status of the southbound SNMP port	step 19
the IEMS CPU usage	step 22
the status of the NTSTD port	step 25
the status of the SCC2 port	step 28
the status of all the IEMS modules	step 31
the database table space	step 34

- 4 To check the status of the Apache server, enter the following command

```
# sh IEMSDiagnostics.sh 1
```

Please refer logs for Test Results >> <IEMS Home>/logs/diagnostics.txt

- 5** Type the following command to view the test results in diagnostics.txt present under the /opt/nortel/iems/current/logs folder:

```
# cat ../logs/diagnostics.txt
```

If the Apache Server is up and running, the following message is displayed:

```
Apache Test      : PASSED
Apache WebServer is running in port --> : 9090
```

If the Apache Server is down, the following message is displayed:

```
Server returned HTTP response code: 500 for URL:
http://192.168.118.252:9090/unauthenticatedservlets/
com.adventnet.nms.servlets.ConnectionCheckServlet
Apache Test     : FAILED: Apache port Not Listening
.. Please shutdown and restart the IEMS server
to start the tomcat server
```

To restart the IEMS server, refer to "Shutting down the IEMS server" and "Starting the IEMS server or changing the IEMS server mode to standby" in *IEMS Administration and Security*, NN10336-611.

- 6** You have completed this procedure.

- 7** To check the status of the Tomcat server, enter the following command:

```
# sh IEMSDiagnostics.sh 2
```

Please refer logs for Test Results >> <IEMS Home>/logs/diagnostics.txt

- 8** Type the following command to view the test results in diagnostics.txt present under /opt/nortel/iems/current/logs folder:

```
# cat ../logs/diagnostics.txt
```

If the Tomcat Server is up and running, the following message is displayed:

```
Tomcat Test     : PASSED
Tomcat server is running
```

If the Tomcat Server is down, the following message is displayed:

```
Server returned HTTP response code: 500 for URL:
http://192.168.118.252:9090/unauthenticatedservlets/
com.adventnet.nms.servlets.ConnectionCheckServlet
Tomcat Test     : FAILED: Tomcat port Not Listening
.. Please shutdown and restart the IEMS server
to start the tomcat server
```

To restart the IEMS server, refer to "Shutting down the IEMS server" and "Starting the IEMS server or changing the IEMS server mode to standby" in *IEMS Administration and Security*, NN10336-611.

- 9 You have completed this procedure.
- 10 To check the minimum required heap size, enter the following command:
- ```
sh IEMSDiagnostics.sh 3
```
- Please refer logs for Test Results >> <IEMS Home>/logs/diagnostics.txt
- 11 Type the following command to view the test results in diagnostics.txt present under /opt/nortel/iems/current/logs (<IEMS Home>) folder:
- ```
# cat ../logs/diagnostics.txt
```
- If the IEMS heap is below the minimum required heap size specified in the /opt/nortel/iems/current/diagnostics.xml, following message is displayed:*
- ```
Memory test-Application heap size : PASSED
```
- 12 You have completed this procedure.
- 13 To check the status of the IEMS server port, enter the following command:
- ```
# sh IEMSDiagnostics.sh 4
```
- Please refer logs for Test Results >> <IEMS Home>/logs/diagnostics.txt
- 14 Type the following command to view the test results in diagnostics.txt present under /opt/nortel/iems/current/logs (<IEMS Home>) folder:
- ```
cat ../logs/diagnostics.txt
```
- If the IEMS port is up, the following message is displayed:*
- ```
BE port check : PASSED -- LISTENING in port 2000
```
- If the IEMS port is down, the following message is displayed:*
- ```
BE port Test: FAILED port 2000 Not Listening ::
.... Please restart the IEMS server and try again
```
- To restart the IEMS Server, refer to "Shutting down the IEMS server" and "Starting the IEMS server or changing the IEMS server mode to standby" in *IEMS Administration and Security*, NN10336-611.
- 15 You have completed this procedure.

- 16 To check the IEMS database connection status, enter the following command:
- ```
# sh IEMSDiagnostics.sh 5
```
- Please refer logs for Test Results >> <IEMS Home>/logs/diagnostics.txt
- 17 Type the following command to view the test results in diagnostics.txt present under /opt/nortel/iems/current/logs (<IEMS Home>) folder:
- ```
cat ../logs/diagnostics.txt
```
- If the IEMS database connection is up, the following message is displayed:*
- ```
Database Connectivity check : PASSED
```
- 18 You have completed this procedure.
- 19 To check the status of the southbound SNMP port, enter the following command
- ```
sh IEMSDiagnostics.sh 6
```
- Please refer logs for Test Results >> <IEMS Home>/logs/diagnostics.txt
- 20 Type the following command to view the test results in diagnostics.txt present under /opt/nortel/iems/current/logs (<IEMS Home>) folder:
- ```
# cat ../logs/diagnostics.txt
```
- If the southbound SNMP port is up, the following message is displayed:*
- ```
SNMP TRAP PORT TEST :PASSED
```
- If the southbound SNMP port is down, the following message is displayed:*
- ```
Timed out. No more retries to
"192.168.118.252:162". RequestID: 1
Time: Wed Oct 20 18:25:22:581 EDT 2004
Request timed out.
SNMP Trap Cannot be received --> Please restart
IEMS server and try again
```
- 21 You have completed this procedure.
- 22 To check the CPU usage, enter the following command:
- ```
sh IEMSDiagnostics.sh 8
```
- Please refer logs for Test Results >> <IEMS Home>/logs/diagnostics.txt

- 23** Type the following command to view the test results in diagnostics.txt present under /opt/nortel/iems/current/logs (<IEMS Home>) folder:

```
cat ../logs/diagnostics.txt
```

*If the CPU usage is below the recommended maximum value, a message similar to the following is displayed:*

```
INFO : CPU usage is 3.3
```

*If the CPU usage exceeds the recommended maximum value, a message similar to the following is displayed:*

```
Warning Message : CPU usage 0.8 exceeds 0.7
```

- 24** You have completed this procedure.

- 25** To check the status of the NTSTD port, enter the following command:

```
sh IEMSDiagnostics.sh 9
```

Please refer logs for Test Results >> <IEMS Home>/logs/diagnostics.txt

- 26** Type the following command to view the test results in diagnostics.txt present under /opt/nortel/iems/current/logs (<IEMS Home>) folder:

```
cat ../logs/diagnostics.txt
```

*If the NTSTD port is up, the following message is displayed:*

```
NTSTD PORT CHECK : PASSED
```

*If the NTSTD port is down, the following message is displayed:*

```
NTSTD PORT CHECK : FAILED
```

- 27** You have completed this procedure.

- 28** To check the status of SCC2 port, enter the following command

```
sh IEMSDiagnostics.sh 10
```

Please refer logs for Test Results >> <IEMS Home>/logs/diagnostics.txt

- 29** Type the following command to view the test results in diagnostics.txt present under /opt/nortel/iems/current/logs (<IEMS Home>) folder:

```
cat ../logs/diagnostics.txt
```

*If the SCC2 port is up, the following message is displayed:*

```
SCC2 PORT CHECK : PASSED
```

*If the SCC2 port is down, the following message is displayed:*

SCC2 PORT CHECK : FAILED

**30** You have completed this procedure.

**31** To check the status of all the IEMS modules, enter the following command:

```
sh IEMSDiagnostics.sh ALL
```

Please refer logs for Test Results >> <IEMS Home>/logs/diagnostics.txt

**32** Type the following command to view the test results in diagnostics.txt present under /opt/nortel/iems/current/logs (<IEMS Home>) folder:

```
cat ../logs/diagnostics.txt
```

*If all the modules are up, a message similar to the following is displayed:*

```
Apache Test : PASSED
 Apache WebServer is running in port --> : 9091

Tomcat Test : PASSED
Tomcat server running

Memory test-Application heap size : PASSED

NorthBoundSNMP Port Check TEST : PASSED

BE port check : PASSED -- LISTENING in port 2000

Database Connectivity check : PASSED
***** SNMP TRAP PORT TEST
: PASSED

Used Table Space 22
Configured Database TableSpace >> 80
IEMS_TS TableSpace Test : PASSED

Used Table Space 1
Configured Database TableSpace >> 80
IEMS_PERF_TS TableSpace Test : PASSED

Event TableSpace Test : PASSED

NTSTD PORT CHECK = PASSED

SCC2 PORT CHECK = PASSED

```

- 33** You have completed this procedure.
- 34** To check the database table space, enter the following command:
- ```
# sh IEMSDiagnostics.sh 7
```
- Please refer logs for Test Results >> <IEMS Home>/logs/diagnostics.txt
- 35** Enter the following command to view the test results in diagnostics.txt present under /opt/nortel/iems/current/logs (<IEMS Home>) folder:
- ```
cat ../logs/diagnostics.txt
```
- If the table space is less than the recommended value, the following message is displayed:*
- ```
Used Table Space 22
Configured Database TableSpace .... >> 80
IEMS TS Database TableSpace Test : PASSED
*****
Used Table Space 1
Configured Database TableSpace .... >> 80
Perf TS Database TableSpace Test : PASSED
*****
Event TableSpace Test : PASSED
*****
```
- 36** You have completed this procedure.

—End—

Configuring IEMS diagnostics parameters

Use this procedure to configure the minimum free heap size, to configure the IEMS table space size or to configure IEMS CPU usage in the diagnostics.xml file.

Free heap size is the minimum threshold to be free out of the allocated JVM heap size (200 MB) when the IEMS server is running.

If the IEMS heap size and CPU usage exceed the recommended maximum value, a warning message is logged. The recommended maximum IEMS heap size is specified in diagnostics.xml.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Telnet to the host where the IEMS server is running.
- 2 Type the following command to switch to the /opt/nortel/iems/current/bin folder:

`cd /opt/nortel/iems/current/conf`
- 3 Open the diagnostics.xml file using a standard text editor (for example, "vi" in Sun Solaris).
- 4 Select your next step.

If you want to	go to
configure the minimum free heap size	the next step
configure IEMS CPU usage	step 7
configure the IEMS table space size	step 9

- 5 Change the "Free_HeapSize_InBytes" parameter value.
The default value specified in the diagnostics.xml is 3,000,000 bytes (approximately 3 MB).
- 6 Go to [step 10](#).
- 7 Change the Min_CPU_Size parameter value.
The default IEMS maximum CPU usage specified in the diagnostics.xml is 80%. The Min_CPU_Size parameter value must be less than 100.

- 8 Go to [step 10](#).
- 9 Change the DBTableSpace_Size parameter value.
The default recommended IEMS table space specified in the diagnostics.xml is 80%. The DBTableSpace_Size value must be less than 100.
- 10 Save the file.
- 11 Restart the IEMS server to implement the changes.
- 12 You have completed this procedure.

—End—

Running a ping test on the GWC network element or SPFS platform

Application

Use this procedure to run a ping test on the Gateway Controller (GWC) network element or SPFS platform from the centralized IEMS interface.

Only one remote operation (ping or traceroute) is permitted on each managed object at one time.

Prerequisites

This procedure has the following prerequisites.

- To perform this procedure on the GWC network element, you must belong to one or more of the following groups: mgcadm, mgcmtc, mgcrw. The GWCs must also be configured to allow the IEMS to communicate with them through SNMP. This is performed through the SAM21 manager (Configuration | Subnet Level Configuration | MIB Reader). The IEMS application server virtual IP address must be added as an allowed MIB reader.

When logged in as iemsadm the Launch Remote Ping menu is still visible, but the Remote ping will fail with the message: Could not retrieve su token for user: username.

- To perform this procedure on the SPFS platform the following conditions apply.
The ping and traceroute functionality is only supported for centralized users that are mapped to one or more of the following groups: emsadm, emsmtc, emsrw.
It is not supported for the iems emergency user iemsadm.

The iemsadm emergency user cannot perform Remote Ping or Remote TraceRoute operations.

- Centralized user accounts must be assigned a restricted access shell for command-line access to perform this procedure for SPFS platforms.
- The GWC network element or SPFS platform must have a software load of (I)SN09 or higher.
- The GWCs must be configured to allow the IEMS to communicate with them through SNMP.
 - select SAM21 manager from Element Managers group
 - right-mouse click and select SAM21 Mgr GUI menu
 - after successful login to the GUI select Configuration

- select Subnet Level Configuration and
- select MIB Reader

The IEMS application server's virtual IP address must be added as an allowed MIB reader.

Action

Step Action

At the IEMS workstation

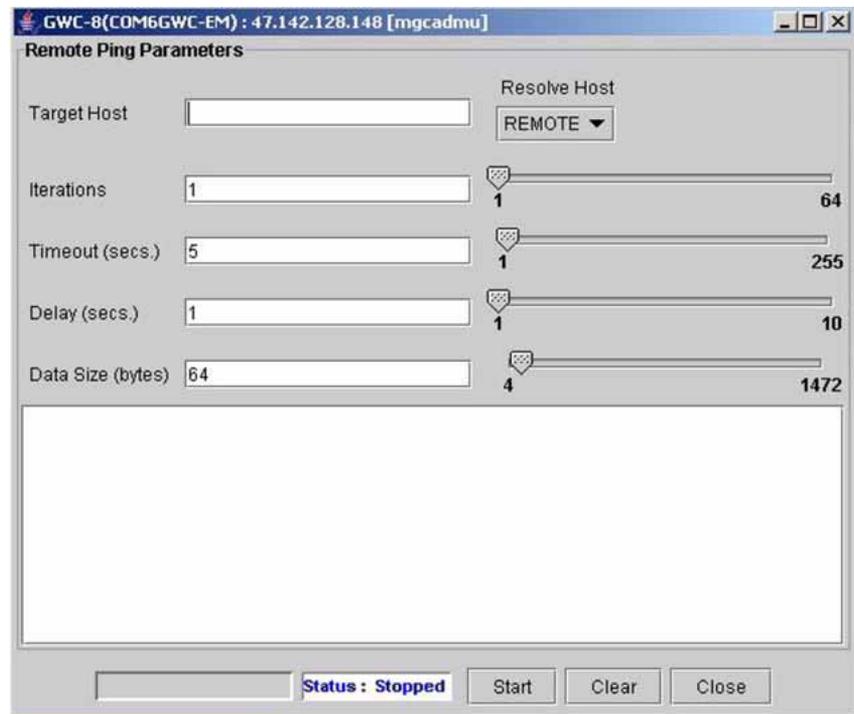
- 1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select your next step.

If you want to run a ping test on	
a GWC network element	go to step 3
an SPFS platform	go to step 5

- 3 Select **Network Elements** under IEMS Topologies, then right-click the GWC map symbol and select **View Children**.
- 4 Go to [step 6](#).
- 5 In the IEMS Topologies tree expand **SPFS** under **EMS Platforms** and select an SPFS unit.
- 6 Right-click the desired map symbol in the IEMS display panel and select **Launch Remote Ping**.

The Launch Remote Ping menu option only appears if you have the appropriate administration privileges.

The Remote Ping Parameters window opens.



- 7 Enter the host name or IP address of the destination host that you want to ping in the Target Host field.
- 8 Select the DNS resolution from the Resolve Host drop-down list. The target address resolution can use the name service of the client (LOCAL), or the name service of the remote launch host (REMOTE).
If DNS is not used, the client tries to resolve the host name or IP address using the default resolver on the client or remote device or platform.
- 9 Enter the number of times you want to repeat the command in the Iterations field.
- 10 Enter the timeout value (in seconds) for the remote host to use in the Timeout field.
- 11 Enter the delay (in seconds) to use between each ping operation in the Delay field.
- 12 Enter the data size (in bytes) of each ping probe packet to use in the Data Size field.
- 13 Click the **Start** button.
The response is displayed in the output display panel.
- 14 You have completed this procedure.

—End—

Running a traceroute on the GWC network element or SPFS platform

Application

Use this procedure to run a traceroute on the Gateway Controller (GWC) network element or SPFS platform from the centralized IEMS interface.

Only one remote operation (ping or traceroute) is permitted on each managed object at one time.

Prerequisites

This procedure has the following prerequisites.

- To perform this procedure on the GWC network element, you must belong to one or more of the following groups: mgcadm, mgcmtc, mgrcw. If you are not a member of one of these groups, the Launch Remote TraceRoute menu option is not visible.
- To perform this procedure on the SPFS platform, you must belong to one or more of the following groups: emsadm, emsmtc, emsrw. If you are not a member of one of these groups, the Launch Remote TraceRoute menu option is not visible.
- Centralized user accounts must be assigned a restricted access shell for command-line access to perform this procedure for SPFS platforms.
- The GWC network element or SPFS platform must have a software load of (I)SN09 or higher.

Action

Step	Action
------	--------

At the IEMS workstation

- | | |
|---|---|
| 1 | Launch the IEMS Java Web Start Client. Refer to " Launching the IEMS Java Web Start Client " (page 21). |
| 2 | Select your next step. |

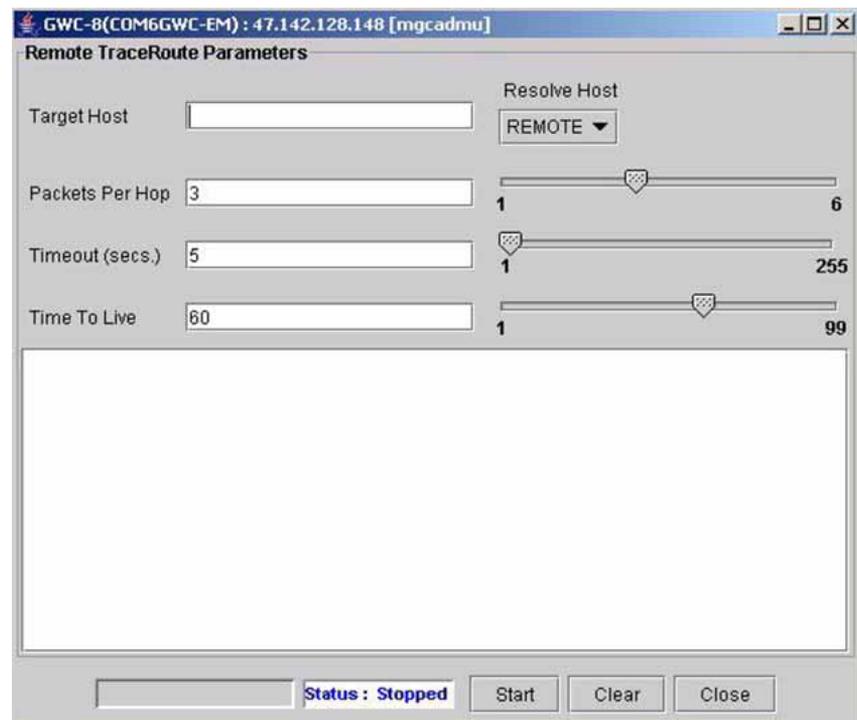
If you want to run a traceroute on	
a GWC network element	go to step 3
an SPFS platform	go to step 5

- | | |
|---|---|
| 3 | Select Network Elements under IEMS Topologies, then right-click the GWC map symbol and select View Children . |
|---|---|

- 4 Go to [step 6](#).
- 5 In the IEMS Topologies tree expand **SPFS** under **EMS Platforms** and select an SPFS unit.
- 6 Right-click the desired map symbol and select **Launch Remote TraceRoute**.

The Launch Remote TraceRoute menu option only appears if you have the appropriate administration privileges.

The RemoteTraceRoute Parameters window opens.



- 7 Enter the destination host name or IP address in the Target Host field.
- 8 Select the DNS resolution from the Resolve Host drop-down list. The target address resolution can use the name service of the client (LOCAL), or the name service of the remote launch host (REMOTE).
If DNS is not used, the client tries to resolve the host name or IP address using the default resolver on the client or remote device or platform.
- 9 Enter the number of packets for each hop in the Packets Per Hop field.

- 10 Enter the timeout value (in seconds) for the remote host to use in the Timeout field.
- 11 Enter the Time To Live (TTL) in the Time To Live field.
- 12 Click the **Start** button.
The response is displayed in the output display panel.
- 13 You have completed this procedure.

—End—

Overview of Core Element Manager integration with IEMS

This feature integrates the functionality of Core Element Manager (CEM) to the Integrated Element Management System (IEMS). CEM is an element manager for the CS 2000 core and Call Agent core. It provides Resource Discovery (RD), Fault Management (FM) and Performance Management (PM) support for the core. You can add, delete, and manage CEM from IEMS.

The Core Element Manager system is an Element Management System which provides the following:

- an exchange of data between a management application (CEM) and a core network element (SDM or CBM). The Core Element Manager is installed on a Sun platform.
- mediation functionality (data accumulation, filtering, manipulation, and transfer) between the CS 2000 Core or Call Agent Core network elements and the CEM workstation

CEM components

The CEM software includes the Core Element Manager GUI, the CEM Server, and the OMC-S in SDM/CBM. The following three components perform the performance management, configuration management, fault management, and security management functionality for the CS 2000 core or Call Agent core.

- The Core Element Manager browser runs on a PC or Sun platform. OAM&P personnel can use the GUI to manage the network elements.
- The Core Element Manager Server runs on a Sun Solaris platform.
- SDM/CBM is the mediation device which connects to the network element and gets raw data such as OMs, logs and also table data. SDM/CBM passes this information to the CEM server software.

The CEM store and forward process (SAF) framework:

- stores and forwards the SDM/CBM data on to the appropriate CEM server process
- synchronizes after disconnection from the CEM server process and the SDM/CBM

By default, the SAF process on the SDM/CBM is not in service after CEM is installed. The SAF process must be switched to the in service state.

For more information about the CEM SAF process, see CS 2000 Core Manager Overview, NN10018-111.

CEM GUI description

Fault Management

The Fault Management function (FM) displays logs of alarm or fault events that occur within the network, usually within a switch node. These alarms or events may have an impact on the overall service of the network element. The Fault Management function provides information about the network element so that you can perform further maintenance operations. Fault Management provides the following capabilities:

- displays alarms for a specific switch node. When a repeated alarm occurs for the same problem and the same resource, the most current alarm is shown. The previous alarms are stored as cleared alarms.
- displays a time-based histogram of alarm activity for time periods of 1 to 30 days. By default, the retention period is 30 days for uncleared alarms and 7 days for cleared alarms.
- displays alarms by selected severities (Critical, Major, Minor, Warning, unknown, or any combination)
- displays the element color to reflect the current alarm status
- displays alarms for specific filters
- provides alarm notifications as they occur
- exports alarm data to file
- prints alarm data
- provides filter criteria for alarms
- provides actions triggered by alarm

Fault management window

Severity	Date	Owner	Category	source	Log Key
Major	Sep 23,2005 10:...		communications	rtpo-mdm.us... C0000002	
Critical	Sep 23,2005 02:...		processingError	znc0s0tm-G... CMT301	
Major	Sep 23,2005 02:...		communications	0x000000630... GWC307	
Minor	Sep 23,2005 10:...		equipment	rtpo-mdm.us... 30110200	
Critical	Sep 23,2005 10:...		communications	rtpo-mdm.us... 70111100	
Critical	Sep 23,2005 10:...		communications	rtpo-mdm.us... 70111212	
Critical	Sep 23,2005 10:...		communications	rtpo-mdm.us... 70111212	
Critical	Sep 23,2005 10:...		communications	rtpo-mdm.us... 70111212	
Critical	Sep 23,2005 10:...		communications	rtpo-mdm.us... 70111212	
Critical	Sep 23,2005 10:...		communications	rtpo-mdm.us... 70111212	

Alarm count by severity				Category
21	276	21	6	other
3	2	2	3	qualityOfService
54	33	15	2	communications
32	30	42	519	equipment

Configuration Management

The Configuration Management function allows you to manage network elements within a circuit core network. The Configuration Management function identifies the configuration and status of the network when it is initialized. The network elements are identified by icons and are arranged according to the network hierarchy. The CEM displays complete information for each target network element and its subordinate elements. The configuration display is updated automatically by the Configuration Manager to maintain consistency between the Element Manager display and its managed objects. This display is called the containment tree.

The Configuration Manager includes the following features:

- Physical, Logical, Icon or List views from the Element Manager
- Pin and Unpin nodes
- nodes sorted by name or severity
- find carriers and linksets
- saving and retrieving of notes for nodes
- table access (add/read/delete/modify tuple operations)
- customs wizards to create/modify/delete trunks and other table access operations
- integration with performance management

- launch the Threshold Management window for a PM resource
- threshold management information for PM resources
- threshold crossed information
- performance management information for PM resources (pmCurrentData)
- print support for the Configuration Management window

Configuration Management window in list mode

The screenshot shows the 'Configuration Management window in list mode' in the Nortel Element Browser GEM17. The window title is 'Untitled-1 Nortel Element Browser GEM17'. The menu bar includes File, Fault, Configuration, Performance, Call Trace, Tools, Administration, and Help. The main area displays a table of alarms with the following columns: A, N, Element, Resource, Log, Probable Cause, Date/Time, and Cleared By. The table contains several rows of alarm data, including elements like EM-15K_PP405X and EM-15KVSS406Y. Below the table is a time-based alarm history chart showing a peak in activity around 16:00. The selected time range is Jul 27, 2003 00:30 to Jul 27, 2003 18:15, with a total of 687 alarms. At the bottom, there is a detailed view of a selected resource, showing columns for A, N, P, W, Element, Resource, Sub No..., State, and Alarm ...

A	N	Element	Resource	Log	Probable Cause	Date/Time	Cleared By
		EM-15K_PP405X	EM-15K_PP405X	00009000	softwareError	Jul 27, 2003 01:12:07	
		EM-15K_PP405X	EM-15K_PP405X	00009000	softwareError	Jul 27, 2003 03:12:08	
		EM-15K_PP405X	EM-15K_PP405X	00009000	softwareError	Jul 27, 2003 05:12:08	
		EM-15KVSS406Y	EM-15KVSS406Y	09990001	equipmentFailure	Jul 27, 2003 06:56:50	
		EM-15KVSS406Y	EM-15KVSS406Y	TMN610		Jul 27, 2003 06:57:17	
		EM-PP394_15K	TIME	70150000	remoteTransmissionError	Jul 27, 2003 12:00:01	
		EM-15K_PP405X	EM-15K_PP405X	00009000	softwareError	Jul 27, 2003 13:12:10	
		EM-15K_PP405X	EM-15K_PP405X	00009000	softwareError	Jul 27, 2003 15:12:11	
		EM-PP394_15K	IP.11	09990012	probCauseUnknown	Jul 27, 2003 15:47:39	

Performance Management

The Operational Measurements (OM) system provides the following measurements for the Circuit Core Networks (CCN) Call Server:

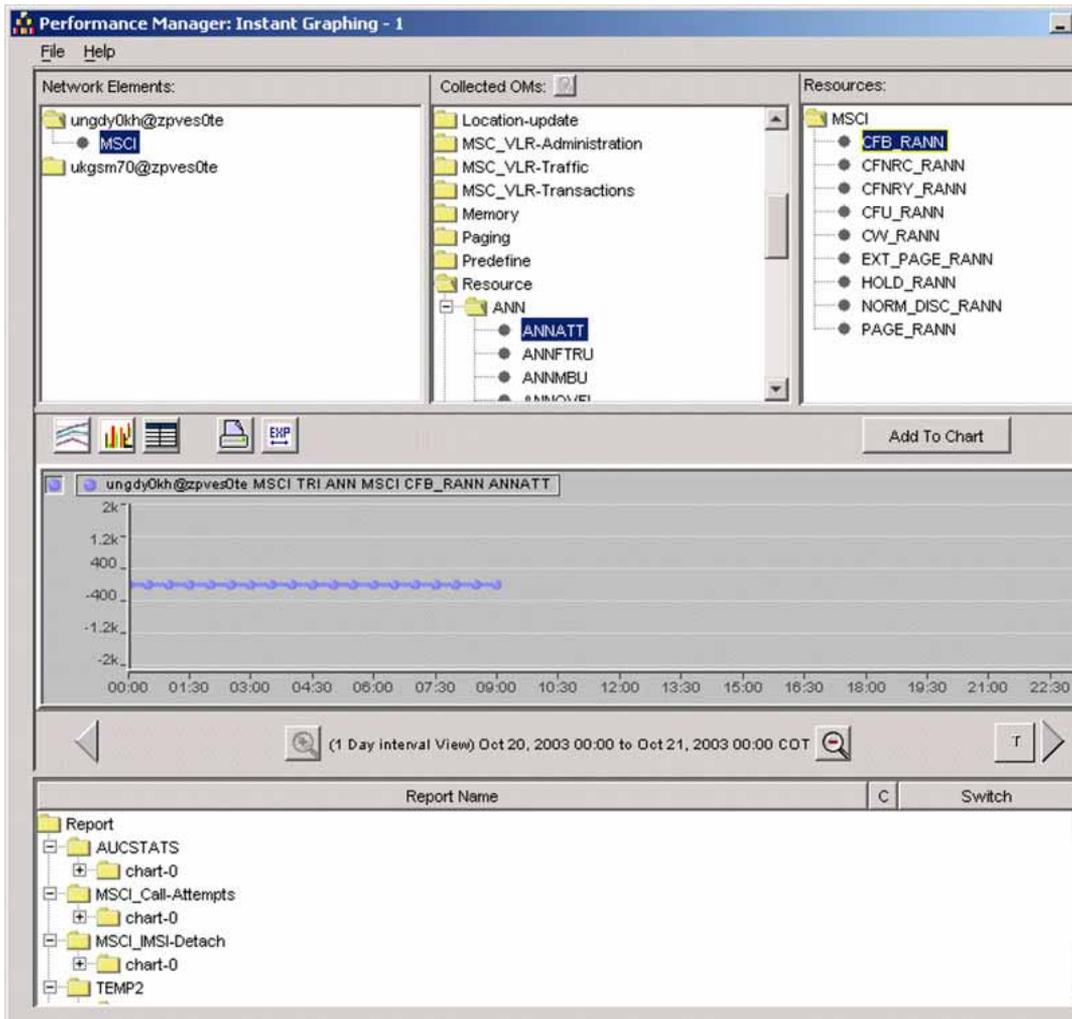
- traffic measurements
- service data

You can view OM records to ensure that the CS switch operates at its fullest potential with optimum efficiency. New OM data is transferred from the switch every transfer period.

The Performance Management functionality does the following:

- provides access to OMs in predefined measurement groups
- displays OMs in operator-configurable studies, including a graph of specific OMs over a given time frame
- configures real-time updates of OMs with the CS transfer period as the minimum update frequency
- displays data from multiple network elements on the same graph
- displays errors such as incomplete OM data for the requested study
- sends the output display to print
- allows OM threshold settings
- displays summary reports on network elements

Performance Management: Instant graphing window



Performance Management: Threshold Manager window

The screenshot shows the Threshold Manager window with the following components:

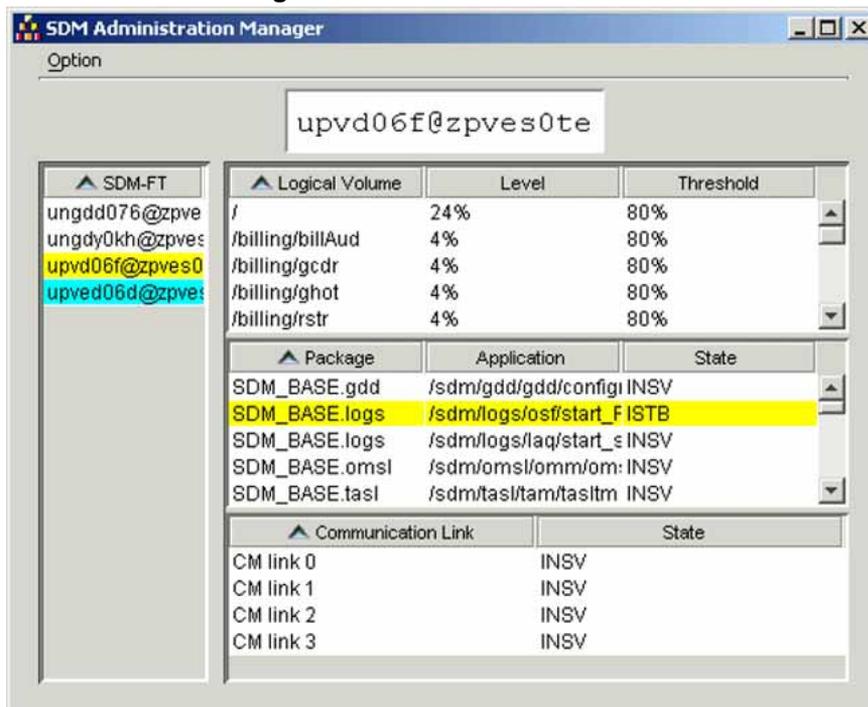
- Network Elements:** A tree view showing a hierarchy starting with 'ungdy0kh@urc2y13c', followed by 'MSCI', '_ALL_NES_TRI', and 'mdm@urc2y13c'. Under 'mdm@urc2y13c', several EM-PP entries are listed, with 'EM-PP289_15K' selected.
- Collected OMs:** A tree view showing a hierarchy starting with 'H248', followed by a list of OMs including 'addRequests', 'addResponses', 'auditValueRequests', 'auditValueResponses', and various 'errorCode' entries.
- Resources:** A tree view showing a hierarchy starting with '~MDM-mdm', followed by 'EM-PP289_15K', and then a list of NSTA entries (NSTA-2 through NSTA-7), with 'ALL_RESOURCES' selected.
- Threshold Summary for:** A table showing the current value and thresholds for various OMs.
- Threshold Editing:** A section for editing thresholds, currently empty.
- Buttons:** 'Reset', 'Apply', and 'Close' buttons at the bottom.

Field	Current Value	Critical		Major		Minor		Warning		Direction (+/-)	En
		Raise	Clear	Raise	Clear	Raise	Clear	Raise	Clear		
addRequests	unknown	0	0	0	0	0	0	0	0	+	
addResponses	unknown	0	0	0	0	0	0	0	0	+	
auditValueRequests	unknown	0	0	0	0	0	0	0	0	+	
auditValueResponses	unknown	0	0	0	0	0	0	0	0	+	
errorCode400Tx	unknown	0	0	0	0	0	0	0	0	+	
errorCode401Tx	unknown	0	0	0	0	0	0	0	0	+	
errorCode402Tx	unknown	0	0	0	0	0	0	0	0	+	
errorCode403Tx	unknown	0	0	0	0	0	0	0	0	+	
errorCode406Tx	unknown	0	0	0	0	0	0	0	0	+	
errorCode410Tx	unknown	0	0	0	0	0	0	0	0	+	
errorCode411Tx	unknown	0	0	0	0	0	0	0	0	+	

Security Management

It is necessary to restrict access to the CEM browser to only users with valid login credentials. The security framework on the CEM system is provisioned with the functionality such as the following:

- login to access the CEM browser
- encrypted login credentials
- account lockout due to consecutive failed login attempts
- change password capability
- configuration of the telnet or FTP session
- time-out interval periods
- generates security alarms and event logs

Administration Manager main window**Commissioning Manager**

After installing the CEM package onto a Sun server, you must set up managed node instances in order to manage network elements. The Commissioning Manager is used to configure coreEMS managed node instances, such as to create, reconfigure and delete a managed node instance. Use the Commissioning Manager command line user interface to configure managed node instances.

For details about how to launch the Commissioning Manager CLI, see ["Launching a CEM Commissioning Manager CLI" \(page 37\)](#). For details about creating and deleting managed node instances, see [Creating a CEM managed node instance](#) and [Deleting a CEM managed node instance](#) in *IEMS Configuration*, NN10330-511.

Overview of high availability & co-residency

OAM&P operations are business critical and require uninterrupted high availability service. IEMS is the centralized authentication server and the GUI for launching applications, fault, performance feeds and some element management functions. Deploying IEMS on a HA platform is recommended for all customers. SPFS-HA provides a high availability middleware for all SPFS applications. IEMS uses SPFS-HA to provide high availability on the Sun N240 hardware platform.

SPFS-HA implements the active-inactive cold start model where applications along with their dependent services are running on one node. They are restarted on a secondary node upon failover.

SPFS-HA supports a simple two-node cluster. Each SPFS-HA cluster has three TCP/IP addresses associated with it. One IP address and its matching host name uniquely identify each node in the cluster (active and inactive node) and one IP address identifies the SPFS-HA cluster.

IEMS is supported both as a standalone application and coresident with CS2M and APS.

- As a standalone application two separate SPFS-HA clusters are required (one SPFS-HA cluster for CS2M with or without APS, and one SPFS-HA cluster for IEMS). Four Sun N240 servers are required to support this configuration (two Sun N240 servers to support the CS2M with/without APS cluster and two Sun N240 servers to support the IEMS cluster)
- When IEMS is co-resident with CS2M with/without APS one SPFS-HA cluster is required. Two Sun N240 servers are required to support this configuration.

Platforms with HA and co-residency support

IEMS and CS 2000 Core Manager on SPFS are available with HA and co-residency on the following platforms:

- On single N240 (simplex) 4G
- On dual N240 (HA) 4G
- On single T1400 (simplex) 4 Gig only - NTRX51KW. For existing T1400 platform versions, a T1400 upgrade is required.

Reconnecting Java Web Start client with the server

If the IEMS server is stopped or shut down in unforeseen circumstances, the IEMS Java Web Start Client tries to connect to server for a certain period (shown in the following figure). The maximum amount (in seconds) for which the IEMS Java Web Start tries to reconnect the IEMS Server is called the maximum retry period.

Client reconnection to server dialog



The progress bar shows that the IEMS Java Web Start Client is trying to reconnect to the IEMS Server. If the IEMS Java Web Start Client successfully establishes the IEMS Server, the Client Reconnection to Server window is closed. After the Maximum Retry Period is reached, the IEMS Java Web Start Client disconnects the IEMS Server and launches the Client reconnection dialog box.

The maximum retry period can be modified using the `MAX_RETRY_PERIOD` parameter in `clientparameters.conf` under the `/opt/nortel/iems/current/conf` directory. For details, refer to "Configuring the client retry time" in *IEMS Security and Administration*, NN10336-611.

Exiting the Java Web Start Client while reconnecting to the server

To exit the Java Web Start Client while the client is reconnecting to the server, click the **Exit** button in the Client reconnection dialog box.

Replicating data for high availability

The files essential for High Availability (HA) have to be replicated by SPFS HA. The following directories (including files in the sub-directories) under /opt/nortel/iems/current/ are replicated by SPFS HA when the active node fails and the inactive node is made active.

- oidtemplates
- state
- perfdata

The state of the failed node must be maintained by the node which was recently made active.

Using Java Web Start Client features

IEMS Java Web Start Client provides other features, such as context sensitive help, changing the look and feel of the client, using custom view filtering criteria, sorting data, and broadcasting messages to clients.

Viewing context sensitive help

Context sensitive help directs the user to an appropriate help section, which provides the specific information about the feature of the IEMS Java Web Start Client in use.

To launch IEMS Help documentation, select **Help-->Help Contents**. The complete IEMS Help Documentation in HTML format is launched in the default browser that has been configured in your system.

To launch context sensitive help in IEMS Java Web Start Client GUIs:

- Press **F1** on any screen
- OR
- Click the **Help** button on the toolbar in a screen.

Performing either of the above actions invokes the help section associated with the current screen. For example, if you press F1 while working on the Fault Management panel, a help file that explains Fault Management opens in a Web browser (the system default browser).

Some of the Client GUI dialog boxes also contain a Help button that gives context-sensitive help on that dialog box.

The browser is not invoked when trying to access help from IEMS Java Web Start Client. The Java Web Start path does not include the default browser, a situation which occurs on Sun Solaris platforms. To correct the situation, in the Java Web Start Application Manager, provide the required command (that is, to invoke the browser from the command line) in the Path field of the General tab.

Configuring the look and feel of Java Web Start Client

Application

Use this procedure to configure the look and feel of Java Web Start Client.

The look and feel of different components in the GUI are different for different platforms, such as Microsoft Windows or Sun Solaris. The default system color of the desktop background, text, caption, and other components can be different depending on the platform.

IEMS Java Web Start Client supports three different types of look and feel:

- Metal (the default look and feel)
- CDE/Motif
- Windows

Prerequisites

No prerequisites are required for this procedure.

Action

Step	Action
------	--------

At the IEMS workstation

- | | |
|---|---|
| 1 | Launch the IEMS Java Web Start Client. Refer to " Launching the IEMS Java Web Start Client " (page 21). |
| 2 | Select the option you require from the Look and Feel menu in Java Web Start Client. |
| 3 | You have completed this procedure. |

—End—

Using the broadcast message feature of Java Web Start Client

Application

Use this procedure to broadcast a message to all the clients connected to the IEMS server.

If two or more messages are sent simultaneously or continuously, the latest messages are appended below the earlier message.

Action

Step	Action
------	--------

At the IEMS workstation.

- 1 To invoke the IEMS Java Web Start Client, refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).
- 2 Select the **File-->Broadcast Message** menu command.
The Broadcast Message window is launched.
- 3 Type the message to be broadcast.
- 4 Ensure that the **Send to all client** option is selected. By default, the **Send to all client** option is selected.

The "Send to my FE client only" option in IEMS has the same function as 'Send to all client' option since in IEMS there is only one FE (Front End) server which services all clients. Later, multiple FE servers can be set up. As the client gets more accustomed to sending broadcast messages this option can be used to only contact clients that are being serviced by the same FE server.
- 5 Click the **BroadCast** button to send the message.
The message is shown in the Broadcast Message window with time, month and day of broadcast.
- 6 Click the **Close** button to close the dialog.
- 7 You have completed this procedure.

—End—

Showing or hiding the toolbar in Java Web Start Client

The toolbar can be hidden using the Show/Hide Toolbar toggle button at the top of the tree to provide an enlarged view of the frame. This feature hides the whole toolbar, not just some of the tools. To launch the IEMS Client, refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).

A tool tip "Hide Toolbar" indicates when the toolbar is visible and "Show Toolbar" indicates when it is hidden. To hide the toolbar, click the Show/Hide Toolbar toggle button. The toggle button changes from vertical to the horizontal position.

Using the IEMS tree

This subsection contains the following procedures:

- ["Adding a tree node" \(page 134\)](#)
- ["Adding user-defined properties" \(page 136\)](#)
- ["Modifying a tree node" \(page 137\)](#)
- ["Removing a tree node" \(page 138\)](#)
- ["Moving a tree node" \(page 139\)](#)

You can add a node anywhere in the tree by specifying the parent node of the node to be added. The menus for the parent and child nodes need not be the same; the child node can have the same tree popup menu as that of the parent node, or any other tree popup menus. To launch the IEMS Client, refer to ["Launching the IEMS Java Web Start Client" \(page 21\)](#).

This IEMS tree fulfills the "Any Node Anywhere" concept, whereby different node types can exist under a parent node. You can place a node in the tree using the Tree Operations menu specific to the frame or using the standard IEMS Java Web Start Client menu. Use the Tree Operations menu (or Node Operations option in the File menu) to complete the procedures in this subsection.

Adding a tree node **Application**

Use this procedure to add a tree node.

The Add Node option opens the Add Tree Node property form. This form allows you to specify the Tree Node Attributes, Panel Attributes, and Frame Attributes. Certain fields are mandatory and you must specify the default values, namely parent node, Tree Name, Panel Name, and popup Menu File Name.

If you do not specify the default properties, the system displays an error message. For example, if you omit the Panel Name, the error message states: "Panel Name is empty. Please give a valid entry".

The user-defined properties for the added node can also be added, modified, or removed at any point. You can add the key and the value into the table for a particular node.

Action

Step Action

At the IEMS workstation

- 1 Select the **File-->Node Operations-->Add Node** menu command.
The Add Tree Node property form launches.
- 2 Select the parent node from the Parent Node drop down to which the child has to be added from the drop-down tree.
- 3 Type the Panel Name, Tree Name, and Menu File Name of the node to be added (mandatory fields).
- 4 Type any other properties required (Action on Close, Icon File Name, Tree Popup Menu, Frame Title, Class Name).
- 5 If user-defined properties are required, add the property key and property value in the user-defined property form.
- 6 Click the **Apply** button to add the node under the specified parent node.
- 7 You have completed this procedure.

—End—

Example: Adding an alarm node under Network Events

Step Action

At the IEMS workstation

- 1 Select the **File-->Node Operations-->Add Node** menu command.
The Add Tree Node property form launches.
- 2 Select the Network Events node from the Parent Node drop down list.
- 3 Type the tree name "Alarms Test" and the panel name "com.adventnet.nms.alertui.AlertApplet".
- 4 Type the menu file name "alarismenu.xml" and select the Action on Close to be "Dispose only".
- 5 Select the tree icon file name images/alarms.png, and the tree popup menu Custom View, frameoptions.xml".
- 6 Type the frame title "Alarms".

- 7 Click the **Apply** button.
The Alarms Test node is added into the tree with the above-defined attributes as its values.
- 8 Click the **Close** button to close the dialog after applying the changes.
- 9 You have completed this procedure,

—End—

Adding user-defined properties

Application

Use this procedure to add user-defined properties.

If the default properties shown in IEMS are not sufficient for your requirements, you can add additional user-defined properties as required. You can include these user-defined properties when adding a node to a tree. You can later add, modify, or delete the user-defined properties.

Action

Step Action

At the IEMS workstation

- 1 Select the **File-->Node Operations-->Add Node** menu command.
The Add Tree Node property form launches.
- 2 Select the parent node from Parent Node drop down to which the child has to be added from the drop-down tree.
- 3 Type the Panel Name, Tree Name, and Menu File Name of the node to be added (mandatory fields).
- 4 Type any other properties required (Action on Close, Icon File Name, Tree Popup Menu, Frame Title, Class Name).
- 5 Click the **Next** button.
The user-defined property form is launched.
- 6 Type the property key (for example, FRAME-TITLE).
- 7 Type the property value (for example, Frame Title)
- 8 Click the **Add** button.

The system adds the user-defined properties to the database, and displays the properties in the table. You can add any number of user-defined properties.

- 9 You have completed this procedure.

—End—

Modifying a tree node

Application

Use this procedure modify a tree node.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Select the **File-->Node Operations-->Add Node** menu command.
The Add Tree Node property form launches.
- 2 Select the parent node from Parent Node drop down to which the child has to be added from the drop-down tree.
- 3 Type the Panel Name, Tree Name, and Menu File Name of the node to be added (mandatory fields).
- 4 Type any other properties required (Action on Close, Icon File Name, Tree Popup Menu, Frame Title, Class Name).
- 5 Click the Modify Node option to change the properties of the node.
- 6 Modifying the default and the user-defined properties.

Example

Change the icon files tick.png and alarms.png from
/opt/nortel/iems/current/images.

Change the pop-up menu filename to Custom Views alone. The node properties are modified.

- 7 Click the **Apply** button
The properties of the selected node are changed.
- 8 You have completed this procedure.

—End—

Removing a tree node

Application

Use this procedure to remove any node from the tree.

The following nodes are default nodes and must not be removed from the tree:

- IEMS Topologies
 - Network Elements
 - Element Managers
 - EMS Platforms
 - EMS Applications
- Fault Management
 - Network Elements
 - Alarms
- Performance
- Inventory
- Administration tools

Action

Step	Action
------	--------

At the IEMS workstation

- | | |
|----------|--|
| 1 | Select the File-->Node Operations-->Remove Node menu command to launch the Remove Tree Node dialog. |
| 2 | Select the tree node to be removed from the drop-down tree of the GUI. |
| 3 | Click the Apply button.
<i>The node is removed from the tree.</i> |
| 4 | You have completed this procedure. |

—End—

Moving a tree node

Application

Use this procedure to move a node in the tree. The Move Node option allows you to position the node anywhere in the tree.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Select the **File-->Node Operations-->Move Node** menu command to launch the Move Tree Node dialog.
- 2 Select the tree node to be moved from the Select the Tree Node to be moved combo box.
- 3 Select the tree node to be moved from the Select the Destination Tree Node combo box.
- 4 Enter the required index in Node Index field.
- 5 Click the **Apply** button to save the changes.
- 6 Click the **Close** button to close the dialog after applying the changes.
- 7 You have completed this procedure.

—End—

Using the LED indicator

The LED indicator is located at the bottom left-hand corner of the screen in the status bar). To launch the IEMS Client, refer to the section "[Launching the IEMS Java Web Start Client](#)" (page 21).

The indicator contains three LEDs representing (in order from left to right) Events, Alarms, and Inventory. The LEDs show the severity of the latest network event, alarm, and inventory.

Setting the theme for Java Web Start Client

Application

Use this procedure to set the theme for the IEMS Java Web Start client.

Themes control the appearance of the GUI components, for example, the icons and fonts used. They can also change the feel of your IEMS environment, allowing you to define your own unique menu styles and window borders.

Prerequisites

To set the themes, the Look And Feel of the client GUI must be set to the default value, Metal.

Action

Step	Action
<i>At the IEMS workstation</i>	
1	Launch the IEMS Java Web Start Client (refer to " Launching the IEMS Java Web Start Client " (page 21)).
2	Select the Tools-->Themes menu command. <i>The Themes Configurator GUI listing all the themes is launched.</i>
3	Click on the required theme from the Theme Name field.
4	Click the Apply button to save the changes.
5	Click the Close button.
6	You have completed this procedure.

—End—

Using custom view filtering criteria

This subsection gives tips for using the custom view filtering criteria to filter events, alarms, and inventory. To launch the IEMS Client, refer to ["Launching the IEMS Java Web Start Client" \(page 21\)](#). For procedure to add custom view for various GUIs, refer to following subsections:

- Managing custom views for events in *IEMS Fault Management*, NN10334-911.
- Managing custom views for alarms in *IEMS Fault Management*, NN10334-911.
- Adding custom topology node in *IEMS Configuration*, NN10330-511.
- Creating a custom view for the inventory panel in *IEMS Configuration*, NN10330-511.

The following is the list of custom views filtering criteria for Events, Alarms, and Inventory View panels of IEMS:

- Most of the properties listed while adding a custom view are string-based. Additionally, if there is a boolean, the properties form indicates a choice box containing three items: "all", "true", and "false". Selecting "true" or "false" has the expected behavior and selecting "all" means the condition is not required.
- For string-based properties, the string value is matched exactly. For example, the string "CS 2000" matches the exact word only.
- The wildcard '*' (asterisk) is supported to replace one or more characters. For example, to view objects whose names start with "sa", you specify the filter criterion as "sa*". Similarly, to view objects whose names end with "com", you specify the criterion as "*com".
- The wildcard "?" is not supported and is treated as an ordinary character.
- To specify multiple criteria for the same property, separate them with a comma. For example, if you want to view objects named USP-Mgr1, USP-Mgr2, and USP-Mgr3, specify them as USP-Mgr1, USP-Mgr2, and USP-Mgr3.
- Status and Severity are also treated as strings. For example, for a filter of Alarms with severity Critical, you specify the criterion "crit*".
- To exclude an item from the filter criteria, add a '!' (exclamation mark) character before it. For example, to view objects which do not start with "sa", specify the property as "!sa*". To view all Alarms except those with severity Warning or Clear, enter any of the following:
 - !war*, !cle* or

- !warning, !clear or
 - cr*, maj*, mino* or
 - critical, major, minor
- In Alarms and Events panel, filtering based on time can be done by specifying the start time and the end time. The formats for specifying the time are as follows:
 - MON DD,YYYYHH:MM:SS AM/PM, for example Mar 27,1998 12:24:12AM and
 - MONTH DD,YYYYHH:MM:SS AM/PM, for example March 27,1998 12:24:12 AM. The incompatibility is due to different JVM versions on client and server sides.
 - It is advisable to leave unused filter criteria fields blank.
 - After defining the filter criteria, you can optionally give the filter a name for future reference and then select the ApplyFilter option. The client then sends a request to the server to filter the objects, while it adds the name of the filter to the tree in the main panel.
 - The time taken for filtering depends on the total number of objects, the complexity of the filter criteria, and the mode of storage.
 - After creation, custom views continue to be updated and navigable for additions/deletions until the client is closed or the custom view is removed using the Remove Custom Views option.

Use the custom views with caution and remove any unnecessary ones. This facilitates quicker updates and clearing of resources associated with each custom view, both on the Client side and the Server side.

Sorting data in Java Web Start Client

Sorting is arranging the data displayed in the panels in ascending order or descending order.

Column sorting

Every column within the following panels can be sorted by clicking the column heading.

- Network Events
- Alarms
- Configured Collection
- Inventory
 - EMS
 - Platform
 - Application
 - NE

There are two types of sorting:

- Server-side sorting
- Client-side sorting

Both server-side and client-side sorting can be done for one column as required. These sort methods are indicated by a combination of the indicators described as follows.

Server-side sorting

A blue triangle (shown in the following table) indicates the entire column is sorted in descending order. An inverted blue triangle (shown in the following table) indicates the entire column is sorted in ascending order. Server-side sorting sorts the complete data.

Example

If the server contains 100 events, performing a server-side sort reorders the complete set of 100 events in the server. To carry out a server-side sort, click on the column header. Repeated clicks on the same column header sort the data in ascending and descending order, alternately.

The sort indicators for server-side sorting are ascending and descending are as specified in the table below.

Icon	Order of sorting
	Ascending
	Descending

Client-side sorting

Client-side sorting sorts the data displayed in the Event Viewer. When the topology/panel contains many entries, you may want to limit your sort to the entries currently displayed. Click the **Ctrl** (Control) key and click on the column to be sorted. A green triangle (shown in the following table) indicates the displayed contents within the column are sorted in descending order. An inverted green triangle (shown in the following table) indicates the displayed contents within the column are sorted in ascending order.

Example

If the server contains 100 events, of which 10 are displayed in the Event Viewer, performing a client-side sort reorders only the events displayed in the Event Viewer. To carry out a client-side sort, press the **Ctrl** (Control) key and click on the column header. Repeated clicks on the same column header sort the data in ascending and descending order, alternately. The sort indicators for ascending and descending as specified in the table below.

Icon	Order of sorting
	Ascending
	Descending

Description of IEMS operational measurements

This section describes the IEMS operational measurements which are collected from the IEMS software. All of the operational measurements templates are located in the /opt/nortel/iems/current/oidtemplates folder.

Number of active clients

The "numOfActiveClients" parameter gives the number of active IEMS Clients connected to the IEMS server. It includes both the IEMS Java Web Start Client and Web Client. This parameter is present in iems_client.xml which is located in the /opt/nortel/iems/current/oidtemplates folder.

Used table space

The used table space for the specified table name can be queried using the "usedTableSpaceInBytes" or "usedTableSpaceInPercent" parameters in iems_database.xml which is located in the /opt/nortel/iems/current/oidtemplates folder. The description of these parameters are explained in the following sections:

Used table space in bytes

The "usedTableSpaceInBytes" parameter gives the size of the table space occupied in bytes.

Used table space in percentage

The "usedTableSpaceInBytes" parameter gives the table space used size in percentage.

Fault operational measurements

The description of the fault operational measurements are described in the following sections. All the fault operational measurement parameters are present in iems_fault.xml which is located in the /opt/nortel/iems/current/oidtemplates folder.

Total number of events

The "numOfEvents" parameters gives the total number events in the IEMS database.

Average event throughput rate

The event throughput rate is the rate at which the IEMS receives the events. This event rate is calculated per second basis. The "avgEventThroughputRate" parameter gives the average event rate on a given time interval.

Maximum event throughput rate

The "maxEventThroughputRate" parameter is the maximum value in the event rates on a given time interval.

Total number of events added

The "numOfEventsAdded" parameter gives the total number of events added to IEMS database on a given time interval.

Total number of events discarded

The "numOfDiscardedEvents" parameter gives the total number of events discarded by IEMS on a given time interval.

Total number of events from unknown devices

The "numOfEventsFromUnknownDevices" parameter gives the total number of events from unknown devices. The following sections describes the events from unknown devices parameters with SNMP or Custlog interfaces.

Number of events from unknown devices as SNMP traps

The "numOfEventsFromUnknownSNMPDevices" parameter gives the total number of events from unknown devices as SNMP traps.

Number of events from unknown devices as Custlog messages

The "numOfEventsFromUnknownCustlogDevices" parameter gives the total number of events from unknown devices as Custlog traps.

Event rate from a device

The "eventRate" parameter gives the rate of events from a specific device. The "eventRateDetails" parameter gives the details of rate of events.

Number of alarms added

The "numOfAlarmsAdded" parameter gives the total number of alarms added to IEMS database on a given time interval.

Total number of alarms based on severity

The parameters in the following table gives the corresponding total of alarms of the severity specified in the Severity column.

Parameter	Severity
numOfMinorAlarms	Minor
numOfWarningAlarms	Warning
numOfCriticalAlarms	Critical
numOfMajorAlarms	Major

Total number of active alarms

The "numOfActiveAlarms" parameter gives the total number of active alarms in IEMS database.

Total number of cleared alarms

The "numOfAlarmsCleared" parameter gives the total number of alarms cleared.

Heap size measurements

The heap size measurements for IEMS can be queried using the "applicationHeapSize" or "maxApplicationHeapSize" parameters in iems_memory.xml which is located in the /opt/nortel/iems/current/oidtemplates folder. The description of these parameters are explained in the following sections:

Application heap size

The "applicationHeapSize" parameter gives the current heap (memory) size taken by the IEMS.

Maximum application heap size

The "maxApplicationHeapSize" parameter gives the maximum heap size reached during the given time interval.

Performance management measurements

The description of the performance management operational measurements are described in the following sections. All the performance management operational measurement parameters are present in iems_performance.xml which is located in the /opt/nortel/iems/current/oidtemplates folder.

Number of attributes collected

The "numOfAttributesCollected" parameter gives the total number of attributes collected by the IEMS performance management jobs.

Number of attributes collected for an interval

The "numOfAttributesCollectedOverThisInterval" parameter gives the total number of attributes collected by the IEMS performance management jobs on a given time interval.

Number of jobs provisioned

The parameters in the following table gives the corresponding total number of jobs in IEMS for a job type in the Job type column.

Parameter	Job type
numOfTransferJobsProvisioned	Transfer job
numOfCollectionJobsProvisioned	Collection job
numOfReportsJobsProvisioned	Report job

Number of successful jobs

The parameters in the following table gives the corresponding total number of successfully completed jobs in IEMS for the specified time interval in the Time interval column.

Parameter	Time interval
numOf24HrSuccessfulJobs	24 hours
numOf12HrSuccessfulJobs	12 hours
numOf60MinSuccessfulJobs	60 minutes
numOf30MinSuccessfulJobs	30 minutes
numOf15MinSuccessfulJobs	15 minutes
numOf5MinSuccessfulJobs	5 minutes

Number of failed report jobs

The "numOfFailedReportJobs" parameter gives the total number of failed Report jobs in the IEMS.

Number of failed collection jobs

The parameters in the following table gives the corresponding total number of failed collection jobs in IEMS for the specified time interval in the Time interval column.

Parameter	Time interval
numOf24HrFailedCollectionJobs	24 hours
numOf12HrFailedCollectionJobs	12 hours
numOf60MinPartialSuccessfulJobs	60 minutes
numOf30MinFailedCollectionJobs	30 minutes
numOf15MinFailedCollectionJobs	15 minutes
numOf5MinFailedCollectionJobs	5 minutes

Number of failed Transfer jobs

The parameters in the following table gives the corresponding total number of failed Transfer jobs in IEMS for the specified time interval in the Time interval column.

Parameter	Time interval
numOf24HrFailedTransferJobs	24 hours
numOf12HrFailedTransferJobs	12 hours
numOf60MinFailedTransferJobs	60 minutes
numOf30MinFailedTransferJobs	30 minutes
numOf15MinFailedTransferJobs	15 minutes
numOf5MinFailedTransferJobs	5 minutes

Number of partially successful jobs

The parameters in the following table gives the corresponding total number of partially successful jobs in IEMS for the specified time interval in the Time interval column.

Parameter	Time interval
numOf24HrPartialSuccessfulJobs	24 hours
numOf12HrPartialSuccessfulJobs	12 hours
numOf60MinPartialSuccessfulJobs	60 minutes
numOf30MinPartialSuccessfulJobs	30 minutes
numOf15MinPartialSuccessfulJobs	15 minutes
numOf5MinPartialSuccessfulJobs	5 minutes

Collection job details

The details of the collection job can be queried for a specific job. The following table has the parameters under corresponding details of the collection job:

Parameter for collection job name	Parameter for collection job identifier	Parameter for collection job start time	Parameter for collection job execution time
fiveMinCollectionJob Name	fiveMinCollectio nJobID	fiveMinCollectionJob StartTime	fiveMinCollectionJobExec utionTime
fifteenMinCollectionJ obID	fifteenMinCollect ionJobID	fifteenMinCollectionJo bStartTime	fifteenMinCollectionJobEx ecutionTime

Parameter for collection job name	Parameter for collection job identifier	Parameter for collection job start time	Parameter for collection job execution time
thirtyMinCollectionJobID	thirtyMinCollectionJobID	thirtyMinCollectionJobStartTime	thirtyMinCollectionJobExecutionTime
sixtyMinCollectionJobID	sixtyMinCollectionJobID	sixtyMinCollectionJobStartTime	sixtyMinCollectionJobExecutionTime

Report job details

The details of the Report job can be queried for a specific job. The following table has the parameters under corresponding details of the Report job:

Parameter for report job name	Parameter for report job identifier	Parameter for report job start time	Parameter for report job execution time
fiveMinReportJobName	fiveMinReportJobID	fiveMinReportJobStartTime	fiveMinReportJobExecutionTime
fifteenMinReportJobID	fifteenMinReportJobID	fifteenMinReportJobStartTime	fifteenMinReportJobExecutionTime
thirtyMinReportJobID	thirtyMinReportJobID	thirtyMinReportJobStartTime	thirtyMinReportJobExecutionTime
sixtyMinReportJobID	sixtyMinReportJobID	sixtyMinReportJobStartTime	sixtyMinReportJobExecutionTime

Transfer job details

The details of the Transfer job can be queried for a specific job. The following table has the parameters under corresponding details of the Transfer job:

Parameter for transfer job name	Parameter for transfer job identifier	Parameter for transfer job start time	Parameter for transfer job execution time
fiveMinTransferJobName	fiveMinTransferJobID	fiveMinTransferJobStartTime	fiveMinTransferJobExecutionTime
fifteenMinTransferJobID	fifteenMinTransferJobID	fifteenMinTransferJobStartTime	fifteenMinTransferJobExecutionTime
thirtyMinTransferJobID	thirtyMinTransferJobID	thirtyMinTransferJobStartTime	thirtyMinTransferJobExecutionTime
sixtyMinTransferJobID	sixtyMinTransferJobID	sixtyMinTransferJobStartTime	sixtyMinTransferJobExecutionTime

IEMS Server restart count

The "systemRestartCount" parameter gives the number of times IEMS Server restarted. This parameter is present in `iems_system.xml` which is located in the `/opt/nortel/iems/current/oidtemplates` folder.

Topology parameters

The description of the topology operational measurements are described in the following sections. All the topology operational measurement parameters are present in `iems_topology.xml` which is located in the `/opt/nortel/iems/current/oidtemplates` folder.

Number of added managed objects

The "numOfAddedManagedObjects" parameter gives the number of managed objects added to IEMS topology on the given time interval.

Number of devices in System_Unmanaged state

The "numOfDevicesInSystemUnManagedState" parameter gives the number of devices that are being unmanaged by the Event throttling process. For a description of System_Unmanaged state, refer to "Understanding the fault interface state of managed objects" in *IEMS Fault Management*, NN10334-911.

Number of unknown device state transitions

The "numOfUnKnownDeviceStateTransitions" parameters gives the number of devices that has gone to unknown state in the given time interval.

Total number of managed objects

The "numOfManagedObjects" parameter gives the total number of managed objects in the IEMS topology.

Number of devices in unmanaged state

The "numOfDevicesInUnManagedState" parameter gives the number of managed objects in unmanaged state.

Number of devices in Throttled State

The "numOfDevicesInThrottleState" parameter gives the number of devices that are being Throttle_Unmanaged state in the IEMS topology. For a description of System_Unmanaged state, refer to "Understanding the fault interface state of managed objects" in *IEMS Fault Management*, NN10334-911.

Number of system Unmanaged device state transitions

The "numOfSystemUnManagedDeviceStateTransitions" parameter gives the number of devices that are being unmanaged by the Event throttling Process due to overload during the given time interval.

Number of deleted managed objects

The "numOfdeletedManagedObjects" parameter gives the number of managed objects deleted on the given time interval.

Number of devices in Unknown state

The "numOfDevicesInUnKnownState" parameter gives the number of managed objects which are in Unknown state.

Number of Throttled device state transitions

The "numOfThrottledDeviceStateTransitions" parameter gives the devices that are being throttled by the Event throttling Process during the given time interval. For a description of System_Unmanaged state, refer to "Understanding fault interface state of managed objects" in *IEMS Fault Management*, NN10334-911.

Logging out of the Java Web Start client

Application

Use this procedure to log out of the IEMS Java Web Start Client.

Logging out of Java Web Start is advisable after you complete required tasks in the IEMS Java Web Start Client.

To exit Java Web Start Client while reconnecting to the server, refer to "Exiting the Java Web Start Client while reconnecting to the server" (page 127) of "Reconnecting Java Web Start client with the server" (page 127).

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Java Web Start Client (refer to "Launching the IEMS Java Web Start Client" (page 21)).
- 2 Select the **File-->Exit** menu command.
OR
Click the **x** button in the task bar of the Java Web Start Client.
A dialog asks for confirmation for exiting the Java Web Start Client with the message "Do you really want to exit the client?".
- 3 Click the **Yes** button in the confirmation dialog to exit the Java Web Start Client.
- 4 You have completed this procedure.

—End—

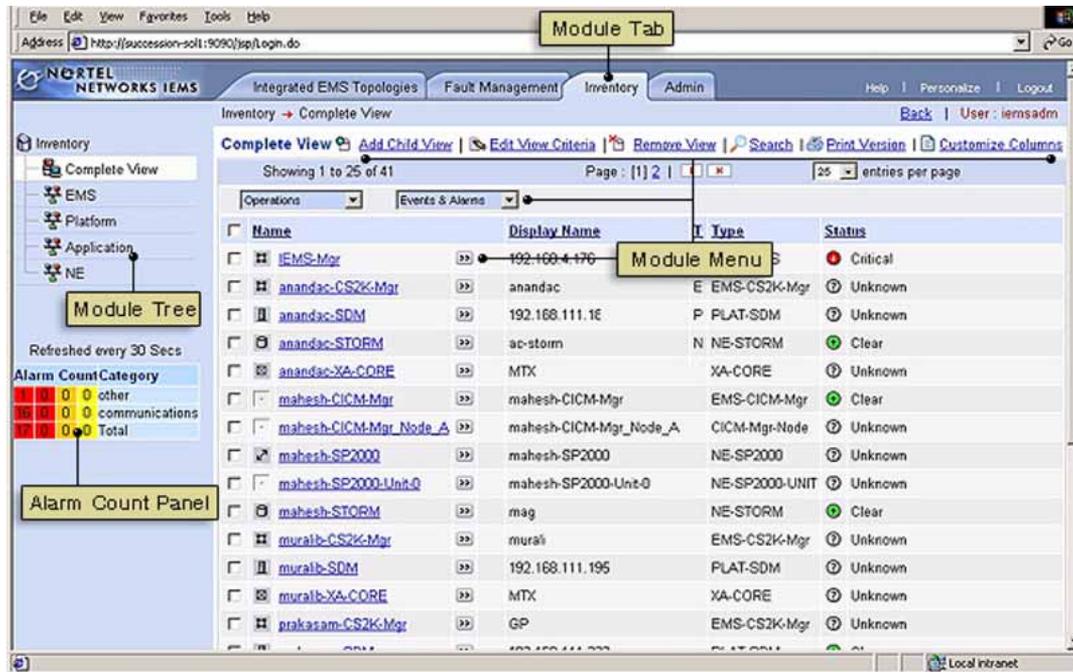
Overview of the Web Client interface

IEMS Web Client is a light-weight interface that allows you to connect to the IEMS Server using a Web browser over the local network or the Internet. Lower download time and lower bandwidth utilization serve as prime factors of the Web Client. Using a Web browser on any PC or UNIX operating system, you can log on to the Web and access IEMS for maps, fault, and other network information. The Web Client enables you monitor your network easily from any place and at any time.

Using the Web Client, you can do the following:

- view network management modules such as topology, fault, inventory, user administration, and add objects which are completely localized
- view network maps that provide a graphical display of network elements
- view faults occurring in a network
- view the database entries of network elements
- create custom views for to view network element information
- search for network elements
- perform administrative functions such as adding new networks or nodes and managing faults
- perform user administration tasks such as adding new users, modifying user profiles, and removing users
- add element managers, EMS applications, EMS platforms and NE objects

There are three frames in the screen; Tree Frame, Display Frame, and the Alarm Count Frame.



Module tabs

Use the module tabs to navigate the features of a module. The modules in IEMS Web Client are as follows:

- IEMS Topologies
- Fault Management
- Inventory
- Admin

Click a tab to display the respective module view in the display frame of the Web Client.

Module tree

A tree on the left hand-side of the Web Client contains nodes. The tree differs from one module to the other. Click a tree node to get related information in the display frame of the Web Client. For example, in the Topologies view, click the Element Managers node in the tree to display the element managers in the network.

Module menus

Menus are available as drop-down boxes, links, and icons. The drop-down boxes and links are available only in the Fault Management and Network Database views. The drop-down boxes contain a set of commands that are helpful when you need to perform an operation over multiple elements in a

view. For example, in the Inventory view, click the icon to perform Delete Object and Traces over a single NE. In the same view, when you need to perform the same operation over more than one NE, select the check boxes of those NEs and then select the option in the drop-down menu.

Alarm count panel

The Alarm count panel shows the alarm count of each severity (major, minor, critical, info) of alarm. This panel is placed below the module tree. When you click the count in this panel, the alarms of specific severity are displayed in the corresponding alarm panel. For details, refer to "Viewing alarm counts" in *IEMS Fault Management*, NN10334911.

This subsection contains the following procedures for the basic features of the IEMS Web Client

- ["Launching the IEMS Web Client" \(page 158\)](#)
- ["Personalizing the Web Client" \(page 159\)](#)
- ["Logging out from the Web Client" \(page 160\)](#)

Launching the IEMS Web Client

Application

Use this procedure to launch the IEMS Web Client from the Java Web Start Client.

Action

Step	Action
------	--------

At the IEMS workstation

1 Launch the IEMS Java Web Start Client. Refer to "[Launching the IEMS Java Web Start Client](#)" (page 21).

2 Click the HTML UI button in the Java Web Start Client toolbar.



The Web Client window opens.

3 You have completed this procedure.

—End—

Personalizing the Web Client

Application

Use this procedure to personalize the Web Client.

You can personalize the Web Client using skins. The skins change the look of the Web Client. By default, the Web Client is displayed with the Steel Blue skin.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Launch the IEMS Web Client (refer to "[Launching the IEMS Web Client](#)" (page 158)).
- 2 Click the **Personalize** menu item provided at the top right side of the Web Client.
The Personalize page is displayed.
- 3 Choose the required skin from the list of skins.
A preview of the skin is shown in the same page.
- 4 Click the **Apply** button.
The complete Web Client's look and feel is changed to the skin type you choose.
- 5 You have completed this procedure.

—End—

Logging out from the Web Client

Application

Use this procedure to log out of the Web Client.

When you have completed all the required tasks in IEMS Web Client, it is advisable to log out of the Web Client.

Action

Step	Action
------	--------

At the IEMS workstation

- 1 Select the **Logout** menu item at the top right hand side of the Web Client.

OR

Click the **x** button in the task bar of the Web Client.

After exiting the Web Client, if you click the **Back** button of the browser to get back to the last accessed page of the Web Client where a task was performed, a log in page appears. Because the last session was closed, the log in page allows you to login.

- 2 You have completed this procedure.

—End—

Troubleshooting tips

You may encounter error messages and difficulties while working with IEMS. This section provides tips to overcome some of the error messages and difficulties faced while working with IEMS Java Web Start Client and Web Client.

1. Disappearance of the Search dialog

When you launch the Search dialog in IEMS and click the IEMS Java Web Start Client main screen, the Search dialog screen disappears. You can find the Search dialog screen behind the IEMS Java Web Start Client main screen. Move the IEMS Java Web Start Client main screen to view the Search dialog. This scenario occurs with IEMS Java Web Start Client on the Sun Solaris platform.

2. Disappearance of the Event Details windows

If you open several Event Details windows you can hide other Event Details windows. To view hidden Event Details windows move the IEMS Java Web Start Client main screen or invoke a new Event Details window. This scenario occurs with IEMS Java Web Start Client on the Sun Solaris platform.

3. Browser not launched when accessing Help

When you access help from the IEMS Java Web Start Client, the browser is not launched. This occurs because the default browser is not included in path of Java Web Start. In the Java Web Start Application Manager, provide the command (used to invoke browser from command line) in the Path field of General tab. This scenario occurs with IEMS Java Web Start Client on Sun Solaris platforms.

4. Security Tree not showing nodes under Users and Groups

If the Security tree does not show nodes under the Users and Groups node, refresh the Security Administration window using the refresh tool button in the toolbar.

5. Topology GUI inaccessible

If the topology GUIs are inaccessible or you cannot right-click the map symbols in the topology GUI, refresh the GUI by clicking the refresh tool button in the IEMS Java Web Start Client toolbar.

6. Security Notice window inaccessible

After you provide the user name and password while logging into the IEMS, the Security Notice window (shown before the Client launch) is launched. If the IEMS Server (to which the client is connected) is shutdown or not running when you are in the Security Notice window, the Security Notice becomes inaccessible. For IEMS Java Web Start

Client, the reconnect dialog can be seen as a task in the task bar. Click the **Exit** button in the reconnect dialog.

7. Unable to launch Web Client from Java Web Start Client

In a workstation with Netscape as default browser, if you are unable to launch Web Client from Java Web Start Client using the toolbar, follow one of these steps:

- a. Remove all the stored cookies.

To remove the cookies in Netscape, follow these steps:

- i. Select the **Edit-->Preferences** menu command.
- ii. In the Privacy&Security tree, select the Cookies node.
- iii. Click the **Manage Stored Cookies** button to launch the Cookie Manager window.
- iv. Click the Remove **All Cookies** button.

- b. Close all the existing browser windows.

8. Launch of IEMS Java Web Start Client hangs

When trying to log into the IEMS, you are unable to connect the IEMS Server using the IP address of the IEMS server and launch the IEMS login page. That is, when you attempt to launch the IEMS Java Web Start Client by selecting **Web Start Client** from the IEMS, the login page appears to hang with no response.

The probable cause can be a DNS configuration issue. The IEMS client workstation and the IEMS server host must be DNS enabled. Determine if there is a DNS issue by performing the following tests:

- Use the nslookup tool on the IEMS Server host to look up the IEMS Server IP and host name. If this test fails, investigate the DNS issue on the IEMS server.
- Use the nslookup tool on the client to look up the IEMS server IP and host name. If the DNS lookup passed on the server, and this test fails, investigate the DNS lookup issue on the IEMS client workstation.

9. Unable to connect to the IEMS server.

The client is unable to connect to the IEMS server with its default browser (http://host_name_IP_address:9090/).

The probable cause can be that the IEMS server has not started. To verify that the IEMS server has started, refer to "Viewing the IEMS server status" in *IEMS Administration and Security*, NN10336-611. If

the IEMS server has not started, start the IEMS server, refer to "Starting the IEMS Server" in *IEMS Administration and Security*, NN10336-611.

10. Map symbols overlap in topology panels after adding objects

If the map symbols are disturbed or moved in the topology panel, then objects are added to the same topology panel. The added map symbols can overlap with existing map symbols. To rearrange the map symbols properly, select the **View-->Refresh** menu command.

11. IEMS Java Web Start Client takes more than twenty minutes to start.

If the IEMS Java Web Start Client takes more than twenty minutes to start, the DNS is not configured against the virtual IP address of box in which IEMS Server is installed. To configure the DNS against the virtual IP address of box in which IEMS Server is installed, follow these steps:

- a. Enter the following command and press the **Enter** key.

```
# getpip.ksh IEMS
```

The virtual IP address is displayed similar to the following output:

```
101.213.112.208
```

- b. Set the above virtual IP address for the DNS configuration. For the DNS configuration procedure, refer to "[Configuring Domain Name Service on an SPFS-Based Server](#)" (page 164)

12. Disappearance of launched applications from the IEMS client

If Mozilla is the default browser in the Microsoft Windows platform, the Mozilla browser does not always come to foreground when an application is launched from IEMS client. If you have launched an application and the application is not displayed, try moving (or minimizing) windows that are in the foreground to uncover the application.

Configuring Domain Name Service on an SPFS-Based Server

Application

Use this procedure to configure Domain Name Service (DNS) on a Server Platform Foundation Software (SPFS) based server.

ATTENTION

Do not configure an SPFS-based server that is hosting the Core and Billing Manager (CBM) as a DNS client. The CBM must never be configured to act as a DNS client.

A HTTPS certificate must be installed and DNS must be enabled on the following SPFS platforms:

- IEMS
- CS 2000 Management Tools
- MG 9000 Element Manager

This procedure provides the instructions for the following tasks:

- ["Configure DNS on a master server" \(page 165\)](#)

ATTENTION

A Call Server LAN (CS LAN) only uses one DNS master server. Configure other hosts in the CS LAN that use DNS to use the DNS master server.

- ["Add \(remove\) a host entry in the DNS database" \(page 168\)](#)
- ["Configure server as a DNS client" \(page 170\)](#)
- ["Turn off DNS capability on the server" \(page 173\)](#)

ATTENTION

Perform the steps under ["Turn off DNS capability on the server" \(page 173\)](#) when the DNS master server function is no longer required, or if the DNS master server function is moving to a different server. If needed the server can then be configured as a DNS client using the steps under ["Configure server as a DNS client" \(page 170\)](#).

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password for the server
- you need the office CLLI to complete the steps under ["Configure DNS on a master server" \(page 165\)](#)

- you need to complete the steps under "Configure DNS on a master server" (page 165) prior to performing the steps under "Add (remove) a host entry in the DNS database" (page 168)
- you need familiarity with the "vi" editor to perform the steps under "Add (remove) a host entry in the DNS database" (page 168)

Action

Perform the following steps to complete this procedure.

Step Action

At your workstation

- 1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- 2 Log in to the server using telnet (unsecure) as follows:
 - a. Log in to the server by typing


```
> telnet <server>
```

 and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that you want to configure as a DNS master server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.
 - b. When prompted, enter your user ID and password.
 - c. Change to the root user by typing


```
$ su - root
```

 and pressing the Enter key.
 - d. When prompted, enter the root password.

Proceed to step 4.
- 3 Log in using ssh (secure) as follows:
 - a. Log in to the server by typing


```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that you want to configure as a DNS master server

ATTENTION

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter the root password.

4 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

5 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
```

```
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Application Configuration
4 - CORBA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
```

```

19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -

```

- 6** Enter the number next to the "DNS Configuration" option in the menu.

Example response

```

DNS Configuration
1 - turn_dns_on (Configure as DNS client)
2 - turn_dns_off (Turn off a system's DNS capability)
3 - enable_dnssvr (Configure as DNS server)
X - exit
select -

```

- 7** Enter the number next to the "enable_dnssvr" option in the menu.

Example response

```

===Executing "enable_dnssvr"
Enter domain name for the office:

```

- 8** When prompted, enter the domain name for the office.

This procedure configures a DNS master server that is not connected to any other DNS zones outside of the CS LAN. To allow possible future connections of CS LAN DNS zones, it is recommended that the domain name for each CS LAN be the office CLLI.

- 9** If prompted, indicate whether you want to overwrite the existing DNS configuration.

Example response

```

Configuring with:
hostname: <hostname>
DNS domain: <office clli>
server IP: <IP address>
Starting DNSSVR through servstart
DNSSVR Started
=== "enable_dnssvr" completed successfully

```

- 10** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

- 11** Verify that DNS is working by typing

```
# nslookup <hostname>
```

and pressing the Enter key.

Example response

```

Server: <hostname>.<domain name>
Address: <IP address>
Name: <hostname>.<domain name>
Address: <IP address>

```

You have completed this procedure.

—End—

Add (remove) a host entry in the DNS database

Step Action

At your workstation

- 1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- 2 Log in to the server using telnet (unsecure) as follows:
 - a. Log in to the server by typing


```
> telnet <server>
```

 and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.
 - b. When prompted, enter your user ID and password.
 - c. Change to the root user by typing


```
$ su - root
```

 and pressing the Enter key.
 - d. When prompted, enter the root password.

Proceed to step 4.
- 3 Log in using ssh (secure) as follows:
 - a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that you want to configure as a DNS master server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter the root password.

- 4 Add or remove host entries in the DNS database, which entails editing two files; the "forward" (hosts) zone file, which translates domain names to IP addresses, and the "reverse" (hosts.rev) zone file, which translates IP addresses to domain names.

Increment the "serial" number at the beginning of each zone file every time you update the file.

The zone files will only be present if a DNS master server was configured. If required, refer to the steps under "[Configure DNS on a master server](#)" (page 165).

Following is an example of adding a host named "annex" with an IP address of "45.136.123.46". The serial number for the file is also incremented to 2. In the example, the domain name (or office CLLI if used as domain name) is "loco".

```
# vi /data/dns/named/hosts
```

Example response:

```
$TTL 3h
; SOA
loco. IN SOA apex.loco. root.apex.loco (
                                2    ; Serial
                                3h   ; Refresh
                                15   ; Retry
                                1W   ; Expire
                                3h  ) ; Minimum

; name servers
loco. IN  NS   apex.loco
; addresses
apex  IN   A   45.136.123.70
annex IN   A   45.136.123.46
```

```
# vi /data/dns/named/hosts.rev
```

Example response:

```

$TTL 3h
; SOA
123.136.45.in-addr.arpa. IN SOA apex.loco.
root.apex.loco (
                                2   ; Serial
                                3h  ; Refresh
                                15  ; Retry
                                1W  ; Expire
                                3h ) ; Minimum

; name servers
123.136.45.in-addr.arpa. IN  NS   apex.loco
; addresses
70.123.136.45.in-addr.arpa IN  PTR apex.loco
46.123.136.45.in-addr.arpa. IN  PTR annex.loco

```

5 Restart the DNS service by typing

```
# servrestart DNSSVR
```

and pressing the Enter key

Example response

```

Stopping DNSSVR
Starting DNSSVR
DNSSVR re-started successfully

```

You have completed this procedure.

—End—

ATTENTION

Do not execute the procedure that follows on an SPFS-based server that is hosting the Core and Billing Manager (CBM). The CBM must never be configured to act as a DNS client.

Configure server as a DNS client

Step Action

At your workstation

- 1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- 2 Log in to the server using telnet (unsecure) as follows:

- a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

- b. When prompted, enter your user ID and password.
- c. Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- d. When prompted, enter the root password.

Proceed to step 4.

- 3 Log in using ssh (secure) as follows:

- a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that you want to configure as a DNS master server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

- b. When prompted, enter the root password.

- 4 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
X - exit
```

```
select -
```

- 5 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Application Configuration
5 - CORBA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -
```

- 6 Enter the number next to the "DNS Configuration" option in the menu.

Example response

```
DNS Configuration
  1 - turn_dns_on (Configure as DNS client)
  2 - turn_dns_off (Turn off a system's DNS
    capability)
  3 - enable_dnssvr (Configure as DNS server)
X - exit
select -
```

- 7 Enter the number next to the "turn_dns_on" option in the menu.

- 8 When prompted, confirm the command by typing

yes

and pressing the Enter key.

- 9 When prompted, enter the DNS domain.

Example

us.nortel.com

- 10 When prompted, enter the IP address of a DNS server.
- 11 When prompted, enter the IP address of a second DNS server.
- 12 When prompted, enter the IP address of another DNS server. If there are no other DNS server addresses to enter, press the Enter key.
- 13 When prompted, enter the name of a search domain.

Example
us.nortel.com
- 14 When prompted, enter the name of another search domain. If there are no other search domains, press the Enter key.
- 15 Accept the DNS configuration that is displayed by typing

ok

 and pressing the Enter key.
- 16 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

select - x

 and pressing the Enter key.

You have completed this procedure.

—End—

Turn off DNS capability on the server

Step	Action
------	--------

At your workstation

- 1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- 2 Log in to the server using telnet (unsecure) as follows:
 - a. Log in to the server by typing

> telnet <server>

 and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d. When prompted, enter the root password.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that you want to configure as a DNS master server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter the root password.

4 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
```

```
1 - View
```

```
2 - Configuration
```

```
3 - Other
```

```
X - exit
```

```
select -
```

5 Enter the number next to the "Configuration" option in the menu.

Example response

Configuration

```

1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Application Configuration
5 - CORBA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -

```

- 6** Enter the number next to the "DNS Configuration" option in the menu.

Example response

```

DNS Configuration
1 - turn_dns_on (Configure as DNS client)
2 - turn_dns_off (Turn off a system's DNS capability)
3 - enable_dnssvr (Configure as DNS server)
X - exit
select -

```

- 7** Enter the number next to the "turn_dns_off" option in the menu.

Example response

```

===Executing "turn_off_dns"
Do you really want to turn off DNS? (default: No):

```

- 8** When prompted, confirm you want to turn off DNS capability by typing

yes

and pressing the Enter key.

Example response

```

Group registered
Stopping group using servstop
DNSSVR Stopped
DNS successfully turned off

```

```
=== "turn_dns_off" completed successfully
```

- 9 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

—End—

Carrier VoIP

IEMS Overview

Copyright © 2006, Nortel Networks
All Rights Reserved.

Publication: NN10329-111
Document status: Standard
Document version: 04.02
Document date: 20 October 2006

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

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

The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose it only to its employees with a need to know, and shall protect it, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

